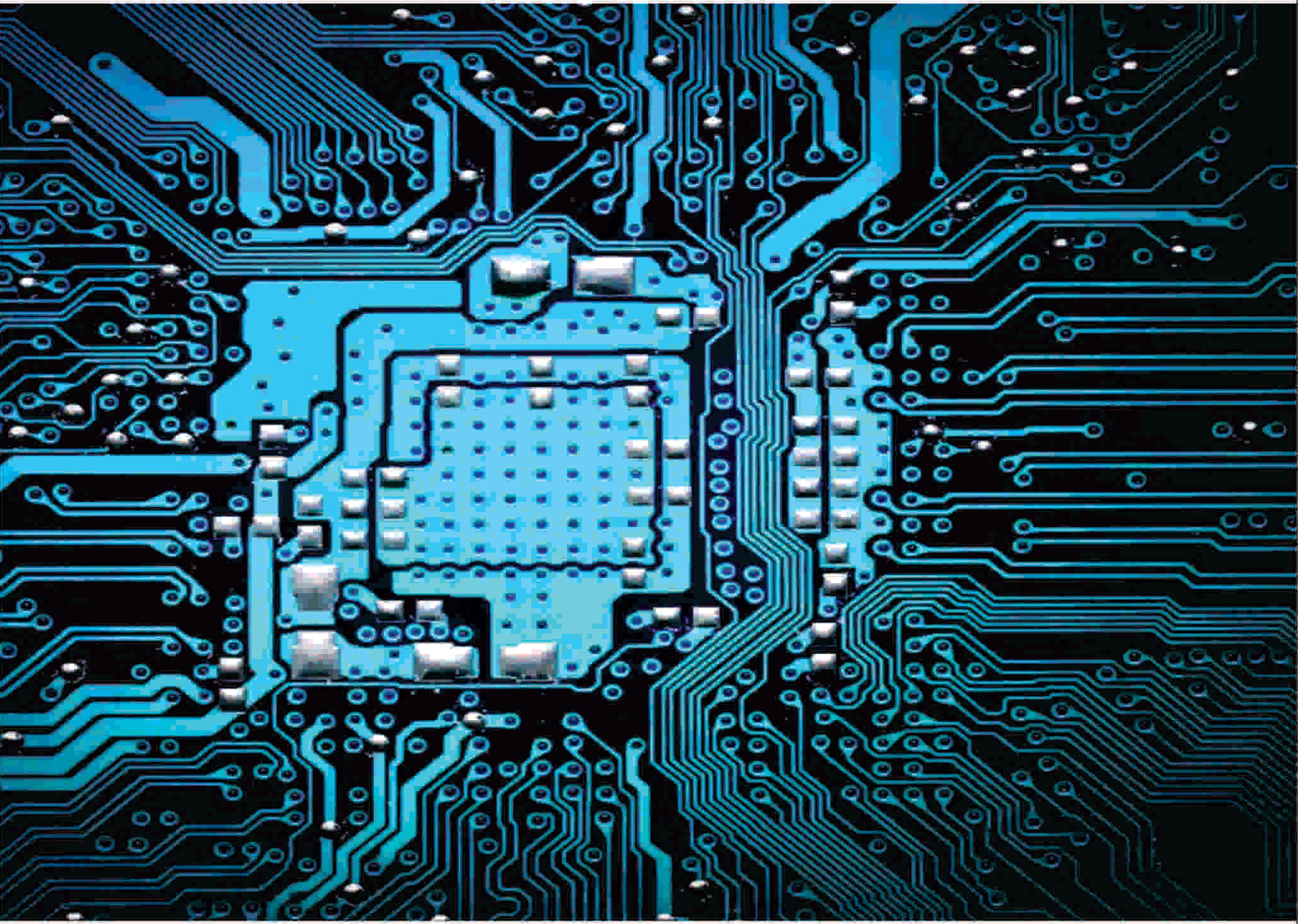
ISSN 2616-6003 (Online)
ISSN: 2522-3429 (Print)

International Journal for Electronic Crime Investigation (IJECI)



Vol. 3 Issue: 3
ISSUE: July - September 2019

Email ID: ijeci@lgu.edu.pk

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

LGU International Journal for Electronic Crime Investigation
Volume 3(3) July - September (2019)

CONTENTS

Research Article

Dr Aftab Ahmad Malik , Mujtaba Asad, Waqar Azeem

Deficiencies In Peca And Proposed Amendments To Facilitate
Investigating Agencies, Courts And Prosecution; Proper Use Of Electronic Devices
For Effective Implementation Of Law 1-6

Research Article

Muhammad Arslan Tariq, Rehmatullah, Waheed-ul-Hassan

Anomaly based Intrusion Detection System 7-13

Research Article

Fatima Fatima

Forensics Analysis of Typewriter and Typewritten Documents 14-22
Research Article

Research Article

Muhammad Shairoze Malik

Cyber Security - Incident Response and Management 23-28

Research Article

Syeda Binish Zahra, Syed Muhammad Shabih-ul Hassan

Effects of Emotions in Cognitive Based Game 29-37

LGU International Journal for Electronic Crime Investigation

Volume 3(3) July - September (2019)

Malik et al LGURJCSIT 2019

LGU International Journal for
Electronic Crime Investigation

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

Research Article

Vol. 3 Issue 3, July - September 2019

Deficiencies In Peca And Proposed Amendments To Facilitate Investigating Agencies, Courts And Prosecution; Proper Use Of Electronic Devices For Effective Implementation Of Law

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

Abstract:

The purpose of this paper is to analyze and propose amendments in the Pakistan Electronic Crime Act (PECA). It is observed that the Act contains some inherent weaknesses and difficulties due to which some criminals may set free. The investigating agencies, courts, prosecution and the defense attorney formulate a system and work within the ambit of the applicable laws. They derive their strength from the explicit provision of Law and the prescribed procedure. In the case of Electronic Crimes, the forensic evidence, its organization and presentation in the court of law is of pivotal importance. Any deficiency, for example, in procurement of evidence may destroy the entire case of the prosecution in court. The lack of evidence or incorrect procedure of its procurement helps the defense attorney. The judges have to give the verdict keeping in view the well organized and consistent evidence and also under the explicit provisions of law. The central idea of this paper is to make effective modifications and amendments in PECA, as it lacks "proper and soundproof" system for procuring general evidence, forensic and electronic evidence. The paper also focuses on these procedure.

Key Words: Electronic Crimes, Cyber Evidence collection, Electronics Devices

1. Introduction:

The extensive use of digital media and electronics devices has caused an increase in cybercrimes and there has been a need to constitute the law for the protection of rights of citizens. This has adversely curtailed some of the constitutional rights of citizens. The digital forensic and evidence collection is of pivotal importance; it includes computer forensic, incidence response, evidence from mobile, videos, voice biometrics, password recovery and data recovery from demaged devices. The PECA "Prevention of Electronic Crimes Act 2016", was introduced to fight with offenses such as harassment, terrorism infringement of right of privacy of citizens and right to express. According to [1], there have been reservationsin favor and against this bill by a few parliamentarians and the media at the time of its promulgation and making it public. It is reported in [1] that the parliament committee did not appreciate some objections such as sinister, menacing, ominous, creepy and baleful.

The difference between PECA and legislation formerly implemented on the subject of cybercrimes are mostly related to the computer-aided crimes, while the present laws are also relevant to the speeches and actions reflecting criminal behavior. The underline philosophy to implements PECA is to deal with extremist and terrorist activities such as the killing of our innocent children at Army Public School, Peshawar.

Major Objectives of PECA have been to prosecute hate speech, harassment online, and fighting with terrorism including criminal defamation using I.T systems. We know that the well known top cybercrimes are infringement of privacy, online harassment, hacking personal data of users by illegal means. More effective legislation is the need of the day. A critical discussion has been presented in [2] stressing the need to take necessary measures to make the legislation more effective for implementation. A detailed discussion, procedure and relevant legal points have been raised in [4] and [5] in the context of "Prevention of Electronic Crime Act 2016" and the use of Cyber Space by terrorist organizations.

2. Some Concerns and Reservations about PECA

The complete procedure for collection of evidence must have been a salient feature; which the Act lacks. The unclear provisions in any law are examined on the basis of "Doctrine of Vagueness", which needs the laws to describe clearly the punishable conduct; otherwise, it may be rendered as void.

Vagueness Definition:

Duhaime's Law Dictionary defines "a law which lacks in precision as not to give sufficient guidance for legal debate. Vagueness is a doctrine of constitutional law; and grounds upon which a statute can be found to be inoperative. Every law must be sufficiently clear for the citizens to grasp its import."

According to [2], terrorists use digital tunnels or darknet, which is difficult to trace without adequate expertise; PECA is silent about these terminologies and technologies. Such issues need to be properly tackled and redressed in the revised/amended version of PECA. According to [3], several provisions of PECA are controversial and create the problems due to the restrictions imposed such as potential harm to the right of privacy. According to [6] PECA provides the provision for warrants of retention, search, to have access and for information collection in real-time.

There are concerns of legal experts about certain sections of PECA such as sections 3, 4, 5, 6, 7 and 8 and it is advocated and proposed to make them more effective to strengthen the investigating agencies specially FIA, the prosecution and hence the Courts.

Section 3 prohibits unauthorized access to the information system or data.

Section 4 prohibits unauthorized copying and transmission of data.

Section 5 prohibits interference with information systems or data

Section 6 provides punishment for unauthorized access to critical infrastructure information systems or data.

Section 7 deals with unauthorized copying or transmission of critical infrastructure data.

Section 8 deals with Interference with the critical infrastructure information system or data.

Section 9 relates Glorification of an offense relating to terrorism

Section 10 properly covers the ambit of cyber terrorism envisaged by the above-mentioned sections from 6 to 9.

The sections 31, 33, 34 and 35 provide the procedure for accessing the Data by the investigating officer.

Under Section 37 exclusive powers are entrusted to the PTA (Pakistan Telecommunication Authority) to remove online or block contents of information, this apparently seems contrary to Article 19 of the Pakistan Constitution according to critics. The information to be removed or blocked normally is repugnant to or derogatory to Islamic injunctions, decency, public order or defense of Pakistan. There is provision for the review of the orders of the authority. However, the High Court has the jurisdiction to listen to appeals.

The PECA defines the dishonest intension as quoted below:

"Dishonest Intention" means intention to cause injury, wrongful gain or wrongful loss or harm to any person or to create hatred or incitement to violence".

The counter-terrorism wing of the Federal Investigation Agency (FIA) has the powers to summon, detain and investigate the political activists and journalists on the issues of “anti-state activities”, propaganda against armed forces, state functionaries and institutions. The PECA provisions must be strong enough to support FIA, prosecution and the court of Law to reach the just decision.

The important factor to be looked into the matter is the intention of the offender. The kind of intention may be that of coercion, intimidation, to create a sense of fear, panic or insecurity. The question arises on how the investigating officer and prosecution should prove the existence of a factor of intimidation, to create a sense of fear, panic or insecurity from the forensic evidence. PECA gives extensive powers to agencies to access private information or Data or to copy and transmit it.

PECA offends the constitutional guarantees of ”due process of law” provided in the Pakistan Constitution. The definition of an “act” is not comprehensive, which is defined as a “series of acts”. Similarly, the definition of dishonest intention lacks having been defined as similar to legal injury. The words “to create hatred” included in the definition, makes it difficult to prove guilt. Moreover, Cyber-terrorism has not been properly linked with violence and the risk of harm.The prosecution shall have to prove the dishonest intention also when the offender has caused, intimidation, created a sense of fear, panic or insecurity. For this purpose, well qualified and trained personnel are required having expertise in legal, electronics and computer science. A detailed overview of Pakistan's Cybercrime Law has been presented in [12].

3. The Notion of Dishonest Intention

Certain actions committed with dishonst intention are offences. For example, opening a bank account, having unauthorized access to the networks, computer accounts or documents and to impersonate a police officer. The acts of lying , misrepresentation, immoral and unethical behavior, theft at work place by violation of “code on coduct”, such as harassment or drug abuse in office; normally such offences are committed with dishonest intetions.

4. PECA Lacks Proper Procedure for Acquiring Evidence

Although the section 31 is related to preservation and acquisition of the Data by the authorized agents, it must be reasonably and properly acquired for criminal investigation. The investigating officer uses randomly his powers what is legally termed as blanket authorization, which lacks checks and balances. The Blacks Law Dictionary defines the Blanket Authorization [16] as a contract letting a party to do an activity with no approval.

This provision is perhaps capable of being used against political opponents. The investigating team may consist of the personnel from the following penal:

- Forensic Specialist,
- High Tech Crime personnel,
- Cyber Security Specialist
- Computer Forensics Lab representative from Computer Crimes unit, Forensic and Technical Services
- Computer Specialist, R&D

5. Important Steps in Digital Evidence Processing

For the purpose of processing the evidence, following procedure should be adhered to in the logical order as per policy and rules of the investigating agency, Evidence Assessment, Evidence Acquisition, Evidence Examination and Reporting. The assessment of forensic evidence is of fundamental importance. As the foresic evidence is fragile and can be demaged or changed, therefore, at the time of acquisition special care must be taken to preserve it with integrity and all contents intact. It ia always recommended to make best bit-by-copy of the original evidence. During the examination of the evidence, we extract, analyse and recover the relevant Data and then legally interpret it after making it logicaly in useful form. Afterwards, we perform activities such as, examination of the partition system, physical extraction, logical extraction of data from drive, extraction of file system and file sizes with their locations, recovery of deleted files, encrypted and compressed data. Final step is the prepreation of written report containing the conclusions and findings.

The findings must enlist all files with detailed description and relevance to evidence along with those of deleted files, graphics, pictures, hidden files and hidden attributes.

6. Forensic Image MD5 must be Prepared at Scene of Offence

According to [13], The basic way to preserve the evidence is obtaining mirror image of hard disk, which is called forensic image or hard drive clone. It is the bit-to-bit exact copy of the original hard disk obtained from the scene of crime.

This paper highly recommends that the image or clone be prepared at the scene of offence at the time of collection of forensic evidence to avoid future complication in the court.

Technically speaking, MD5 is a versatile method called Message Digest Algorithm. Actually, it is a cryptographic Hash function, which can check and verify that the contents of the file or drive have not been changed. On input of any size it returns the requisite output authenticating the input. "The output from MD5 is a 128-bit message digest value". The following are relevant particulars discussed [14]:

Digest sizes: 128 bit

Block sizes: 512 bit

Rounds: 4

7. Devices where the Criminal Data Resides

There are several ways and means to store the Data and place it. The most useable in practice are the Cloud Storage, Mobile devices like USB, Compact Disk, and other portable storage media, printed material, hard disk (Secondary memory devices), audio and video Disks Photographic images or stored data while communication onto websites using computers, mobile devices, and Networks.

8. National Force for Cybercrimes NR3C

According to [7], the Federal Investigating Agency (FIA) established the National Response Centre for Cyber Crimes in 2007 to fight against the misuse of technology in society. It possesses expertise in IT, digital forensics and Technical investigation. It is providing training to the Police, Judiciary, Lawyers and academia through short courses, seminars and workshops to create proceedings. The protection of recovered forensic information has been an important and debatable issue due to the undefined chain of custody of the information. Unfortunately, no proper procedure has been prescribed in PECA on how to collect and organize information.

The protection of recovered forensic information has been an important and debatable issue due to the undefined chain of custody of the information. been an important and debatable issue due to the undefined chain of custody of the information.awareness. There are a few examples of the areas of forensics used and exploited by offenders, such as legal difficulties arising due to ignorance of investigating officer.

It has been observed that often the embarrassing situations do arise in the court of law merely due to ignorance or lack of knowledge for not following up proper and complete procedure on the eve of collecting information at the scene of offense. There are four important pillars i.e. the court of law, the prosecutor, investigating officer and the attorney of the offender. Any pitfall in the collection of forensic evidence may destroy the case of the prosecution. Most of the time, the investigating agencies and investigating officers do not take the prosecutor in confidence. The prosecutor is also sometimes ill-informed about complete evidence collected and how it was acquired. In the case of naïve evidence and violation of procedure by investigating officer makes the case stronger for attorney of the offender.

9. Acquisition and Preservation of Data for Evidence

In case the forensic information is lying in the hands of unconcerned and incompetent personnel, it is liable to be forged or altered either at the disadvantage to the offender or to save him from the offense and allegations. The percentage of this factor is high. Therefore, the question of acquisition and preservation of Data is extremely important. Following are some points to observe while collecting and preserving the forensic Data:

- In case of Disks, a bit by bit copy be prepared at the time of procuring it on the scene of offence,
- The reliable chain of custody must exist in the office of Investigating agency who can preserve it with great care and caution.
- In case it is to be sent to the IT Experts, another similar bit-by-bit copy with complete index be prepared. This is what we term as forensic duplication of evidence.
- The copy may be handed over to the experts for evaluation in LAB, while the original documents or Disk shall reside with a reliable chain of custodians.

10. Preparing Clone and Mirror Image of the Hard Disks and a Golden Rule

Technically, the forensic image of the hard disk is termed as mirror image or hard drive clone. It is a pre-requisite for digital forensics proceedings to create an exact digital image of the devices such as fingerprint, hard drive, SSD, USB or other media. We create a unique digital image required for court proceedings so that the authenticity of collected forensic evidence is not challenged.The Golden Rule of digital evidence is that original media should never be changed. Therefore, it is very strongly recommended that the bit-by-bit mirror image (copy) be prepared, the process is called forensic imaging.

It is useful to know the difference between clone and image of a disk or media. The colon can be prepared by using image. The clone is a working and functional copy of the original hard disk, while the image is an "archive" of the disk and can be used to make a bit-by-bit true copy. The procedure for copying the disks has been discussed in depth in [8],[9], [10] and [11]. The digital forensic experts must know what is the appropriate tool is to be used to create the clone or an image; he must have appropriate qualifications and training. When the creation of image is complete any industry-standard tool can be used. A hash generation process looks up the entire zeros and ones which are across the source media. One way is copying Data from one Hard drive to another drive, the drive which is of larger size its blank spaces are filled with zeros after copying data onto it. We may copy Data from drive to a file sector by sector; the authors of this paper don't recommend this manner.

Conclusion

The PECA sections 3, 4, 5,6,7,8, 26 and 27 particularly need revision/amendments while other provisions also need minor revision, where there are pitfalls. The fundamental purpose of the promulgation of PECA was to facilitate certain procedures well defined under digital transformations, because of recent improvements in the innovation and advancement in electronic devices and procedures. The terrorists use digital tunnels or darknet, which is difficult to trace without adequate expertise; PECA is silent about some terminologies and technologies.This aspect and feature must be fulfilled.The investigating officers must be qualified and well trained in the current state-of-art in Internet, Computing, Information Technology and Law. The training facilities for FIA investigating teams may be arranged at the universities having advanced forensic Labs, for Example, Lahore Garrison University Lahore. The legal difficulties arising due to unqualified investigating officers may be minimized by either their replacement with highly skilled and qualified personnel or their training must be a regular feature to properly tackle the well-known Cybercrime categories particulrly Money Laundering, Hacking and Identity theft, violation of Intellectual property rights, Bank Frauds, financial misappropriation and electronic terrorism.

Acknowledgment

The authors are grateful to Mr. Kaukab Jamal Zuberi, Director Digital Forensics Research and Service Center (DFRSC), Lahore Garrison University for his encouragements. The authors also extend the gratitude to Dr Dil Muhammad Former Professor of Law College Punjab Univeristy, Lahore for guidance.

References:

[1]:Farieha Aziz (2018): "Pakistan's cybercrime law: boon or bane?"

Heirich Boll Stiftung, The Green Political Foundation and Perspective of Digital Asia.

[2]: Amir Shahzad (2019): "Cyber-Terrorism Law, Implementation and Ways Forward", LGU International Journal for Electronic Crime Investigation; LGUIJECI MS.ID-006 ; Volume 3(2) April – June.

[3]: Eesha Arshad Khan The Prevention of Electronic Crimes Act 2016: An Analysis, LUMS Law Journal Volume 5.

[4]: Zuberi, Kokab Jamal(2019): "Critical Review of Prevention of Electronic Crime Act 2016" (May 7)

[5]: Zuberi, Kokab Jamal. 2018. "Use Of Cyber Space By Terrorist Organization." Electronic Crime Investigation

[6]: Daudpota, Faisal (2016): "An Examination of Pakistan's Cybercrime Law"

https://ssrn.com/abstract=2860954 or http://dx.doi.org/10.2139/ssrn.2860954

[7]: www.fia.gov.pk

[8]: Sammons, J. (2015), "Digital forensics: threatscape and best practices". Syngress.

[9]: Gary Hunt, What is a Forensic Image? Best Practices, Forensics https://qdiscovery.com/what-is-a-forensic-image/

[10]: https://capsicumgroup.com/2-key-differences-between-digital-forensic-imaging-and-digital-forensic-clone-and-how-they-can-affect-your-legal-case/

[11]: "How To Make The Forensic Image Of The Hard Drive", https://www.digitalforensics.com/blog/how-to-make-the-forensic-image-of-the-hard-drive/

[12]: Faisal Daudpota(2018),"An Examination Of Pakistan's Cybercrime Law' (2016) Ssrn http://dx.doi.org/10.2139/ssrn.2860954

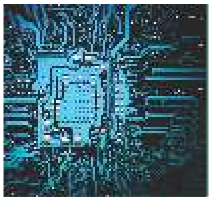
[13]: Gary Hunt,"What is a Forensic Image?"

Best Practices, Forensics.

[14]: Ronald Rivest, "Structure: –MerkleDamgård construction Designers"

[15]: Sarah V. Hart, John Ashcroft ,Deborah J. Daniels, " Forensic Examination of Digital Evidence, A Guide for Law Enforcement; Office of Justice Programs U.S. Department of Justice; 810 Seventh Street N.W.

[16]: https://thelawdictionary.org › blanket-authorization



Tariq et al LGURJCSIT 2019

LGU International Journal for
Electronic Crime Investigation

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

Research Article

Vol. 3 Issue 3, July - September 2019

Anomaly based Intrusion Detection System

Muhammad Arslan Tariq[1], Rehmatullah[2], Waheed-ul-Hassan[3]
arslan.tariq@lgu.edu.pk[1], rehmatullah@lgu.edu.pk[2], waheedhassan@lgu.edu.pk[3] Lahore Garrison University

Abstract:

In the digital World full of hackers and scammers, data security is what everyone needs the most. Hackers and scammers invent new ways of stealing information on daily basis. A method to come up with more precise system is Intrusion Detection system. IDS is todays need because, it helps the individuals to keep up their confidentiality and integrity. Intrusions, that disturbs the security and secrecy of the system, has become major concern for many organizations. The logic and ways Intrusion Detection System uses are related to these days. Through cloud computing, Intrusion Detection System has creäted a world where it can flourish and be most operative. By means of cloud computing, the fundament has engrossed with the Intrusion Detection technology.

Keywords— Anomaly Based IDS, IDS, Poly kernel, Normalized poly kernel RBF kernel

I. Introduction

An Intrusion Detection System is employed to differentiate every kind of vulnerable links available in traffic and systems that cannot be identified with traditional firewall. It includes network attacks against susceptible facilities, attacks on data driven applications and host-based networks such as enhancement in privilege, unlicensed access and logins to sensitive data and vulnerable files (i.e. Malwares, Trojans, and worms).

A. Need for Intrusion Detection System

Confidentiality is the main concern between individual and corporate sector. If these problems are not solved, businesses will not be in a better position to truly take advantage of all. Like, Sony Pictures Entertainment [1] experienced one of the most vulnerable commercial attack in the history. Thousands of records grabbed by hackers were revealed online with personal details of almost 6,000 employees of Sony, including Sony feature films and the salary details of top management. The hackers also achieved to retrieve details about Deloitte financiers who are Sony's auditors.

The above-mentioned data breach, that happened on 24th November, caused in the halt of whole computer network of one of Hollywood's prime and most authoritative studios. Here is the collective report that the hacking was carried out by North Korea in payback for the future release of a Sony comedy movie called "The Interview". The storyline tracks Seth Rogan and James Franco who were working in the CIA (Central Intelligence Agency) to eliminate Kim Jong-un the dictator of North Korea.

Industrial think tanks observed that almost 60,000 new, vulnerable computer programs and 315,000 new, vulnerable files are discovered daily. From 2006 to 2012, the number of security happenings stated by federal agencies amplified from 5,503 to 48,562 - a rise of 78.2% - and in 2013 McAfee investigation estimated that worldwide cybercrime failures might total $400 billion. Cyber-attacks are a risk to America's nationwide and financial security, in addition to separate privacy, to the fundamental and most important factor, corporate strategies, and knowledgeable property for all [8].

Cloud computing, though, has taken new applicability to IDS structures, resulting flow in the IDS marketplace. An important element of today's security top preparations, Intrusion Detection Systems are created to sense attacks that can happen regardless of preventive procedures. In fact, Intrusion Detection System is today's unique top selling security equipment and it is predicted to remain increase. Despite everything, cloud security is far too multifaceted to be checked physically.

This study deals with anomaly-based intrusion detection system. It uses support vector machine for model evaluation.

B. Support Vector Machine

Support vector machine (SVM) is the best-recognized algorithm for classification of binary data. It uses statistical learning method for classification and regression by using different kernel functions. Its applications include a wide range of pattern recognition applications and now it is popular in networks security due to good generality nature and to overcome the curse of dimensionality. The SVM selected the appropriate parameters for model evaluation.

C. Limitations of SVM

SVM is a supervised learning model required labelled data for learning. It is designed for Binary classification [14]. Another issue is training of support vector machine (SVM) is a time-consuming process and required a huge dataset. Thus, it is computationally costly, and resource restricted for informal networks, that increase the architecture complexity and decrease accuracy [10].

To resolve this issue NSL-KDD binary dataset is used where data is labelled as normal or Anomaly only.

II. Literature Review

Computer world is growing explosively. Computer System suffer security vulnerabilities that are technically difficult and economically costly. On KDD, test set is a classification rate of 86% to nearly 100%.

There square measures some issues within the KDD knowledge set that cause the analysis results on this knowledge set to be dishonest. That square measure mentioned below:

One of the foremost vital insufficiencies within the knowledge discovery in database's (KDD) dataset is that the immense variety of redundant stored information, that causes the training algorithms to be projected towards the frequent records, So, to stop them from learning uncommon records that square measures typically additional harm to networks like R2L and U2R attacks. Furthermore, the presence of these frequent records within the check set can cause the assessment results to be biased by the strategies that have higher detection rate on the repeated records [3].

Solution for this is to first take away all the redundant records in each training and testing set. Moreover, to make a different set of the knowledge discovery in databases (KDD) knowledge set, we have a tendency to willy-nilly sampled records from the #successfulPrediction price teams, in such how that the numeral of records chosen from every cluster is reciprocally proportional to the proportion of records within the original #successfulPrediction price teams. for example, the quantity of records within the #successfulPrediction price cluster of the KDD toy constitutes zero.04% of the initial records, therefore, 99.96% of the records during this cluster square measures enclosed within the generated sample. The generated knowledge sets, square measure KDDTrain+ and KDDTest+.

Dataset social control is important to boost the performance of IDS once amount of dataset is large. Hence, technique used is Min-Max technique of social control.

Features will be selected based on information gain. It was calculated as

Let [5] S be a group of training set samples with their match up labels. Imagine there are m categories/classes and the training set contains si samples of category/class I and s are that the total variety of samples within the training set. predictable data required to classify a sample is computed by:

Let Sj contain sij samples of class/category i. A feature F with values will divide the training set into v subsets wherever Sj is that the set that has the worth fj for feature F [5]. moreover, Entropy of the feature F is calculated as

$$I(s_1, s_2, s_3, \ldots\ldots s_m) = -\sum_{i=1}^{m} \frac{s_i}{s} \log_2\left(\frac{s_i}{s}\right)$$

Information gained for F is calculated as:

$$E(F) = \sum_{j=1}^{v} \frac{s_{1j} + \cdots + s_{m_j}}{s} * I(s_{1_j}, \ldots, s_{m_j})$$

The dependency magnitude relation [6] is solely calculated therefore Dependency ratio

$$Dependency\ Ratio = \frac{HVF}{TIN} - \frac{OTH}{TON}$$

Where
HVF = highest variety of occurrence variation for a category label in attribute f.
TIN = total variety of occurrences of that category within the dataset
OTH = variety of occurrences for different category labels supported a or a group of Variations.
TON = total variety of instances of category/class labels within the dataset creating OTH.

It helps to pick out options by high worth to low worth and so they're evaluated.

Rule induction is [15] one in all the major varieties of data processing and in unsupervised learning systems it is probably the most common variety of information discovery. Rule induction on a data is a vast responsibility wherever all doable patterns are completely force out of the information.

For the how much the rule to be helpful there must be two things that provide a great information

o Accuracy - however typically is that the rule corrects?
o Coverage - however typically will the rule apply?

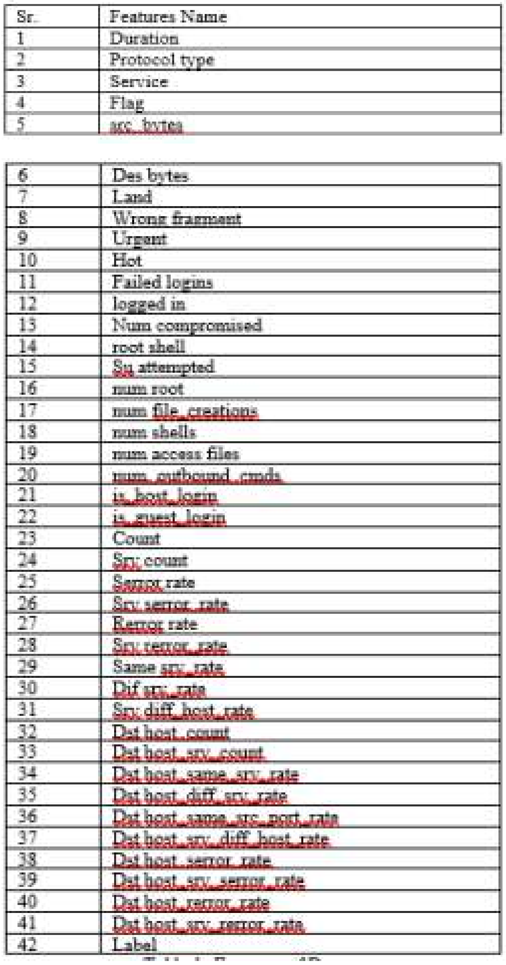
III. NSL-kdd dataset

The dataset employed in the study is NSL-KDD. NSL-KDD could be a dataset counseled to resolve a number of the characteristic issues of the KDD'99 dataset [9]. Although, this new sort of KDD information set still suffers from a number of the issues mentioned by McHugh and won't be an ideal demonstration of current real networks, attributable to the deficiency of public datasets for network-based Intrusion Detection Systems, it is still sensible as a good benchmark dataset to assist researchers to compare completely different intrusion detection ways.

Moreover, the quantity of records within the NSL-KDD train and test set are affordable. This advantage makes it cheap to run the experiments on the whole set while not the requirement to arbitrarily choose a little portion. Therefore, analysis results of various analysis work are reliable and comparable.

Sets	No of records
NSL-KDDTest+	22544
NSL-KDDtrain+	125973

Features of datasets are:



Sr.	Features Name
1	Duration
2	Protocol type
3	Service
4	Flag
5	src_bytes
6	Des bytes
7	Land
8	Wrong fragment
9	Urgent
10	Hot
11	Failed logins
12	logged in
13	Num compromised
14	root shell
15	Su attempted
16	num root
17	num file_creations
18	num shells
19	num access files
20	num_outbound_cmds
21	is_host_login
22	is_guest_login
23	Count
24	Srv count
25	Serror rate
26	Srv serror_rate
27	Rerror rate
28	Srv rerror_rate
29	Same srv_rate
30	Dif srv_rate
31	Srv diff_host_rate
32	Dst host_count
33	Dst host_srv_count
34	Dst host_same_srv_rate
35	Dst host_diff_srv_rate
36	Dst host_same_src_port_rate
37	Dst host_srv_diff_host_rate
38	Dst host_serror_rate
39	Dst host_srv_serror_rate
40	Dst host_rerror_rate
41	Dst host_srv_rerror_rate
42	Label

Table 1- Features of Dataset

IV. Working of Anomaly Based Intrusion Detection System:

Anomaly based refer to the statistical measure of system features. For this NSL-KDD dataset is used.

In general, Anomaly based detection involves following steps:

1. Pre-Processing

It is an important step in data mining process. It converts the raw into understandable format. There it required a training dataset for the learning of IDS. It contains 41 features.

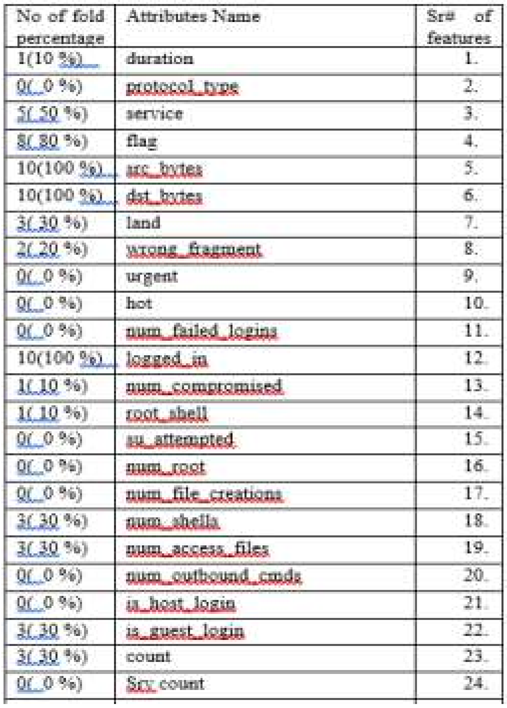
2. Feature Selection

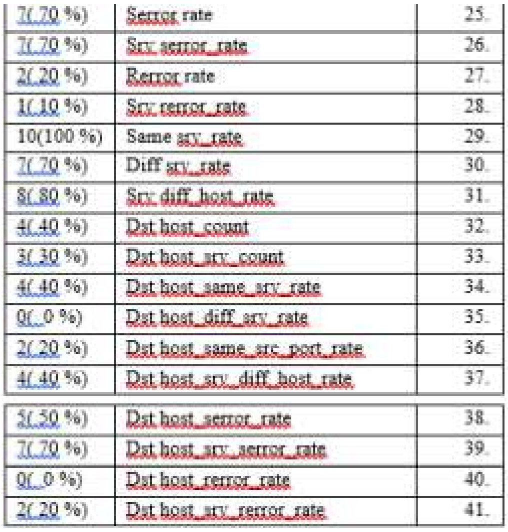
In machine learning it is a procedure of choosing a subset of pertinent features/attributes used to create model. For specific results we need relevant features. Feature selection methods are adopted for following motives

- Over simplification of model so it becomes easy to understand.
- Shorter training time.
- To avoid curse of dimensionality.
- Enhance generalization by reducing over fitting.

Feature are selected using Cfs Subset Evaluation with Genetic Search algorithms. Attributes are selected using percentage folds.

number of folds (%) attribute





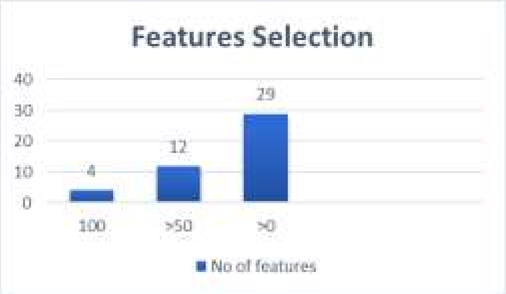
No of fold percentage	Attributes Name	Sr# of features
1(10 %)	duration	1.
0(0 %)	protocol_type	2.
5(50 %)	service	3.
8(80 %)	flag	4.
10(100 %)	src_bytes	5.
10(100 %)	dst_bytes	6.
3(30 %)	land	7.
2(20 %)	wrong_fragment	8.
0(0 %)	urgent	9.
0(0 %)	hot	10.
0(0 %)	num_failed_logins	11.
10(100 %)	logged_in	12.
1(10 %)	num_compromised	13.
1(10 %)	root_shell	14.
0(0 %)	su_attempted	15.
0(0 %)	num_root	16.
0(0 %)	num_file_creations	17.
3(30 %)	num_shells	18.
3(30 %)	num_access_files	19.
0(0 %)	num_outbound_cmds	20.
0(0 %)	is_host_login	21.
3(30 %)	is_guest_login	22.
3(30 %)	count	23.
0(0 %)	Srv count	24.
7(70 %)	Serror rate	25.
7(70 %)	Srv serror_rate	26.
2(20 %)	Rerror rate	27.
1(10 %)	Srv rerror_rate	28.
10(100 %)	Same srv_rate	29.
7(70 %)	Diff srv_rate	30.
8(80 %)	Srv diff_host_rate	31.
4(40 %)	Dst host_count	32.
3(30 %)	Dst host_srv_count	33.
4(40 %)	Dst host_same_srv_rate	34.
0(0 %)	Dst host_diff_srv_rate	35.
2(20 %)	Dst host_same_src_port_rate	36.
4(40 %)	Dst host_srv_diff_host_rate	37.
5(50 %)	Dst host_serror_rate	38.
7(70 %)	Dst host_srv_serror_rate	39.
0(0 %)	Dst host_rerror_rate	40.
2(20 %)	Dst host_srv_rerror_rate	41.

Table 2- Selected Features of Dataset

Features selected are:

No of fold percentage	Features selected	No of features
100	5,6,12,29	4
>50	3,4,5,6,12,25,29,30,31,34,38,39	12
>0	1,3,4,5,6,7,8,12,13,14,18,19,22,23,24, 25,26,27,28,29,30,31,32,33,34,36,37, 38,39,41	29

Table 3. Feature selected on the basis of fold percentage



Graph 1- Features Selected

3. Parameter Optimization

It is a process of choosing optimal parameter for learning algorithms. This measure is known as hyperparameter and resultant model solves problem optimally.

4. Classification

Classification is a process of arrangement of optimized parameters so that useful information can extract in data. It assigns items in a collection to categories or classes. It results in the formation of a model.

In machine learning, modelling SVM's are supervised learning models with linked learning algorithms that examine facts used for classification or regression study.

Models are developed using SMO. Sequential minimal optimization (SMO) is a process for elucidation the quadratic programming (QP) problem that rises during the learning of support vector machines. Following kernels are to be used.

Poly kernel is said to be polynomial kernel. It finds the similarities not only between features but also among there subsets. Polynomial kernel is defined as:

$$K(x, y) = (x^T y + c)^d$$

In this,
x , y = vectors in vector space
c= effect of higher degree order term vs lower degree term. C always greater than 0. If c=0 then kernel is said to be homogenous.

Normalized poly kernel is the refined form of Polynomial kernel. First data is normalized and then processed. It is defined as:

5. Evaluation

Model will be evaluated on the bases of confusion matrix. Multiple scores are measured such as: accuracy, precision, recall, F-measure by performance of 10-fold cross-validation.

V. Result

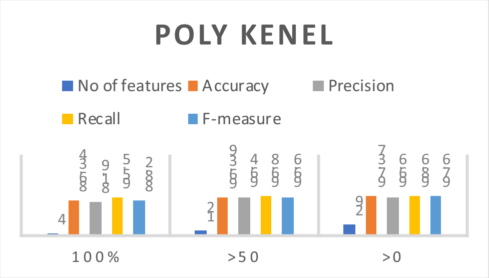
This proposed study of IDS is tested using WEKA (Waikato Environment for knowledge Analysis).

The dataset NSL-KDD has advantages over KDD99 due to Removal of redundant records and affordability for use in experimental purpose. Classification results are based on NSL_KDD 20%. The cross-validation folds are set to 10.

For Poly kernel

No of fold percentage	No of features	Accuracy	Precision	Recall	F-measure
100 %	4	0.8634	0.819	0.955	0.882
>50	12	0.9639	0.964	0.968	0.966
>0	29	0.9737	0.966	0.986	0.976

Table 4- Poly Kenel

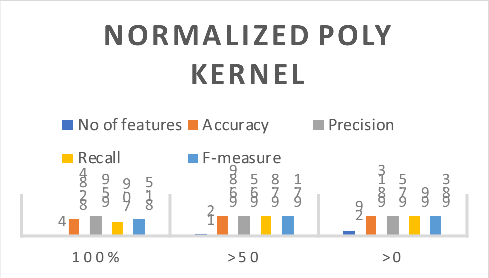


Graph 2. Poly kernel Evaluation results.

For Normalized Kernel

No of fold percentage	No of features	Accuracy	Precision	Recall	F-measure
100 %	4	0.8284	0.959	0.709	0.815
>50	12	0.9689	0.965	0.978	0.971
>0	29	0.9813	0.975	0.99	0.983

Table 5- Normalized Kernel

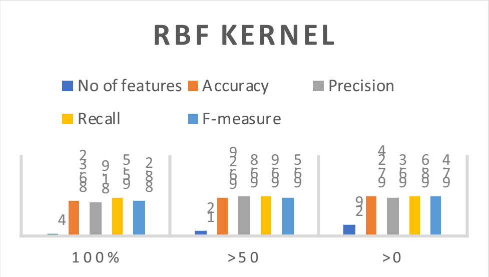


Graph 3- Poly Kernel

For RBF kernel

No of fold percentage	No of features	Accuracy	Precision	Recall	F-measure
100 %	4	0. 8632	0.819	0.955	0.882
>50	12	0.9629	0.968	0.969	0.965
>0	29	0.9724	0.963	0.986	0.974

Table 6- RBF kernel

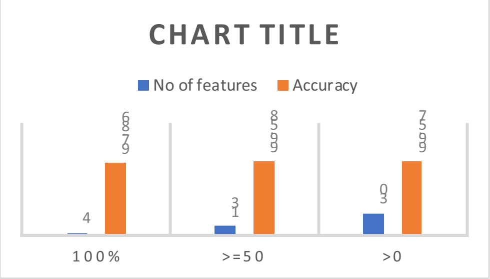


Graph 4- RBF Kernel

For Decision tree (J48)

No of fold percentage	No of features	Accuracy	Precision	Recall	F-measure
100 %	4	0.9786	0.965	0.997	0.98
>=50	13	0.9958	0.995	0.997	0.996
>0	30	0.9957	0.996	0.996	0.996

Table 7- Decision Tree

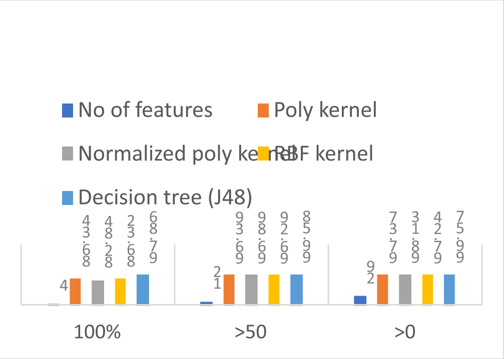


Graph 5- Decision Accuracy

As the no of attributes increases the accuracy increases to some extent. The normalized poly kernel achieved high accuracy then other SMO kernels. This classification evaluation is binary class evaluation.

No of fold percentage	No of features	Poly kernel	Normalized poly kernel	RBF kernel	Decision tree (J48)
100 %	4	86.34	82.84	86.32	97.86
>50	12	96.39	96.89	96.29	99.58
>0	29	97.37	98.13	97.24	99.57

Table 8- Binary class Evaluation



Graph 6- Comparison

VI. Conclusion

IDS is today's need because, it helps the individuals to keep up their confidentiality and integrity. Intrusion that disturbs the security and secrecy of the system, has become major concern for many organizations.

Hence, there's a desire of strong IDS which might observe completely different attack with high attack recognition accuracy. In this, we've got proposed a technique of intrusion detection using SVM which might increase the intrusion detection correctness.

VII. References

[1] Newsweek. (2017). Sony Cyber Attack One of Worst in Corporate History. [online] Available at:

[2] http://www.newsweek.com/sony-cyber-attack-worst-corporate-history-thousands-files-areleaked-289230 [Accessed 22 Dec. 2017].

[3] A. A. Rao "A Java Based Network Intrusion Detection System (IDS)".

[4] M. Tavallaee, E. Bagheri, W. Lu, A. A. Gorbani "A detailed analysis of KDD CUP 99 dataset"

[5] J. McHugh, "Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory," ACM Transactions on Information and System Security, vol. 3, no. 4, pp. 262-294, 2000.

[6] H. G. Kayac?k, A. N. Z. Heywood, M. I. Heywood "Selecting Features for Intrusion Detection: A

[7] Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets"

[8] A. A. Olusola., A. S. Oladele. and D. O. Abosede "Analysis of KDD '99 Intrusion Detection Dataset for Selection of Relevance Features" Proceedings of the World Congress on Engineering and

[9] Computer Science 2010 Vol I WCECS 2010, October 20-22, 2010, San Francisco, USA ISBN: 978988-17012-0-6

[10] Byunghae, C., kyung, W.P. and Jaittyun, S. (2005) Neural Networks Techniques for Host Anomaly Intrusion Detection using Fixed Pattern Transformation in ICCSA. LNCS 3481. 254-263.

[11] Anon, (2017). Saggi e Memorie di storia dell'arte. [online] Available at: http://www.ccianet.org/wpcontent/uploads/2014/04/Cybersecurity.pdf [Accessed 22 Dec. 2017]

[12] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," Submitted to Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), 2009.

[13] J.F Joseph,A. Das,B.C. Seet, (2011) Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA. IEEE Transaction on dependable and securecomputing, Vol. 8, No. 2, MarhApril 2011.

[14] T. Shon, Y. Kim, C. Lee and J. Moon, (2005), A Machine Learning Framework for Network Anomaly Detection using SVM and GA, Proceedings of the 2005 IEEE.

[15] S. Peddabachigari, A. Abraham, C. Grosan, J. Thomas (2005). "Modeling Intrusion Detection Systems using Hybrid Intelligent Systems." Journal of Network and Computer Applications.

[16] R.C. Chen, K.F Cheng and C. F Hsieh (2009),using support vector machine and rough set for network intrusion system.

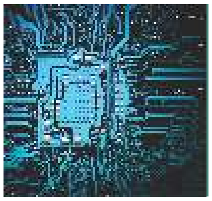
[17] K. T. Khaing (2010),"Recursive Feature Elimination (RFE) and k-Nearest Neighbor (KNN) in SVM."

[18] J. Han and M. Kamber, "Data Mining Concepts and Techniques" Morgan Kaufmann publishers .an imprint of Elsevier, ISBN 978-1-55860-901-3. Indian reprint ISBN 978-81-312-0535-8.

[19] G. P. Dubey, Prof. N. Gupta, R. K. Bhujade "A Novel Approach to Intrusion Detection System using Rough Set Theory and Incremental SVM". International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume 1, Issue 1, March 2011.

[20] A. A.Olusola, A. S. Oladele and D. O. Abosede, "Analysis of KDD '99 Intrusion Detection Dataset for Selection of Relevance Features. Proceedings of the World Congress on Engineering and Computer Science 2010 Vol. I WCECS 2010, October 20-22, 2010, San Francisco, USA.

[21] B. Hur, Asa, Horn, David, Siegelmann, Hava, and Vapnik, Vladimir; "Support vector clustering" (2001) Journal of Machine Learning Research, 2: 125-137.



Tariq et al LGURJCSIT 2019

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

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 3 Issue 3, July - September 2019

Forensics Analysis of Typewriter and Typewritten Documents

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

Abstract:

This article reviews the forensic examination of the typewriter and typewritten documents. The main purpose of examination is to identify the source or origin of the typewritten documents or the link between two typescripts that can be vital to a court of law. Immense application of the typewriter increased the production of fraudulent documents for deceit. Typewritten documents are examined using scientific methods based on class and individual characteristics. These are physical and chemical methods of observation and comparison.

1. Introduction

The beauty of letters written on a paper fascinates the attention of the reader particularly in case of scripts produced by the electronic typewriter in offices and institutions (5). There are various typed and office printed documents which have been produced in different forms for a significant time period. The first typewriter introduced commercially was as long as 1873 which further made the introduction of electronic typewriters. It was followed by the development of computers and printers as advances were made in technology. Large application of these devices in workplace and home increased the production of fraudulent documents greatly over the years (1, 2).

Typewriters are being frequently used to write threatening letters, ransom and extortion notes for criminal objectives. It is mistakenly considered by criminals that the impressions produced make the letters or notes imperceptible. It is not only true in case of pen and paper that leave traces behind about the source of a document but also mechanical devices do so. Typed or copied documents can have distinctive marks often left by typewriters, printers and copy machines. These marks can help the investigator to reveal any alteration in document or the exact machine that produced the document in question. In case of typewriter, the document examiner finds out the make and model number, compares the typed note with a suspect typewriter for the match/mismatch if available (4).

The information obtained from the forensic document examination can be presented to a court of law or to investigating police officer that seeks evidence relevant to the source or origin of questioned document. These information can be conveyed in different ways including obvious typed or printed words or marks in a script and other elusive hidden marks that cannot be seen with naked eyes such as misalignment of characters, microscopic damage to typeface of a typewriter, security or water or pressure marks exerted during typing to hold the paper mechanically in a typewriter or printer. By concentrating on such information, document examiner can determine the forgery. Although there are many cases where evident falsification can immediately be seen such as one of document relevant to attempted suspicious purchase of Uranium in Iraq by the Sadam Hussain Government from Niger where an outdated letterhead was typed with incorrect symbol of Niger presidency (1).

For the admissibility and validation of typewritten evidence to a court of law, proper documentation must be followed for document examination that can be obtained by following country or state's administrative protocols and scientific procedures (1, 2).

2. Typewriting

Typewriters have now been used for more than 100 years with modification in form and manufacture standards. Initial experimentation evolved a standard typebar machine, is still found in use today. Beside these simple and basic models, more advanced and different forms of typewriters have been introduced into the industry of which some have become outdated (2, 3). Typewriters are of two types, a typebar typewriter and the interchangeable single element typewriter. The typebar typewriters have typeface element that is fastened into the machine permanently whereas the interchangeable element typewriters have typeface that is fixed to a type ball, printwheel or thimble that can be exchanged and removed easily from the machine (1, 13). Of such single element typebar machines unfortunately are replaced now by computers which are connected to printers that use daisy-wheel, dot-matrix, and ink-jet or laser technologies. These have provided a variety of means to printed characters on documents involved an in criminal activity. Over and above the content typed can provide evidence of worth to the investigator or court (2, 3 & 4). The document examiners when handling typewritten questioned document, look at typeface and letter spacing of the machine or typebar element as follows(1, 6);

2.1. Typeface

Typewriter manufacturer adopted a general style of typeface for many years following with differences in size and design. Some of makers can have fairly large differences in their products, and some with more understated. Larger differences or variations are of numerals including figures such as 2s with or without straight bases, 3s with curved or flat tops, and 4s either with an open or enclosed triangle. Capital letters are also of larger variations such as M and W are made to type with center either extending to the whole or half of the height of letter. Smaller variations are found in lowercase letters such as the letter a shape at bottom and letter t with cross bar position and length. Each style differs radically like those of shaded characters with differences in line width, making the letter "cubic", rectangular designs with rounded corners rather than circular, and designs similar to cursive handwriting (2, 3 & 8).

All these designs can be moved manually or electrically after mounting on typebars or single elements typically called as "golf ball" or "daisywheels" because of the appearance. They are easily removed and replaced by other styles from a machine. Earlier, these typefaces were designed and made for the machine by the manufacturer but now supplied by specialist producers for typewriter manufacturer. Document examiners should have a collection of typefaces of different machines with classification system that can enable them to find out the style that resembles the typewriting found on the questioned document. The collection is also used for the identification of common origin when comparing typewriting from questioned and known document (2, 3 & 7).

2.2. Letter Spacing

The typewriters involve a mechanism that is used to ensure proper spacing of the letters. Most collective spacing is 10 to 12 letters to an inch of typewriting. Commonly, document examiners do not refer to spacing characters per inch, rather length covered by 100 characters. Therefore, typewriters that print 10 characters to the inch with spacing of 254mm per 100 characters are known as pica machines. While those that print 12 characters to the inch with spacing of 212mm per 100 characters are referred to as elite machines. Other letter spacing used by manual, electrical typebar and single element machines are of 185, 200, 210, 220, 225, 230, 236, 250 and 260 (1, 2 & 3). Proportionate letter spacing is obtained by machines that print letters based on units depending on their width. Typical units are 1/32 or 1/36 of an inch with result nearly similar to pica and elite spacing (2, 3, 7 & 14).

3. Typewriting Identification

Typewritten documents can be examined by using the scientific principles of observation, reasoning with appropriate tests and comparison with known reference standards. The main task of the examiner is to determine the similarities or differences between the two pieces of typescripts. At first, the examiner will identify the source of production of the disputed document either it was typed on a manual typebar machine, single element or produced by ink-jet or laser printer (1). Secondly, the document examiner will identify the manufacturer, model of the machine, a particular machine that was used for alteration and addition to a document other than that was used to type original document, date of the document typed at, and the manufacturer year of the typewriter or in some cases ink or paper (1, 2 & 3).

Typewritten documents can be simplified both as class and individual characteristics. Class characteristics include those of specific make and model number of machine, identified by comparing the typefaces with a reference collection such as Haas Atlas. It is now in the form of computer database program which contains the images of the typefaces with reference to typewriter make, name, manufacturer and serial number (1, 2, 4 &18). While individual characteristics involve the comparison of a questioned document to a particular typewriter machine. Such characteristics are developed through use and misuse of the machine in the form of wear on a character and faulty alignment. Such evidence linked to a specific typewriter was found in USA Unabomb case of 1998 conviction of Theodore J. Kaczynski (1, 20) known as the Unabomber in which a unique characteristic of the letter "u" was identified from the correspondence from Kaczynski that matched the letter "u" on a typewriter key seized during investigation. Individual characteristics can be attributed to a particular machine if it is a typebar machine whereas machine with an interchangeable element, only a text can be associated with a particular element rather than a machine (1, 2, 4 & 9).

The main approach of the document examiner in most of the examination for efficient identification is the comparison of questioned document with known or standard documents rather than those of individual characteristics. This is observed due to a wide variety of characters, word spacing and page styles all on the same printer produced by word processing software (1, 2 & 3). According to Ellen David, many typewriter manufacturers have merged and been producing particular typeface or letter spacing that may not be peculiar to one make and model of machine. Therefore it is possible for a machine to produce different results for various reasons such as changing of the print element in interchangeable element machine while many electronic typewriters can also produce typed documents at two or different spacing (1, 7 & 10).

3.1. Comparison of Typescripts

The comparison of the typescripts is similar to that of handwriting analysis where the two documents are observed side by side, noting each letter, figure, comma, question mark, currency sign, and other considerable characters if they match. Obvious signs of imperfections caused by damage or clear misalignment are noted and compared. The whole depiction of important features, similarities and differences or variable, is evaluated to reach a conclusion. In most of the comparison cases, the variation within the sample is relatively considerable that can be caused due to number of reasons such as looseness in mechanism of the typewriter, quality of ribbon, and features associated to the typist. Features obtained from side by side comparison are sufficient enough to arrive at any proper conclusions (1, 2, 3 & 10).

The significant points for the comparison of the typescript are the overall size and design of the typeface letters and numerals such as capital M and W, the figure 2 with or without straight base, and curve at the ending of letters like f or t (1, 6). Spacing and size of letters were fundamentals of the document examination such as in case of Killian documents dispute where the allegedly forged documents were brought to public notice during the US presidential campaign of George W. Bush in 2004. Two document examiners, Richard Polt and Flounder came to conclusion that was based partly on letter spacing. Results concluded that the Killian documents presented could matched the modern technology based computer and printer using Microsoft Word with default font. These documents were allegedly typed in 1973 when the proportional print typewriters were in use while the original documents were produced on a typewriter with differential spacing and straight apostrophes. The forged documents produced were with proportional spacing and curly apostrophes which can be achieved on a computer (1).

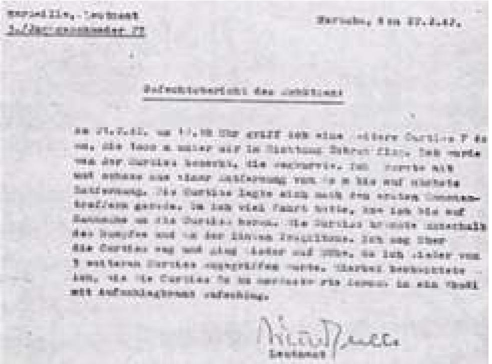
3.2. Image Comparison

At early days, type scripts were examined by comparing them with known or standard typeface specimens printed on cards which were projected onto a large screen and sent to another computer for analysis. A modified examination if necessary, can be performed by using the specialist spacing grids in the form of plastic sheets marked with regular spaced vertical lines especially designed to fit the spacing selected by typewriter manufacturer. The relative position of the grid lines when placed over the typed character, gives a clear clue of accuracy of its alignment (1, 2, 3 & 6).

Other than grids, high resolution imaging software can be used for comparison that produces direct superimposition of images with differences among them. Traditionally, it was done optically by using comparison projectors such as Docucenter 4500 that project the two document images together onto one. The two documents when superposed appear to be one if they are same. The differences in the two documents can be seen by oscillating the images or lightening the documents with different colors such as red and green. Even smaller differences produced from different typewriters can also be detected by contrasting smaller variations found in the output of one machine such as alignment, wear or damage (2, 3).

3.3. Typewriting Dating

A typed document can be dated by using features which are present in one sample but absent in other. Most of the time, a document is questioned to establish certain time period when it was typed such as combat report in 1942 by Lieutenant Marseille, a German fighter pilot during world war II known as "Star of Africa" on the battlefields of northern Africa. The authentic report dated 27.2.1942 has been written on a German typewriter likely Triumph having typeface amongst the old type models with closed middle element "M and W" as shown in



Marseille, Leutnant
3./Jagdgeschwader 27

Martuba, den 27.2.42.

Gefechtsbericht des Schützen

[illegible]

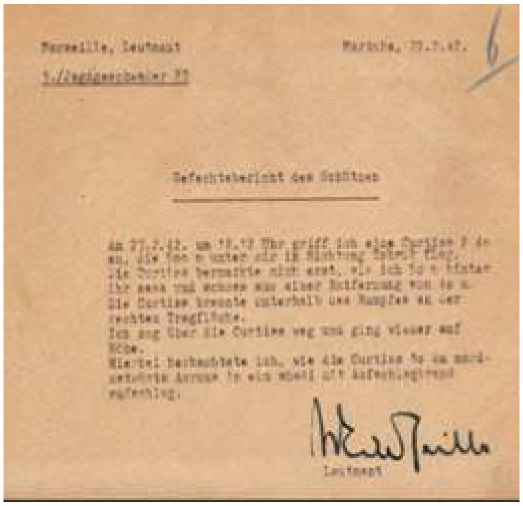
Leutnant

Figure 1: Authentic report by Lieutenant Marseille from 1942 (19).

This typewriter was manufactured between 1930 and 1940, and equipped with the Pica type font "Ro 1"whose earlier version started in 1964 (2, 3 & 19). The type font produced by "Ransmayer & Rodrian" in Berlin, contains following new types;

- " M W " characters with shortened middle element was produced in 1951.
- " f " character was produced with shortened horizontal middle line in 1957.
- " r " character was produced with horizontal line lengthened on the right side in 1961.
- " i " character was produced with shortened horizontal headline in 1964.

Therefore, the results obtained from the examination of falsified or questioned combat report are contrary to the date 27.2.1942 as it contained the characteristic features which were not introduced in typed year of the report as shown in following figure (19);



Marseille, Leutnant
3./Jagdgeschwader 27

Martuba, 27.2.42.

6

Gefechtsbericht des Schützen

Am 27.2.42. um 11.17 Uhr griff ich eine Curtiss P 40 an, die 500 m unter mir in Richtung Tobruk flog. Die Curtiss bemerkte mich erst, als ich 50 m hinter ihr sass und schoss aus einer Entfernung von 50 m. Die Curtiss brannte unterhalb des Rumpfes an der rechten Tragfläche.
Ich zog über die Curtiss weg und ging wieder auf Höhe.
Hierbei beobachtete ich, wie die Curtiss [illegible] Acroma in ein Wadi mit Aufschlagbrand aufschlug.

Leutnant

Figure 2: Falsified combat report Lieutenant Marseille from 1942 (19).

The samples of the output of a machine produced at a regular interval, can be examined by discovering the old and new occurrence of the damaged characters with changing pattern of faults. Like from noting the fault found in a certain document but not another then the time period during which fault existed can be discovered by the analysis of sequence of dated documents. Features other than fault or damage to a typewriter, after repairing can also be used to give information about the date of typing (2, 3 & 11).

4. Linking Typewriting to a Typewriter

Substantial evidence other than deduced from typescript, is the actual machine identification that was used to type it. It is used as a significant evidence in the investigation of a trail in civil or criminal court. It is not always the case to compare the typewriting with typewriting, instead quick comparison of typescript with typeface on the machine is made. Exclusion or inclusion of the typewriter or typeface element is made if clear differences are found after comparison such as a round top 3 on a document and flat-topped 3 on the machine. Sample is taken out for more detailed comparison if such difference is not seen (2, 3).

During the comparison of typescript with typewriter, the typeface in the typebar machine and the typewriter its self are to be regarded as one such as in single element models either type ball or type wheel, the typed material has both a machine and an element in a combination of two. It is not found in practice for the typewriters to be set to a standard of absolute perfection by limiting the value of results obtained from the comparison of their products. Therefore, variations can be found in the typebar machines, type elements and mechanism of typewriters using those elements (2, 3 & 7). Difference found after maintaining quality control is small to be of forensic value. One source within forensic science, produces variability when compared. If such variation of significance found between the sources, no key comparison can be placed. Small variations found between typewritings produced from different machines are no larger than those from one machine. Features that develop during lifetime of a typewriter such as fault from wear or damage, are of greater significance as these occur randomly for the most part. These features are different for different typewriters as follow (2, 3 & 9);

4.1. Mechanical Faults

Visible imperfections in the typescript can occur in a number of ways such as damage to individual characters and misalignment of certain characters. The damage can be in the form of bent or chipping of the metal type due to the depression of two keys of the typebar machine together and collision between the two components, showing results in subsequent printed impressions. Type ball machines have less dominant damage due to small molding defects during manufacture that can be appeared on a typewritten page. However, print wheel characters are also susceptible to mechanical fault. The damage in the metal type of the type bar machine remains unchanged permanently while the damage in the plastic material of type wheel elements deteriorates quickly once the coating surface has been broken (2, 3 & 7).

Misalignment of certain characters can occur during manufacturing of metal type pieces bearing characters which are fused onto the ends of the type bars. The consistency applied for affixing them is not always perfect, resulting in small differences in the relative positions of the printed characters. The twist or bent in a type bar, will result in misplaced impressions of the characters diverging upward, downward, left or right, at an angel or combination of two or more from their ideal positions. Depending on the distortion of the type bar, twisting can result in an uneven image by printing character more heavily on one side than other or at top or bottom. Looseness can occur during mechanical process which can produce characters with aligned or out of their positions. No constant misalignment of a single character can be revealed if there is great variation in the relative positions of all the keys (2, 3 & 10).

The rotating mechanism in the type ball machines, can print characters out of adjustments due to wear or damage resulting in misplacement of characters on the row or column. As it is a mechanical fault of the machine so it will be present though the type ball is changed. Damage to the base of the element which is to position it mechanically, can also misplace a vertical row of characters. As this fault is in element then it can be disappeared if the element is changed and when the same element is placed in another machine, same defect will be appeared again (2, 3 & 7).

Print wheel machines unlike conventional type bar machines, also give displacement of the printed characters but with one character position only due to the distortion to the type bar of the wheel. The spacing of daisy wheel machines is very consistent varying between machines. The causes of variation could be both in the machines and element (2, 7 & 15).

4.2. Other Faults

There are various other reasons that can produce less than imperfect results from the typewrites as follow;

- Dirty characters can misprint a letter such as an unlinked circle printed as a solid one. This can be corrected easily as it is a temporary condition.
- Mechanism of the shift key can move too far or not that results in capital letters and position higher or lower than they should be.
- Loose paper holding mechanism may result into unevenly separated lines of the typescripts.
- Disposition of the platen or flat metal plate can cause all the characters to print heavily at the top or bottom.
- Spacing mechanism of the platen sometimes can misfire or backfire by giving unrequired gap between characters or crowding of two letters on each other.
- In electric type bar machines, the pressure adjustment for each character is different so printing constantly more heavily or lightly.
- Defective alignment of the ribbon in the typewriter can cut off the top or bottom of the characters. Similarly, mixture of black and red typescript is print out if dual color ribbon is used (2, 3 & 8).

5. Sample Collection

The role of forensic investigator in comparison of typescript is either to identify the source or origin of a document or the link between the two or more typewritten documents. In most of the cases, the typewriter acquisition as an evidence is a lead for various reasons such as discovering of characters which appear on the typescript but not in the typeface of the typewriter. This points out a possible source if the key of relative character is not replaced or it is damaged that can be seen upon examination of the machine (2, 3). Recovery of ribbon, correcting tapes and electronic memories as evidence from the machine can be dealt later for the comparison to the typewriter rather than samples from it. Extra element is taken with the machine if it is acquisition of single element machine (2, 3 & 9). When it is not possible to remove the machine, then samples should be taken either by using a ribbon or a piece of carbon paper with control of ribbon in template position. It may provide better results if the carbon paper is new or ribbon is in good condition. In some cases, it can produce so thick lines limiting the details if heavily inked fabric ribbon is substituted but satisfactory for carbon paper as it gives clearer outline of the characters (2, 3 & 8). Samples of entire keyboard both with and without operation of shift key, should be taken to record all the features of the characters including upper lowercase letters, figures, and punctuation marks etc. While taking the samples, the question passage should be typed four to five times in same layout as that of being compared so that the output consistency can be tested. Machines collected, should be identified with details such as make, model and serial number. Possible valuable evidence can be obtained from the known materials that have been typed on the same machine being questioned when there has been a change over a period. When the date of the typewritten document is questioned, the letters typed on or around, before and after this date are significant. If a typewritten document has more than one possible sources, document examiner may make a primary examination of obvious features such as center of capital Ms and Ws, straight or round tape of figure 3 and open or close end of figure 4. The typeface in the typewriter machines as compared to the modern machines, is fixed, therefore a mismatch likely indicates that different machines or different elements have been used (2, 3 & 9).

6. Other Examination Process

There are various means of connecting a typescript with a typewriter other than comparison of typescript. Most significant of these are the examination of the ribbon, ink analysis, identification of erasures or addition and who typed it as explained following (2, 3);

6.1. Ribbon-Composition Identification

Identification and examination of typewriter ribbon is essential for a typewritten document if suspected as altered or added. These are temporary equipment which do not need identical replacement therefore stating that difference in the ink of the ribbon in a machine and on the paper, does not exclude the typewriter machine from the one used to type that particular typescript. As the ribbons are made in large numbers to a controlled standards so it is of little worth to compare the ink or plastic material on the typewritten paper with other document or in a ribbon of a typewriter. However this is useful to compare two typescripts that might have been typed approximately at the same time on the same machine (2, 22).

There are two basic types of typewriter ribbon, the fabric and carbon ribbon. The fabric ribbon uses ink and does not retain legible image of the prepared text whereas the carbon ribbon can retain readable text by using carbon film. Both of the types can be distinguished clearly under low-power magnification. Other types are correction ribbon including lift off and cover up which also retain images that can be compared with text and carbon ribbons (21, 22 & 23).

Carbon ribbons are produced by a number of different manufacturer that can be distinguished on paper by microscope. Comparison of paper fiber-transfer is possible by using comparison microscope as the polythene backing on carbon ribbon with low density can assume the imprint of fibers in the paper. Scanning electron microscope (SEM) is used for the sequencing of typing stroke order determination of the fabric ribbons and deposits from the carbon ribbon. In case of typing which crosses a signature made with ball point pen, can determine the stroke order from the carbon ribbons. Scanning electron microscope analysis gives clear separation of different types but being partially destructive method as piece of questioned document is removed, is a drawback though recent development made it possible to enlarge specimen chamber (12, 22).

6.2. Ink Identification

Ink and paper analysis sometimes can determine the age of the production of typed document by working on dating of inks production and composition. Document examiners try to determine as much information as possible from typescript by using nondestructive techniques of observation and comparison with naked eye, magnifying glass and optical techniques such as Video Spectral Comparator (VSC), Ultraviolet light UV and Infrared IR. However in some cases, these methods become insufficient for the identification of the ink used to type the questioned document so therefore chemical methods are applied which can cause partial destruction of the document such as Thin Layer Chromatography (TLC), High Performance Liquid Chromatography (HPLC), Capillary Electrophoresis (CE) and Gas Chromatography. Ink libraries are being developed yet with limited samples (5, 17 & 24).

6.3. Typewriting Erasures Identification

Typewriting documents can be subjected to alteration by using special correcting fluids which is normally used for the correction of typing mistakes. This can be identified by using strong lighting source directly on the page or through the page from the back side as the paper of the typed document is likely to be thinner than the layer of dried correcting fluid. Suitable inert volatile liquid is used that soaks into the paper and correcting fluid by making it more translucent and does not affect the typewriting. As the solvent is volatile so the examination and photograph must be made quickly. The procedure can be repeated as it does not affect the paper permanently (2, 4 & 11).

Mechanical means are also used for erasing the typewriting using sharp blade for scraping the surface or hard rubber to erase. Oblique lights are used for identification of what was erased by examining indentations and traces of ink remaining. Infrared (IR) light is used for identification of erased typewriting where an invisible component of the ink that penetrates more deeply into the paper, may luminesces in this spectrum. However, typewriting produced with carbon ribbon adhere only to the surface of the paper which can be easily lifted off with an inbuilt adhesive tape and their remained indentation can identify the erased typing (2, 12 & 16).

6.4. Added Typescript Identification

Alignment consistency testing can determine the timing of the two pieces of typewriting on the same document or paper. It is assumed for the cases where the piece of typewriting on a document was not present when it was seen first or when it was signed or added later for the deceiving objectives. For the purpose to add an extra typewriting to an already typed document, it has to be replaced in the machine with accurate alignment both horizontally and vertically. It is not easy as it sounds to ensure the exact alignment of the added portion in a correct position.

Gird method is helpful for the examination of this typewritten evidence. Grid covers the main body of the typescript so that each character on a line is in position in its box and centrally placed. Only alternate lines will be positioned accurately if half spacing is applied while the other lines will fall into place. This method shows either characters fall into the correct place or not in the grid. Any crease or fold in the typewritten document can cause problems as it reduces the length of the paper sheet and appearance out of alignment. It should be considered before making any conclusion (2, 3 & 7).

6.5. Typist Identification

There are different typing methods developed by technical changes in fashion or styles, apply individuality to the basic pattern. Therefore, a letter can be typed in number of ways causing variations such as spacing of lines, size of the margins, and indentation depth at the beginning of paragraph, number of spaces after commas or periods, and use of capital letters (2, 3 & 10). All of these variables are consistent for one typist. Typewriting in questioned made with manual machine, can give the touch of the typist which is an indication of who typed it. It is helpful in exceptional cases where heavy pressure is applied even though sometimes the periods and letters are punched out of the paper. All of these factors are not unique and can be relevant to the operator how he/she was taught. Like a person with no proper training of laying out a letter is unable to create a well-produced piece of typescript as compared to a professional typist (2, 3).

The common authorship of two pieces of typewriting can be obtained by the identification of the errors made in them such as infrequent typist may have problem with figure 1 who is quite likely to use capital I. This evidence can be sufficient in a limited population where to pinpoint only one or two people for a particular style of typing. It is also possible for a person to mask his ability by copying errors of another person therefore considering all possibilities. Identification of typist can be made by the comparison of known and questioned document using previously typed material by the suspect (2, 3 & 10).

7. Conclusion

Typewritten document is one of the class of questioned document examination that always has been needing solution. Careful observation and comparison is made for the examination of typescripts produced on a typewriter. The charge of document examiners is to discover either two or more pieces of the typescripts are similar or there are clear differences. If they have differences then it is indication of two different source and if these characters are found to be similar in two typescripts, then they are concluded to have a common source of production or one machine has been used. Class and individual characteristics are used for the comparison of typescripts and a typewriting machine. Scientific methods of examination by physical or chemical means are performed for comparisons. Some of these methods can be destructive but advances in science reduced the chances. Careful observation must be made before reaching any conclusion.

8. References

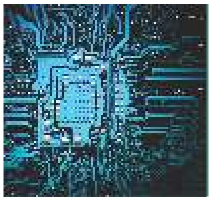
1. D. Catalin, "Forensic Examination of Typewritten and Office Printed Document," International Journal of Criminal Investigation, vol. 1(1), pp. 11-16.
2. E. David, "Scientific Examination of Documents," Taylor & Francis Group, 4th Ed, 2018.
3. E. David, "Scientific Examination of Documents," Taylor & Francis Group, 2nd Ed, 2003.
4. P.L. Douglas, "Forensic Document Examines Dissect Typewriters & Photocopiers," Dummies; A Wiley Brand. Available: https://www.dummies.com/education/science/forensics/how-forensics-document-examines-dissect-typewriters-and-photocopiers/
5. K.M. Varshney et al., "Ink analysis from typed script of electronic typewriters by high performance thin layer chromatography," Forensic Science International, 72th Ed, pp. 107-115, 1995.
6. E.B. Peter, "Image Processing of Forensic Documents," University of Mannheim, Germany, 1995.
7. O. Hilton, "Problems in Identifying Work

from Print Wheel Typewriters," Forensic Science International, 30th Ed, pp. 53-63, 1986.

8. O. Hilton, "Identification of Typewriting. Problems Encountered with Shaded and Proportional Spacing Type Faces," The Journal of Criminal Law, Criminology, and Police Science, Vol. 48(2), pp. 219-223, 1957.
9. W. Colleen, "Hand Book of Forensic Services," Federal Bureau of Investigation, 2003.
10. O. Hilton, "The Influence of Variation of Typewriting Identification," J. Crim. L. & Criminology, vol. 50, pp. 1959-1960, 1957.
11. O. Hilton, "The Complexities of Identifying the Modern Typewriter," Journal of Forensic Sciences, Vol. 17(4), pp. 579-585, 1972.
12. W.L. Leaver, "Introduction to Forensic Document Examination," The Forensic Laboratory Handbook: Procedures and Practice, pp. 223-248.
13. Borashin, "Typewriter Forensic Identification," New Modes of Reading and Writing, 2011. Available: https://newmodes2011.wordpress.com/2011/02/03/typewriter-forensic-identification/
14. O. Hilton, "Test Plate for Proportional Spacing Typewriter Examination," 47 J. Crim. L. Criminology & Police Sci., vol. 47(2), pp.1956-1957, 1956.
15. M.A. Lamar, "An Analysis of the Identification Value of Defects in IBM Selectric® Typewriters," Journal of Forensic Sciences, Vol. 29(2), pp. 624-627, 1984.
16. J.A. Lewis, "Forensic Document Examination; Fundamentals and Current Trends," Academic Press is an imprint of Elsevier, 2014.
17. L.C. Bate et al, "Application of Activation Analysis to Forensic Science: Physical Evidence," International Journal of Applied Radiation and Isotopes," vol. 14, pp. 549-556, 1963.
18. D.A. Crown, "Class Characteristics of Foreign Typewriters and Typefaces," J. Crim. L. Criminology & Police Sci., vol. 59(2), pp. 298-323, 1968.
19. Bernhard Haas, "Typewriting Cases," Forensic Document Examiner, Winnenden, Germany, 2019. Available: http://schriftexperte.de/en/cases/
20. E.H. Dorothy-Anne, "Handwriting, Typewriting, Shoeprints, and Tire Treads,"

FBI Laboratory's questioned Documents Unit, vol. 3(2), 2011. Available: https://archives.fbi.gov/archives/aboutus/lab/forensicsciencecommunications/fsc/april2001/ held.htm

21. M. Jacques and P. Roman, "The Examination of Typewriter Correctable Carbon Film Ribbons," Forensic Science International, vol. 26, pp. 71-80, 1984.
22. F. Gerhart, "Methods of Associating Typewriter Ribbons and Correcting Tapes with a Questioned Text," Journal of Forensic Sciences, Vol. 34(5), pp. 1183-1195, 1989.
23. R. Hunton and J. Puckett, "Restoring Texts of Typewriter Ribbons: A Reliability Study of the RAW-1 Ribbon Analysis Workstation," Journal of Forensic Sciences, Vol. 39(1), pp. 21-27, 1994.
24. N. Sarah, "Typewriter Inks: An Annotated Bibliography," Technology and Structure of Records Materials, 2006.



Malik LGURJCSIT 2019

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

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 3 Issue 3, July - September 2019

Cyber Security - Incident Response and Management

Muhammad Shairoze Malik
shairozemalik@lgu.edu.pk
Lahore Garrison University

Abstract:

Today, Information Technology has bought a lot of benefits for the mankind but it has also made us susceptible to failures and attacks as well. This article discusses the increasing complexity of cyber-security threats and capabilities of information security teams in applying controls required to effectively respond to threats. In this article, the main stages of managing information security incidents and events are discussed, designed to help create an effective response process to security incidents and as a result to reduce losses and quickly restore performance in dynamically changing IT infrastructure and threat landscape.

Keywords: Cybersecurity Incident Response, Cyber Threats, Incident Logging, Incident Management, Cyber-Security Warning Systems, Organization Security.

1. Introduction

As organizations become more and more technology dependent, they become more vulnerable to information security attacks. The situation can be summarized by following quotes:

"It is inescapable at some phase that associations will endure a data security incident. Such an incident may bring about numerous negative effects, for example, loss of organization reputation and client confidence, legal issues, lost efficiency and direct monetary loss. [1]"

It is not economically feasible for an organization to implement unbreakable security measures to protect their assets [2], so they need to prepare for a response in case of a security attack on their ICT infrastructure.

An information security incident can be defined as;

"An identified occurrence of a system, service or network state pointing to a possible breach in information security, policy or failure of controls or a previously unknown situation that may be related to the security, and has a significant probability of compromising business operations and threatening information security. [3]"

Reducing the potential risks of violation of the availability, integrity and confidentiality of information resources due to information security incidents can be achieved by their timely detection in conjunction with the response. Moreover, responding to information security incidents is often less expensive and more effective than investigating them. An information security incident can lead to malfunctioning of systems, services, networks and as a result prolonged unavailability of critical business processes, loss / modification of the transmitted or stored information without the possibility of its recovery, reputational risks of the owner of the information resources and contractors.

A practical approach to building a reference process is described in detail in following international standards:

ü ISO / IEC 27001: 2013 Information Security Management System.

A standard that contains both recommendations for the construction, implementation, use and support of the information security management system as a whole, and approaches to managing information security incidents [4].

ü NIST SP 800-61 Computer Security Incident Handling Guide.
A comprehensive security incident handling guide that describes various approaches to incident response and handling [5].

ü CMU / SEI-2005-TR-015 Defining incident management process for CISRT.
A document for evaluating the performance of the CISRT (Critical Incident Stress Response Team) unit that provides prevention, processing and response to information security incidents [6].

ü ISO / IEC TR 18044: 2004 Information Security Incident Management.

The document established recommendations for information security incident management regarding planning, operation, analysis and improvement of the process [7].

ü NIST SP 800-83 Guide to Malware Incident Prevention and Handling.
A guide to preventing and handling malware incidents involving workstations and laptop infections [8].

ü NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response.
A guide to investigative techniques for responding to identified incidents [9].

ü ISO / IEC 27035-2:2019 Guidelines to Plan and Prepare for Incident Response.
It points to the development of guidelines to enhance an organization's actual readiness to respond to a security incident [10].
These two can be regarded as the main guidelines related to incident management;

ü ISO-IEC 27035 [10]

ü NIST Special Publication 800-61 [5]

They offer a structured approach to planning and preparing for incident response, what to do when incident strikes and how to extract lessons afterwards.

SANS [11] and ENISA [12] also provided

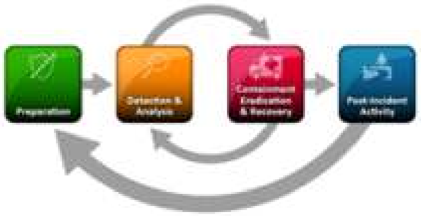


Fig 1: NIST-SP 800-61 r2 Incident-Response-Life-Cycle

In general case, the life cycle of managing events and incidents of information security is usually divided into following stages:

1. Plan & Prepare
2. Detection & Reporting
3. Assessment & Containment
4. Incident Response
5. Lessons learnt

Next, we consider each stage of the information security incident and event management process in more detail.

2. Plan & Prepare

Planning and preparing is presumably the most significant step in incident response. An association that is not set up to deal with an incident is more likely to fail in detecting and in turn responding to an information security incident in their vicinity. A main recommendation is the establishment of a security response team based on the experiences at LRZ-CSIRT [13]. The planning phase includes the formation of an incident response program including procedures, policies, compliance and governance documents, etc. For effective execution, the socializing of the different aspects of this program is also required. The studies and experiences provided by Werlinger et al. [14], Metzger et al. [13], Ahmad et al. [15], hove and Tarnes [16], gives an overview of many technical measures that can be taken to prepare for incident detection and response. They can be summarized in following steps:

- Organize a round the clock call-tree among

all departments in the organization, so a breach can be communicated as soon as possible.
- Implement IDS / IPS and other monitoring systems.
- Make sure that incident response team is fully equipped with required equipment, access, software, chain of custody forms, secure storage and a control room.
- Train incident responders with the organization's IT infrastructure including installed software, policies, protocols & permitted ports, etc.
- Use a single email address with shared mailbox vs. a distributed list for better achieving. The access to the mailbox should only be for the incident response team members.
- Organize internal and external training sessions for the staff members.
- Run mock realistic breach scenarios to test the detection tools and response process.

2.1 Detection & Reporting

The purpose of detecting computer attacks is to timely respond to incidents related to them in order to further take measures to eliminate the consequences of such incidents.

The timely detection of a security breach is a major problem in implementing security measures. An observation made by researcher Koivunen [17] was that in majority of the incidents studied none to the victims discovered the security breach own their own, but they had to rely on automated tools for timely detection of breaches.

In the course of activities to detect computer attacks, the following processes should be implemented:
- Monitoring the implementation of uniform operating rules for the detection of computer attacks on information resources.
- Control over centralized updating of decision rule databases for computer attack detection tools.
- Detection of previously unknown computer attacks at the network level, including the use of network traffic analysis tools on communication channels.
- Detection of previously unknown computer attacks conducted using malicious software, including using methods of behavioral analysis of software.
- Develop decisive rules for unknown computer attacks.

2.2 Assessment & Containment

The analysis of an incident can be done in two stages:

i. Initial Incident Analysis
ii. Comprehensive Incident Analysis.

The objective of the initial analysis of the incident is the establishment of the circumstances and possible consequences of the incident.

The objective of the comprehensive incident analysis is the point out the causes of the incident and the actual consequences to the infrastructure.

The purpose of the analysis of the data on security events is to identify information security incidents, including those related to previously unknown computer attacks, as well as incidents related to the insufficient effectiveness of the measures taken to protect information.

Information is collected from results of all information protection tools used in accordance with the security policies adopted in information systems. These are sources such as:

- Attack detection tools and firewalls used on communication channels through which information resources are accessed.
- Network traffic analysis tools using data mining techniques.
- Detection tools for attacks and firewalls used in local area networks in which the components of information resources are located.
- Software Behavioral Analysis Tools.

The collection of information from these sources is recommended in an automated mode. In this case, the rules for normalizing information security events are implemented. Information about security events is compared with information about the vulnerabilities of components of information resources to predict the possible actions of an attacker during computer attacks.

When analyzing data about security events using automated tools, correlation rules are applied [14]. Correlation rules are determined by responsible employees or, a third party security firm, taking into account information obtained during the inventory and identification of vulnerabilities in information resources. In the process of functioning, constant work is carried out to adapt the sources of data on security events with the means of their analysis to increase the efficiency of detection of computer attacks, as well as work on formation of new correlation rules and signatures.

It is suggested that incidents be recorded utilizing computerized methods for accounting and processing dependent on markers that influence the level of negative effect of an incident, since the manual procedure of incident handling is ineffective as they prompt a high asset utilization of work force and altogether increase the reaction time to information security incidents of high criticality.

It is particularly challenging to handle an incident when IT operations are outsourced among several suppliers. In such cases, priority handling to incidents becomes a major issue, i.e. "what does it mean for the customer, when a server is down? (de Souza et al., 2011) [18].

2.3 Incident Response

Different organizations have different approaches to handle an incident. For some, it is important that the incident is handled properly and its future occurrence must be controlled or any other similar vulnerability in system should be rectified. While for others, it is important to minimize the damage of business operations by fast recovering of systems using temporary means if necessary [16].

Software and hardware documentation were identified as the most important information for dealing with incidents, Kurowski and Frings (2011) [19].

An organization's information security incident response process can be divide into following stages:

- Fixing the state and analysis of objects of information resources involved in the incident.
- Coordination of activities to stop the impact of computer attacks, the conduct of which caused the occurrence of the incident.
- Fixation and analysis of network traffic circulating in the information resource involved in the incident.
- Determining the causes of the incident and its possible consequences for the information resource.
- Localization of the incident.
- Collection of information for the subsequent establishment of the causes of the incident.
- Planning for incident response.
- Disaster management.
- Control of liquidation of consequences.
- Formation of recommendations for improving regulatory documents ensuring security of information resources.

2.4 Lessons Learnt

An incident is deemed completed after all measures have been taken, provided that the establishment of the causes of the incident has shown the adequacy of the measures taken. Analysis of the results of the elimination of the consequences of the incident includes and assessment of the following aspects:

- Damage caused to the information resource and its owner as a result of the incident.
- Shortcomings in ensuring the security of information that did not allow to prevent the incident.
- Timeliness of incident detection.
- Personnel actions in localizing the incident and liquidating its consequences.
- The timing of the aftermath of the incident.
- When assessing the harm caused to an information resource and its owner as a result of an incident, the following are taken into account:
- Personnel labor and other costs associated with the elimination of consequences.
- Damage caused to the public interests and interests of the owner of the information resource, including those related to violation of confidentiality.
- When assessing deficiencies in ensuring information security, the following are determined:
- Regulatory requirements, non-compliance, lack of effectiveness which made the incident possible.
- Additional protective measures that are not

mandatory in accordance with the current regulatory documents, but which could prevent the incident.

Conclusion

Depending on the organization's activities, methodological recommendations of international standards, which describe a fairly complete set of measures necessary to build the process of managing incident and information security events, can be the optimal choice of application. Regardless of which methodology is selected or developed for managing incidents and information security events, it should:

- Take into account the needs of the organization.
- Be as automated as possible.
- Run non-stop (24 hours a day, 7 days a week).
- Be applicable to the organization, taking into account the corporate culture and available resources.
- Reflect in the form of a model the real landscape of information security threats relevant to the organization.
- Be transparent to all interested parties, including company management, representatives of regulators, external and internal auditors.

References

[1] Ahmad A, Hadgkiss J, Ruighaver AB. Incident teams - challenges in supporting the organizational security function. Comput Secur 2012;31(5):643-52

[2] Anderson R, Barton C, Bohme R, Clayton R, Eeten M, Levi M, et al. Measuring the cost of cybercrime. In: 11th Workshop on the Economics of Information Security (WEIS'12); 2012.

[3] ISO/IEC 27035-1:2016 Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management. Retrieved on October 2, 2019, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-1:ed-1:v1:en

[4] ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements. Retrieved October 1, 2019, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

[5] Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone - "Computer Security Incident Handling Guide". Retrieved on October 1, 2019, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[6] Alberts. Christopher, Dorofee. Audrey, Killcrece. Georgia, Ruefle. Robin, and Zajicek. Mark, "Defining Incident Management Processes for CSIRTs: A Work in Progress," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, Technical Report CMU/SEI-2004-TR-015, 2004. Retrieved on October 1, 2019, from http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=7153

[7] Hamidovic, Haris. (2011). An Introduction to Information Security Incident Management Based on ISO/IEC TR 18044:2004. VI. Retrieved on October 1, 2019, from https://www.researchgate.net/publication/254864149_An_Introduction_to_Information_Security_Incident_Management_Based_on_ISOIEC_TR_180442004

[8] Murugian Souppaya, Karen Scarfone "Guide to Malware Incident Prevention and Handling for Desktops and Laptops" revision 1, 2013. Retrieved on October 1, 2019, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf

[9] Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang "Guide to Integrating Forensic Techniques into Incident Response", 2006. Retrieved on October 1, 2019, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

[10] ISO/IEC 27035-2:2016 Information technology - Security techniques - Information security incident management

- Part 2: Guidelines to plan and prepare for incident response. Retrieved on October 2, 2019, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-2:ed-1:v1:en

[11] Kral P. The incident handlers handbook. SANS Institute; 2011. Retrieved on October 2, 2019, from https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

[12] ENISA, Good practice guide for incident management; 2010. Retrieved on October 2, 2019, from https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management/at_download/fullReport

[13] Metzger S, Hommel W, Reiser H. Integrated security incident management e concepts and real-world experiences. In: Sixth International Conference on IT Security Incident Management and IT Forensics (IMF); 2011. pp. 107-21.

[14] Werlinger R, Muldner K, Hawkey K, Beznosov K. Preparation, detection, and analysis: the diagnostic work of IT security incident response. Inf Manag Comput Secur 2010;18(1):26-42.

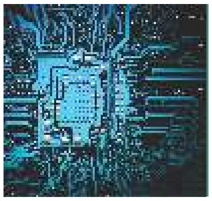
[15] Ahmad A, Hadgkiss J, Ruighaver AB. Incident response teams - challenges in supporting the organizational security function. Comput Secur 2012;31(5):643 - 52.

[16] Hove C, Tårnes M. Information security incident management: an empirical study of current practice. Norwegian University of Science and Technology; 2013.

[17] Koivunen E. Why wasn't I notified: information security incident reporting demystified. In: 15th Nordic Conference in Secure IT Systems (NordSec 2010); 2010.

[18] de Souza CRB, Pinhanez CS, Cavalcante VF. Information needs of system administrators in information technology service factories. In: Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology (CHIMIT '11). New York, NY, USA: ACM; 2011. p. 10. Retrieved on October 3, 2019 from https://dlnext.acm.org/doi/abs/10.1145/2076444.2076447.

[19] Kurowski S, Frings S. Computational documentation of IT incidents as support for forensic operations. In: IT Security Incident Management and IT Forensics (IMF), 2011 Sixth International Conference on; 2011. pp. 37- 47.



Zahra et al. LGURJCSIT 2019

LGU International Journal for
Electronic Crime Investigation

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

Research Article Vol. 3 Issue 3, July - September 2019

Effects of Emotions in Cognitive Based Game

Syeda Binish Zahra[1], Syed Muhammad Shabih-ul Hassan[2],
binishzahra@lgu.edu.pk[1], shabih@pac.edu.pk[2],
Department of Computer Science, Lahore Garrison University (LGU)[1]
Professional Academy of Commerce[2]

Abstract:

Recognition of emotion has been done through different perspectives and is useful in many domains of Human Computer Interaction (HCI), especially in intelligent systems, interactive robots, web applications interaction, and to elaborate social media. Our aim is to design a system which encapsulates the behavior's set into roles which helps other developers in wrap behaviors into segments that can diverse dynamically, based on player moves. Games utilize contextual data about players and their environment to explore new means of interactions and enhance game experience. Cognitive science plays an important role in the performance of cognitive ASs. Recent research claims that the cognitive based games must incorporate in adaptive mechanisms especially in real- time adaption. Our research focuses on the domain of computer games based on emotions of player. In this research paper, we will layout a framework for adaptive agent game at which player's emotions are shown at each move in emotion avatar. With the help of cognition adaptive nature, system can change its level of difficulty as any change occur in performance of player. After achieving a real cognitive improvement, system will be able to provide appropriate challenges. Emotions in games enhance the motivation of player's by dynamically adapt the procedure of agent systems.

Keyword: Dimensional Model (DM), Classification Model (CM), facial expression emotions (FEE), Affective Virtual Reality (AVR), Game State (GS), AS (AS), Heart Rate Variability (HRV)

1. Introduction:

Psychology has many topics in his area but most important concept is "Emotion". In computer science paradigm, we can handle the emotions in the "Human-Computer Interactions (HCI)". In computer science, we can model emotions in two categories.

i. Dimensional Model (DM)
ii. Classification Model (CM)

In DM, emotions are understandable by designed in a coordinate system and mentioned in space. In CM, emotions are described after categorization. In general, emotions are categorized in four categories, i) behavioral reaction ii) expressive reaction iii) physiological reactions iv) subjective feelings [1]. Our research is basically based on behavioral reaction category

Behavioral Reaction: Behaviors shows complete picture of feelings and in our mechanism, behaviors are based on engine of game. There are five types in which behaviors are categorized [2]. Our agent-based system supports all these five categories.

i. Responsive: behavior should be "Responsive" such as quick reaction.
ii. Interruptible: behavior may be affected by other events, actions and behavior.
iii. Collaboration: it should respond corresponding to the other behavioral action.
iv. Generative: they can be easily created by other programmers which are at initial stage.
v. Resumable: we can continue the process if it break at any stage.

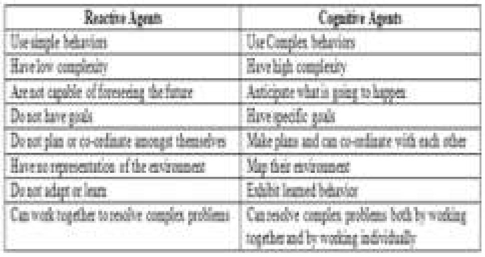
Emotions are conveying meaning through facial expressions and these emotions are handling of skin, movements, and facial muscles. These facial expression emotions (FEE) are analyzed through computer science techniques such as computer vision and image processing.

Agents are characterizing by their location of placement. In general they are categorizing in three types. First type is known as "Purely Reactive Agent". In these type insects, virtual insects and insect-like robots are used. This type is considered as most general one. Second category is "Continuum of Agents" which deals with animals and robots, in other words they deal in artificial life. Third class name is "Cognitive Agents or Thinking Agents". They are based on humans (may be humans are consider as virtual humans) and intelligent agents. The classification of agents is shown in figure 1.

Purely Reactive Agents
Insects, Insects-like robots, Virtual insects
Continuum of Agents
Animals, Robots, Artificial life
Cognitive Agents or "Thinking" Agents
Humans, Intelligent Agents, Virtual Humans

Fig. 1: Categories of Agents

Reactive agents performance is very limited when we compare it with cognitive. Cognitive agents have more plan ability; they have more co-ordination power with other sets or themselves. In other words cognition reacts when an event happens [3]. Whereas, reactive agents are worked collectively with the bounding of all together in terms to solve complex problems. Some comparison is given below in figure 2.



Reactive Agents	Cognitive Agents
Use simple behaviors	Use Complex behaviors
Have low complexity	Have high complexity
Are not capable of foreseeing the future	Anticipate what is going to happen
Do not have goals	Have specific goals
Do not plan or co-ordinate amongst themselves	Make plans and can co-ordinate with each other
Have no representation of the environment	Map their environment
Do not adapt or learn	Exhibit learned behavior
Can work together to resolve complex problems	Can resolve complex problems both by working together and by working individually

Fig. 2: Comparison between reactive agents and cognitive agents

Facial expressions can be helpful in game scenario by showing the response of game player (emotional response), such as what are the feeling of a player at different levels specially game levels became harder and harder; with the help of these features we can get a feedback of player in terms of emotions through the process of game design [4, 5, 6, 7].

The latest "resurrection" of activity in VR, spurred with the incipient gaming technologies. Designers of Human-Computer Interaction (HCI) system are utilized in the immersion experience, distribute compelling, announce different multidimensional input/output contrivance, interactive style with approach of 3D world. Furthermore, one research area of HCI is controvertible, that achieves best place in upcoming time which creates strives towards straightforward communication in person Encephalon and computer systems. In 2006, Cairns present an idea that accurate "Immersion" which may only be access through proper utilization of latest Encephalon-computer Interfaces [8]. But, as that day concerns, it is paramount to accept, in leading, how it may be conceivable to quantify and, emotional connectivity and person engagement influence with basic worlds utilizing "Psychophysiological" methods. Encephalon-Computer Interaction (BCI) systems endeavor to ameliorate HCI and increment the engagement impression by precisely interfacing with the nerve system of human and abstracting the unreal fence to emotional interaction controlled by ordinary input-exhibit strategies. These incipient channels of interface can have the possibilities for the purpose of introduction an immensely colossal number of incipient communication methods in latest HCI systems, and may be they are able to amend the process of interaction considerably. As the interaction process has been highly predicated when we use "Conventional" techniques, in that system operators mostly deal with "Physical Interaction" contrivances to optically discern, sense haptic, auricular discern, act, and in a few perspective even verbalize with the scheme. As a development to these conventional schemes; the near-term purpose of BCI structures, may be able to convert user Noetic conceptions and concerns by blunt contact to the user Encephalon and utilize this advice as an incipient method channel for HCI structures [9]. Researchers have move their attentions towards prelude of straight Encephalon system interaction from HCI structure, Aljandro at el. and Avinash at el. Cited some examples in their literature [10], these examples discuss quantification of melancholy, control mechanism and stress-level at adaptation of game [12, 13]. Affective computation is described under the umbrella of research sub-categories into BCI systems. Affective computation, in basis, file psycho physiological signals which receive from the computer-users, which after facilitating the whole system to retrieve data of pertinence to their cognitive states and emotions. This input data could give many distinguish features for latest HCI systems, endeavoring to fortify the development of tenable immersive interpretations. When we discuss briefly VR field and the pertinence of affect issues, analysts have calculated the implementation of constructive realities in many distinctive areas. As well as regalement, Vrs and soi-disant “serious games” counterparts have been utilized for purposes of training [7, 8, and 9], pain diversion, rehabilitation régimes, and emotional disorder therapy, to mention but a handful of applications. The all above mention discussion focus the attentions of users interaction with virtual situation, and to increment their impression of immersion and presence within them, so efficaciously distributing incipient proficiency, erudition or may be in rare cases, alternate as a form of clinical diversion. In 2006, Joel's advise that transmutations in the exhilaration level, affect the cognitive and recollection action. He suggested that recollection performance adjustment (either impairments or ameliorations) are fully time dependent and the emotional experience background. Ergo, describe the users' emotions perception, when bare to virtual realities and handling their affective experiences in the virtual situations. We conceptualized, evaluated and designed an AVR, capable to arouse sundry emotional maturities on the component of the user's utilizer. In the latest study, by using the architecture of Affective VR, a computing scheme which is based on affect was conceptualized, evaluated and designed. By doing this, the affair in the middle of human emotions and psycho physiological signals have been the investigation focus, and evoked through the designed AVR. To back this work:

The AS control consideration; and fully check has been perform in WM [2] [3] [4]. Consideration and WM are the two cognitive skills assessment tools that are essentially cognate; input information as signal regulates which create attention and WM absorb it [5]. When we are taking about other processes of cognition they are perpetual. Recent work in understanding of game environment suggests that WM does not consistent effected with the negative valence [2] [4]. However, utilizing felicitous can be incremented by the attention through which a player can activate [4].

The latest strategy in this current research cognition based game has adaptive nature through which a player transmute the difficulty level of game in authentic time which is based on the players' performance [6] [7].

However, when we talk about adaptive mechanisms they ignore the paramount AS role on performance of cognition. The analysis and detection of AS Include in this flexible structure can amend the adaptation which has a positive impact on the cognitive performance of player [9]. The main goals of this research are twofold: 1) investigating WM achievement with comparing desktop with VR when a player playing a video game, and 2) examine the role of arousal and valence on performance of WM.

Games are fun and fun is playing games. When we are talking about computer games, they are measured in affective computing. Games have properties such as they are interactive, result-oriented, competitive, dynamic, has excited nature. Because of these characteristics, we can influence player's state of emotions.

1.1. Affect and Cognition:

AS, represented arousal and valence in a two dimensional form, which can have effects of both negative and positive on WM and attention [10]. Benin et al. [2] in his paper summarize the hypotheses related to the following question. “How emotion affects recollection?” While negative and positive valence conventionally enhances recollection, arousal avails recollection. Furthermore, when emotion avails to process information (encoding), it additionally facilitates the storage of that particular information (consolidation) [2]. This affair between cognition and affect has withal been studied in terms of physiological to utilizing mainly HRV as a quantification of cognitive load and stress.

1.2. Affect detection in gaming:

User experience related to earnestness and vividness of emotions are highly suggested [12]. In last few years, researcher induced the utilization of VR in video games especially has brought an instrument in engagement and immersion of game player's. In the virtual world the feelings of player our reported to incipient the immersion degree level [12]. AS presence in game have been suggested the direct influence in the presence of earnestness and vividness of emotions [12]. Many researchers referred VR as "Affective medium" because it has the capacity to evoke and the AS concentration [12].

AS is utilized to improve adaptive assessment i.e. closed-loop input in video games that are based on habituating the game confer to the current AS of player [13]. AS can withal for purpose as well as to amend the player experience.

1.3. Cognitive Training Affects:

A new trend of cognitive skill effect is studied in video games. However, most of the games do not induce the beneficial skills of cognition. Studies were highlighted reiterated contributions of cognitive skills without adaptation of difficulty [13]. Recently, Anguera et al. engendered a new video game "Neuro racer". In this game, he demonstrated authentic amendments to improve the cognitive skills for example multitasking and attention. His game habituates the player's performance through the difficulty level in order to opportunely check their cognitive art. With the utilization of such approaches we can handle the emotional disorder's like despondence and cognitive capabilities like in different other games such as in game "EVO" [7]. Some certain elements related to game are integrated to gain rewards, increasing more fun levels in game and in releasing mental stress [13]. This incipient game generation for the use of train cognitive system demonstrates the paramount of keenly intellective flexible mechanisms in terms to test the player and introduce personalized training. Mishra et al. [13] demonstrate that the closed-loop as input channel should utilize the performance of player's additionally authentic data related to time computed as player perform some comportment and interaction.

2. Related Work:

Machine-learning techniques and genetic algorithms are the latest trends which are used in gaming to learn player's game and make a game more challenging. Curz and Demasi designed an "Intelligent Agent Employing Genetic Algorithm techniques" to make a user game level into a best fit curve [18]. In these types of games player's activity is monitor and then made decisions about game goals. Our aim too is to monitor a player's activity in game and after collecting the information of player's progress and system defines player's emotions about game activities.

Now a day, a "Dynamic Game Difficulty Balancing" (DGDB) technique is used to adjust parameters of games. In other words, this mechanism is incorporate adaptation in games. By using, that technique we can monitors the performance of player in terms of game's level difficulty. Chapman's and Hunicke make an approach in which they can handle the environment setting of games. By doing this they measure the game harder and easier level of challenges [19]. Resident Evil uses a "Difficulty Scale" parameter in their systems to measure the performance of player according to player's grade [20]. Mario Kart introduces a bounce feature to help in upgrading player's position. Imbert and de Antonio use emotion-driven reasoning technique in the model of Cognitive Architecture to handle social behavior and emotions [21].

Yeh et al. [4] described the strategy of negative emotions that how they influence WM in an ingeniousness of game by simply inquire participants to play game in three incrementing levels of difficulty. Homogeneous to Bennion et al. [2], he fined a point that arousal can avail the WM but negative effects could be generated. They defined a game with evading negative emotions in the game which increases the challenges to arouse the player's consideration.

3. Framework:

This part represents the necessary data for guiding the designers of games for enhancing their game through the concepts and techniques for artificial intelligence to incorporate player's emotions and feeling. So we present software framework architecture in figure 3 and define their components in detail form. This system framework architecture is visible in figure 1 to provide a flexible model of artificial intelligent based games. Further components with different roles are clearly separated to provide flexibility in implementation of each component to the designer. As we know each decision in agent based systems, is based on “Local Situation” and this decision is affected only “Local Situation” [22].

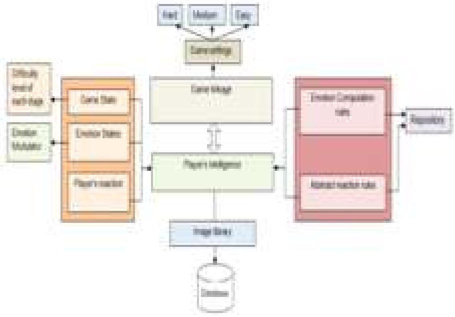


Fig.3: Framework Architecture

3.1. Game Linkage (GL):

GL provides the fundamental functionality to the player to interact with the agent system. In order to co-operate such communication, a protocol is used for communication to characterize the specific picture message to convey player's emotions [23]. As a player execute a particular action in this game, the GS become changed for that particular reason, through the process of cognition player avatar is selected and successfully send to the Player's Intelligence phase.

3.2. Player's Intelligence (PI):

This component part works with all the parts of system. Firstly, it connects with a communication protocol to game GL to communicate with game system. When the state of game or emotion is changed by taking further step in game; the state sends next latest avatar command to PI. PI then receive a corresponding avatar from IL after the conformation of rules.

3.3. System Rules:

The system makes its decision, based on logics of AI in the rule form. This rule system works as backbone of AI system. In our system this part is split into two parts, i) Emotion Computation rule (ECR) and ii) Abstract Reaction Rule (ARR). In order to design a system for AI rules, programmers can choose many programming languages. In our system we use C#. The main beneficial point of our system is that programmers can switch player's emotions by just switching the system rule.

3.4. System states:

This part is split into three further components. Game state: each game has many level of competition. Game player have to complete a level to reach at next level. After completion of one level, the state will updated and state of game will be changed. Emotion state: after each step or decision command at each level, emotion of avatar will be changed according to the situation. Player's reaction will vary after each move or after each change in avatar.

4. System Input:

We capture emotions as input parameter through facial expressions. The main purpose of this research idea is to design a novel scheme based on player's emotions interaction in a game. We build a system, which directly handles the player's facial expressions. Our proposed system handles five categories of emotions (happy, sad, surprise, angry, fear) out of eight emotions (Happy, Sad, Fear, Normal/ Neural, Surprise, Anger, Disgust, Contempt).

Normal/ Neutral
Surprise
Happy
Contempt
Emotions
Sad
Disgust
Fear
Anger

Fig.4: Types of Emotions

4.1. Methodology:

Our Agent based system focuses on characters (characters which player used to play). System thoroughly monitors the game activities by continually collecting data at each move of player and at each level.

At each move made by player, our agent system predicts player's emotions about game difficulty. The following are the decisions of our proposed agent based system. These rules are graphically defined in figure 5.

i. If player move is valid and accurate, our agent system makes "Happy Face"

ii. If player move is invalid and not up to the mark, our agent system makes "Sad Face"

iii. If player move take much time in decision, system makes "Disappointed Face"

iv. If player continuously made wrong moves then system generates "Angry Face"

v. If player hit a move and generated results are excellent, then system generates "Surprise Face"

vi. At the start of game Player's emotions described by "Normal Face"

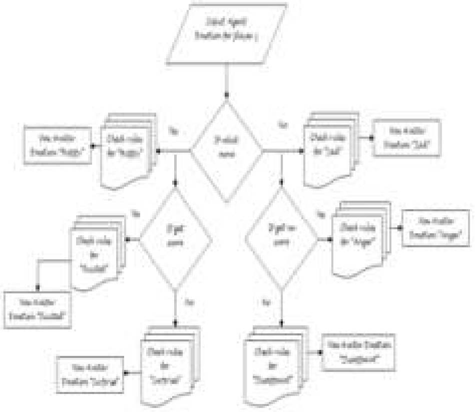


Fig.5: Rules for Player's Emotions

4.2. System Outcomes:

In our idea, we employ the player's emotional states, in plan to increase the social assessment. At that stage we neither use any conquer substantive player's emotion structure. Our main focus is to introduce a new idea based on intelligent system, to build a new avatar of player that is dynamically build emotions. That avatars are selected on the player's selection of objects and player's score gained. Our system behaves like a commentator of sports and any TV-show game and tries to simulate human behavior.

4.3. Algorithm:

We use C# language to build our agent based system for defining the player's emotions in game at each move in each level. The system pseudocode is visible in figure 6, 7 to provide a main methodology of artificial intelligent based games.

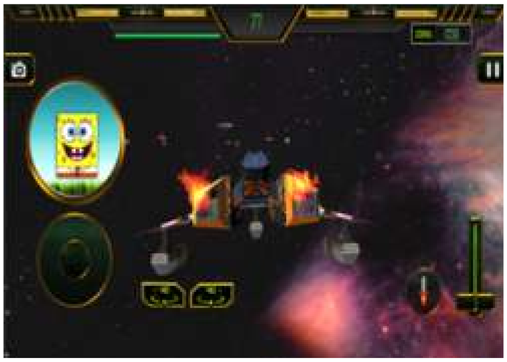


Fig. 8: Best player move, "Happy" avatar.

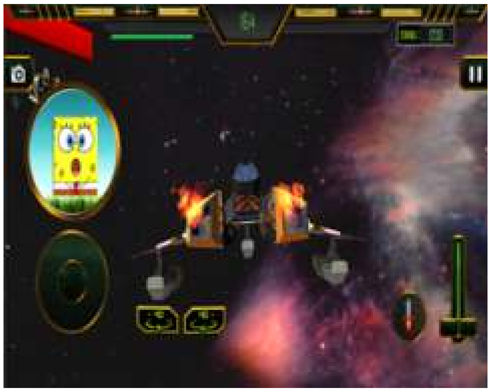


Fig. 9: little mistake in player's move, "Surprise" avatar.

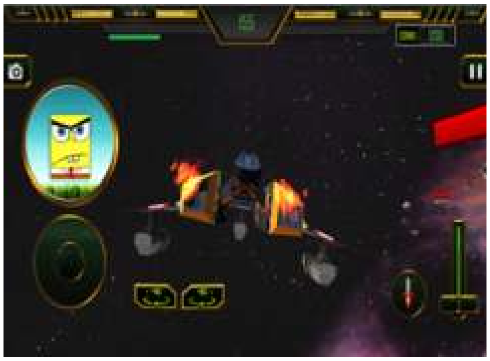


Fig. 10: not an accurate move, "Contempt" avatar.

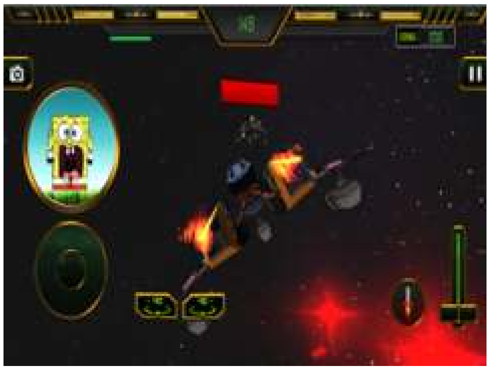


Fig. 11: Player's wrong move, “Fear” avatar.

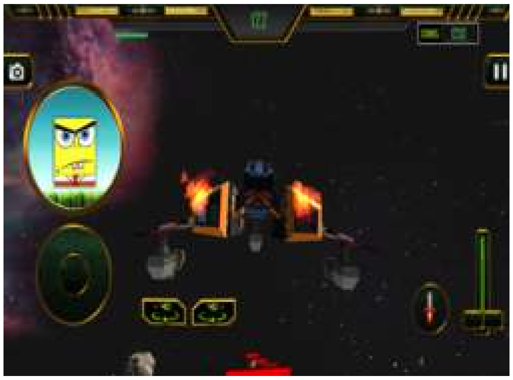


Fig. 12: Not best player move, “Disgust” avatar.

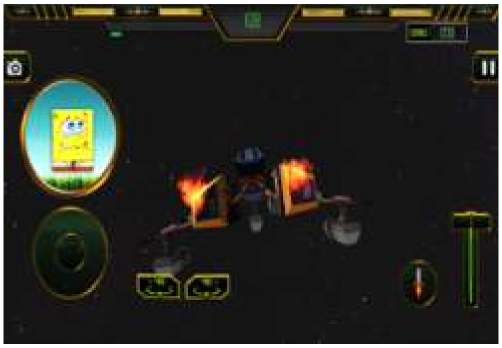


Fig. 13: Player going to be loses the game, “Sad” avatar.

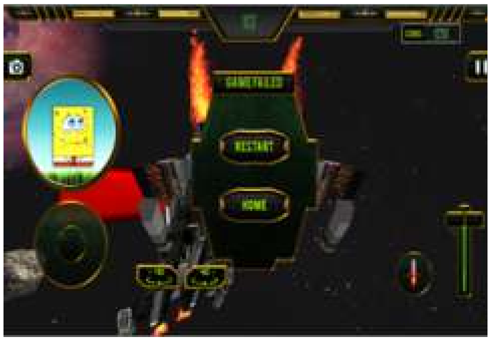


Fig.14: Player loses the game, “Sad” avatar.

5. Future work:

Future work may be based on emotion distinguished between the player's different smiles such as some smiles are only close-lip and some smiles convey real meaning of laugh means obviously big smile. Both are handling in our system as “happy”. Really need is to distinguish such difference in emotion types.

Emotion agent system is based on image processing and artificial intelligent approaches by characterize and analyze the FEE. System collected this FEE which is stored in a database on a windows computer. This system handles five categories of emotions (happy, sad, surprise, angry, fear) out of eight emotions (Happy, Sad, Fear, Normal/ Neutal, Surprise, Anger, Disgust, Contempt). As our system generate output in image form, in future researcher can enhance these outputs at audio messages corresponding to behavior, can generate any text message on screen corresponding to player's behavior, and any animation based on type of emotions as define in figure 4.

6. Conclusion:

In our research paper, we design a framework for constructing a game based on artificial intelligence techniques, to present player's emotions at each level of game or at each move. Our work exhibit the usefulness of generic framework architecture for game player's emotions. By using this novel approach, designers can design their games by search processing, way of inducing and utilization of player's emotions. We can motivate player's by dynamically adapt the procedure of agent systems. Another important element is improving the game experience with the emotion images explaining the emotions of player, it will introduce the social interaction. Our research idea will help the game's developer in player's characters creation for the development of new games, insert new emotions and adaptation of social assessment.

References:

1. Pieter Desmet, "Measuring Emotion: Development and Application of an Instrument to Measure Emotional Responses to Products," In Funology, edited by Mark A. Blythe, Kees Overbeeke, Andrew F. Monk, and Peter C. Wright (Human-Computer Interaction Series 3. Springer Netherlands, 2003), 111.

2. Maria Cutumisu, Duane Szafron, "An Architecture for game behaviorAI: Behavior Multi-Queues" in proceeding of the fifth artificial intelligence for Interactive Digital Entertainment Conference, 2009.

3. William John Teahan, "Artificial intelligence-Agent Behaviour I", William John Teahan & Ventus Publishing ApS, ISBN 978-87-7681-559-2, page 9-11.

4. Rajava Niklas, Saari Timo, Laarni Jani, Kallinen Kari, and Salminen Mikko. "The Psychophysiology of Video Gaming: Phasic Emotional Responses to Game Events," 2005. In Proceedings of DIGRA Conference, http://www.digra.org/wp-content/uploads/digitallibrary/06278.36196.pdf

5. Regan L. Mandryk and M. Stella Atkins, "A Fuzzy Physiological Approach for Continuously Modeling Emotion during Interaction with Play Technologies," International Journal of Human-Computer Studies, 65, (2007): 329–47.

6. Jing-Kai Lou, Kuan-Ta Chen, Hwai-Jung Hsu, and Chin-Laung Lei, "Forecasting Online Game Addictiveness." In 11th Annual Workshop on Network and Systems Support for Games (NetGames), 2012.

7. Richard L. Hazlett, "Measuring Emotional Valence During Interactive Experiences: Boys at Video Game Play," In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1023–26, New York, NY, USA, 2006.

8. Paul Cairns, Anna Cox, Nadia Berthouze, Samira Dhoparee, and Charlene Jennett, "Quantifying the experience of immersion in games," in Workshop on the Cognitive Science of Games and Gameplay, Vancouver, 2006.

9. Anton Nijholt, Bos, Danny Plass-Oude, and Boris Reuderink, "Turning shortcomings into challenges: Brain–computer interfaces for games," Entertainment Computing 1, vol. 1, no. 2, pp. 85–94, April 2009.

10. Alejandro Rodríguez, Beatriz Rey, Miriam Clemente, Maja Wrzesien, and Mariano Alcañiz, "Expert Systems with Applications Assessing brain activations associated with emotional regulation during virtual reality mood induction procedures," Expert Systems with Applications, vol. 42, no. 3, pp. 16991709, February 2015.

11. Avinash Parnandi, Youngpyo Son, and Ricardo Gutierrez-Osuna, "A ControlTheoretic Approach to Adaptive Physiological Games," in 2013 Humaine Association Conference on Affective Computing and Intelligent Interaction, Geneva, 2013, pp. 7-12.

12. Günter Edlinger, Clemens Holzner, Christoph Guger, C. Groenegress, and Mel Slater, "Brain-Computer Interfaces for Goal orientated Control of a Virtual Smart Home Environment," in Neural Engineering, 2009, NER '09. 4th International IEEE/EMBS, Antalya, 2009, pp. 463-465.

13. E. Lalor et al., "Brain Computer Interface based on the Steady-State VEP for Immersive Gaming Control," EURASIP Journal on Applied Signal Processing, vol. 49, no. 1, pp. 63-64, 2004.

14. H. Gunes et al., "Categorical and dimensional affect analysis in continuous input: Current trends and future directions," Image and Vision Computing, vol. 31, no. 2, pp. 120–136, 2013.

15. M. Suriya-Prakash et al., "Is heart rate variability related to cognitive performance in visuospatial working memory?" PeerJ PrePrints, vol. 3, 2015.

16. G. Riva et al., “Affective interactions using virtual reality: the link between presence and emotions,” CyberPsychology & Behavior, vol. 10, pp. 45–56, 2007.

17. J. Mishra et al., “Video games for neuro-cognitive optimization,” Neuron, vol. 90, no. 2, pp. 214–218, 2016.

18. P. Demasi and A. Cruz, “Online coevolution for action games,” in Proceedings of the 3rd International Conference on Intelligent Games and Simulation, pp. 113–120, London, UK, 2002

19. R. Hunicke and V. Chapman, “AI for dynamic difficulty adjustment in games,” in Proceedings of the 19th National Conference on Artificial Intelligence, pp. 91–96, USA, July 2004.

20. Resident Evil 5 Official Strategy Guide, “Prima Publishing,” 2009.

21. R. Imbert and A. de Antonio, “An emotional architecture for virtual characters,” in Proceedings of the International Conference on Virtual Storytelling (ICVS '05), Springer Lecture Notes in Computer Science, no. 3805, pp. 63–72, 2005

22. M. Mujtaba, Syeda Binish Zahra, “How life becomes artificial when we enter in Computer Zone”, in International Journal of Computer Application, Issue 4, and Volume 2 (March-April 2014), ISSN: 2250-1797.

23. Syeda Binish Zahra, “Effect of Visual 3D Animation in Education”, in European Journal of Computer Science and Information Technology, Vol. 4, No. 1, pp.1-9, January 2016.

LAHORE GARRISON UNIVERSITY

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

VISION

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

MISSION

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

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

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