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

International Journal for Electronic Crime Investigation

(IJECI)

VOL: 5
ISSUE: 2 Year 2021

Email ID: ijeci@lgu.edu.pk

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

LGU International Journal for Electronic Crime Investigation
Volume 5(2) Year (2021)

SCOPE OF THE JOURNAL

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

SUBMISSION OF ARTICLES

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

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

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

LGU International Journal for Electronic Crime Investigation
Volume 5(2) Year (2021)

CONTENTS

LGU International Journal for Electronic Crime Investigation
Volume 5(2) Year (2021)

Advisory Board

Editorial Board

Chief Editor

Assistant Editors

Reviewers Committee

Need for Implementing Control on Political Parties Funding

Kaukab Jamal Zuberi
Chief Editor

Internet has become a part of our life. We use internet to search information, deliver education, communicate with each other, doing medical operations, entertainment and monitor various devices ranging from CCTV cameras to pacemakers. Cyber world therefore, is a space on which we are depending by one way or other every single day. Among the broadband networks, beneath us, and the wireless signals around us, the local networks in our schools, hospitals and businesses, and the massive grids that power our nation, classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than any time in human history. It is a great irony of our cyber age that the technology which enables us to create, build and facilitate our lives also empowers those who would disturb and destroy.

So, cyberspace is real. And so are the risks that come with it.

Cyber space has been declared as the fifth domain of war. Any attack on the cyber space is now considered as the attack on the sovereignty of the country. Next wars will also include cyber-attack directed towards the critical infrastructure of the enemies.

Critical infrastructure as defined in Prevention of Electronic Crime Act 2016 is defined as follows:

"“Critical Infrastructure” means critical elements of infrastructure namely assets, facilities, systems, networks or processes, loss or compromise of which could result in,:-

(a) Major detrimental impact on the availability, integrity or delivery of essential services, including those services, whose integrity, if compromised, could result in significant loss of life or casualties, taking into account significant economic or social impacts; or

(b) significant impact on national security, national defense, or the functioning of the state”.

Destruction of critical infrastructure may result in provision of critical services to the citizens and/or result in huge economic losses to the country. It may also cause huge losses of life.

Types of Cyber Warfare:

Cyber Espionage

Traditional espionage is not an act of war, nor is cyber-espionage, and both are generally assumed to be ongoing between major powers. Despite this assumption, some incidents can cause serious tensions between nations, and are often described as "attacks". For example

i. Massive spying by the US on many countries, revealed by Edward Snowden.

ii. After the NSA's spying on Germany's Chancellor Angela Merkel was revealed, the Chancellor compared the NSA with the Stasi.

iii. The NSA recording nearly every cell phone conversation in the Bahamas, without the Bahamian government's permission, and similar programs in Kenya, the Philippines, Mexico and Afghanistan.

iv. The security firm Area 1 published details of a breach that compromised one of the European Union's diplomatic communication channels for three years.

Out of all cyber-attacks, 25% of them are espionage based

Sabotage

Computers and satellites that coordinate other activities are vulnerable components of a system and could lead to the disruption of equipment. Compromise of military systems, such as C4ISTAR components that are responsible for orders and communications could lead to their interception or malicious replacement. Power, water, fuel, communications, and transportation infrastructure all may be vulnerable to disruption. According to Clarke, the civilian realm is also at risk, noting that the security breaches have already gone beyond stolen credit card numbers, and that potential targets can also include the electric power grid, trains, or the stock market.

In mid-July 2010, security experts discovered a malicious software program called Stuxnet that had infiltrated factory computers and had spread to plants around the world. It is considered "the first attack on critical industrial infrastructure that sits at the foundation of modern economies," notes The New York Times.

Denial-of-Service Attack

In computing, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. DoS attacks often leverage internet-connected devices with vulnerable security measures to carry out these large-scale attacks. DoS attacks may not be limited to computer-based methods, as strategic physical attacks against infrastructure can be just as devastating. For example, cutting undersea communication cables may severely cripple some regions and countries with regards to their information warfare ability

Electric Power Grid

The electric power grid is susceptible to cyberwarfare. The United States Department of Homeland Security works with industries to identify vulnerabilities and to help industries enhance the security of control system networks. The federal government is also working to ensure that security is built in as the next generation of "smart grid" networks are developed.

Propaganda

Cyber propaganda is an effort to control information in whatever form it takes, and influence public opinion. It is a form of psychological warfare, except it uses social media, fake news websites and other digital means. In 2018, Sir Nicholas Carter, Chief of the General Staff of the British Army stated that this kind of attack from actors such as Russia "is a form of system warfare that seeks to de-legitimize the political and social system on which our military strength is based".

Jowell and O'Donnell (2006) state that "propaganda is the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist". The internet is the most important means of communication today. People can convey their messages quickly across to a huge audience, and this can open a window for evil. Terrorist organizations can exploit this and may use this medium to brainwash people. It has been suggested that restricted media coverage of terrorist attacks would in turn decrease the number of terrorist attacks that occur afterwards.

Economic Disruption

In 2017, the WannaCry and Petya cyber-attacks, masquerading as ransomware, caused large-scale disruptions in Ukraine as well as to the U.K.'s National Health Service, pharmaceutical giant Merck, Maersk shipping company and other organizations around the world. These attacks are also categorized as cybercrimes, specifically financial crime because they negatively affect a company or group.

There is a controversy against the term “cyber warfare”. Some believe it is not the right term. Eugene Kaspersky, founder of Kaspersky Labs, concludes that "cyberterrorism" is a more accurate term than "cyberwar". He states that "with today's attacks, you are clueless about who did it or when they will strike again. It's not cyber-war, but cyberterrorism.

In either way, it is the responsibility of the government to develop an effective cyber security strategy and develop a qualified manpower in various domains of cyber security.

A recent study conducted by Comparitech

has revealed that Pakistan ranks 7th among the countries having the worst cybersecurity. This makes Pakistan one of the most unprotected countries. Recent attack on FBR was one of the many attacks successfully conducted on Pakistani critical infrastructure. The cyber-attacks can result in very high losses. If we do not develop a comprehensive cyber security policy and give incentives to develop high level of professionals in this team, we keep on risking to compromise our cyber space. Pakistan is at risk and we need to act fast.

Fatima *et al.LGU (IJECI)* 2021

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

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 5 issue 2 Year 2021

Identification of Violent Behavior in Serial Killers Using Handwriting

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

Abstract:

This review paper highlights the hidden violent and aggressive behavior in serial killers by analyzing its handwriting features. Identification of violent behavior in handwriting is very important as it has close relation with personality disorder or psychopathy and its associated crimes that can be overcome in future. Graphology is a scientific method to identify an individual's personality, temperament, professional and intellectual behavior, social and inner capacities by evaluating and understanding patterns revealed in handwriting. Handwriting analysis describes a psycho-social-behavior like that of psychologist who emphasis on biological and psychic components interactions revealed in one's handwriting e.g. serial killers. Graphology experts approach advanced technology and research studies to facilitate the process of handwritten images of general public data and observe the signs of violence in their graphical handwritten features. It can be used as coherent and resourceful profiling instrument to enrich the information and to assist the forensic psychologists, psychiatrists and investigators in their investigation.

Keyword: Graphology, Violent Behavior, Personality Disorder/Psychopathy, Serial Killers.

1. Introduction

Currently crime rate is accruing rapidly with unique cases reported on news and social media that involve violent and aggressive nature. Among these cases, gang rape committed in Delhi India in 2014 was the most famous case in which four accused brutally raped the girl in some dishonorable and indescribable violent ways [1]. Ryan International School was another highlighted crime case in India that involved murder of class two student by the accused who was in class eleven just for delaying class exams. However, it was difficult to believe that the accused could be such violent and aggressive as he was composed and well-known for performing musical instrument in school [2]. Similarly, three men were killed in 2013 by a British woman Joanna Dennehy who was 31-year-old [3] and 30 people were murdered by Ted Bundy, the most famous serial killer in America [4].

It is easy to criticize one's evil conduct but more difficult to understand him [5]. Aggressive and violent nature is common behavior behind calm and cool exterior of criminals that leads them to commit brutal crimes [6]. This behavior differentiates them from normal people and categorizes them as personality disordered or psychopathic [7, 8, 9]. Psychopathy accounts for a set of personality traits including low emotional responses, lack of sympathy and being impulsive with deprived behavioral controls that results into criminal or antisocial behavior. Additionally, psychopathic behavior exhibits extreme egoism, inability to express love, and failure to establish personal relationships and environmental interaction. Psychopaths show tricky and scheming interpersonal style that leave vast destructive impact on their personal as well as social life and work. Nearly 1% of general population and 15-25% of prison population as compared to offenders, contribute to psychopathy including serial killers with more serious violence predominantly in men than women [5].

Psychopathy especially Antisocial Personality disorder (APD) mainly in serial killers has been assessed in various ways mainly from two aspects, psychological and psychiatric [9, 10]. Psychological studies involve behavior analysis based on sets of lengthy structured interviews, while psychiatry studies involve understanding of mental features such as amygdale and fMRI study etc. [11]. Likewise, self-report scales are highly associated with observing measures of psychopathy such as Levenson Self-Report Psychopathy Scale. However, self-report scales are of limited efficacy in clinical or forensic settings to detect APD as dishonesty and lack of understanding are the signs of APD. For that reason, handwriting analysis should be supplemented as supportive tool to self-report scales for assessing the negative personality traits including dishonesty, aggression, violence, emotional instability, unreliability and insincerity in serial killers. Two instruments namely Psychopathy Checklist-Revised (PCL-R) and Psychopathy Checklist-Screening Versions (PCL-SV) are considered as gold standard for diagnosing and assessing psychopathy in forensic samples. PCL-R is structured as a two-factor model i.e. emotional and interpersonal traits, while PCL-SV is classified as four factor model i.e. life style, affective, antisocial and interpersonal components. However, emotional and interpersonal deficits compel the psychopaths towards crime rather than any other factor or motive. Handwriting analysis can be used as precautionary approach to have awareness about antisocial personality disorder and its possible threat ahead of time [5].

Graphology or handwriting analysis is still an intact scientific study to determine the personality disorder or traits, writer behavior or psychological temperament [12]. Human beings have used handwriting for centuries as a way of communication, nevertheless, studies have proved that it also links to human psychological and brain activities [13]. Like all other actions, handwriting is considered an important feature of human brain that forms neurological characters and pattern based on writer habits. These patterns are driven by unique neuromuscular movement (hand) to write [14]. Central nervous system controls the writing organ that makes writing as an unconscious yet revealing process. Forensic graphologists use handwriting as an investigative tool to determine and reveal emotions, mood and mental health from brain impulses in criminal personality [15]. Psychopathic people that have personality disorder, reflect dysfunctional amygdale in their handwritings [16].

Many research used Apriori Algorithm [17] while some used computers as an advanced technology for various applications and crime analysis. Several studies considered handwriting as an identification tool as it is used as a biometric behavior [18]. Graphologists, psychologists, investigators and specialists should follow a common rule that there is no such thing as a psychopathic handwriting as there is no completely honest (normal) or dishonest (psychopath) one and every individual has a negative potential or choice to let run his/her actions (conscious) or to control it (unconscious). Psychopathy, dishonesty or hypocrisy has no equivalent and fixed sign, thus hypotheses should be built for graphological analysis of a psychopath as it requires to associate marks between negative feature and a writing sample [5]. Large number of research is available on handwriting analysis that predict personality traits [3, 5, 6, 10, 13], however research that predict violent and aggressive behavior in psychopath's or serial killer's handwriting is limited [19]. Research studies [15] show that exceptionally larger alphabets should be considered as red flag in handwriting sample and visualized writer's personal importance [20]. Handwriting is considered as a major element to study red flags that can lead to violent behavior in future. It requires further research that can assist to diagnose antisocial personality disorder from handwriting sample and will be a great support for the society [1].

2. Graphological Analysis of Dangerous Signs

There are measureable handwriting features that can be used as an identification tool to describe writers and can be significant for forensics, library science, data science and biometric purposes [1, 4, 9, 18]. Graphologists go through set of specific features in an individual handwriting that conveys a specific message primarily describing aggressive and violent behavior. Some of the potential features for aggressive and violent behavior are discussed as followings;

- **Level of Organization:** psychopath's handwriting with respect to graphology can be comparatively conformist with little rhythm, somewhat ordinary, repetitive, rigid and number of abnormalities. An organized writing is defined as precise, ordered, simple and balanced. However, the graphic gesture in a more common public situation is simplified, combined and calligraphic apparently with more positive sense of writing [21, 5].
- **Overly Wide Spaces between Words:** individual placing words with abnormal distance indicates paranoia and the distance put between each words represents the distance that the writer maintains between him and other people. People with abnormal distanced handwritings are distrustful and tend to be nervous for others motives intentions. They want to control everyone that makes them aggressive and paranoid. They hardly trust in others and there is lack of intimacy in their lives [13, 22].
- **Word Height:** word height is another feature that shows violent nature of an individual and Upper Zone with extremely larger alphabets indicates severe ethics. In most of the cases, graphologists noticed that the middle zone is more evident as compare to upper and lower zones which are instable and tense. Such features

indicate special consideration for sensations, unfulfilled desires and instinctive frustrations, imbalance and extreme structure of goals or motives and dishonesty [21].

- **Closely Spaced & Overly Spaced Letters:** these features indicate an individual is suffering from two negative aspects and confirm their uptight and paranoid nature. People with these feature are socially unstable and have real social problems. Loops that come to a point in Upper Zone represents frustration, pressure, irritation, nervousness and fear [23, 13].
- **Incoherent Baseline:** individual with incoherent baseline shows aggression in personality, failure to maintain a coherent or clear four dimensional pattern and trouble to fit with any kind of society. People with this type of feature tend to be sociopath who disconnect from the society and disrespect the societal norms [24].
- **Heavy Pressure, Uneven Slant & Baseline:** individual with this feature represents extreme angularity with heavy pressure in writing that suggests aggression, violent and defensive tendencies [13, 25]. Rigidity, anxiety, alertness, cruelty, insincerity, sadism and lack of cooperation are negative features associated with vertical writing slant. People with twisted and deformed handwriting tend to be potentially dangerous, crooked, biased, abnormal in thinking if they are forced to change themselves [13, 26]. Psychopaths whose writings are connected to the left slant or margin indicate connection to the past, very deep attachments for parents particularly mother, vulnerable childhood, and lack of independencies or positive activities [21].
- **Disconnected Writing:** people with this type of writing feature represent isolation, little coordination and withdrawal from positive life experiences that lead them to violent behavior. Narrow or mirrored elements in the writing may represent a sign shallowness of strong environmental influence and disproportionate reactions on writer. On the other hand, flat writing with false connection represents no sign of feelings or empathy for others and self-interest [1, 21].

East Tennessee University published a report on handwriting which contains a list of signs representing dangerousness and personality disorder as explained in figure 1 [7]. Handwriting features identified by handwriting analysis as well as by speech patterns are listed in figure 2 that represent signs of dishonesty and Personality disorders [27].

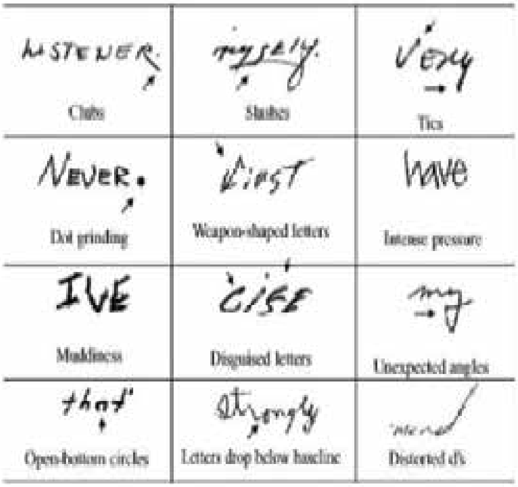


Figure 1: Signs of dangerousness in handwriting [1].

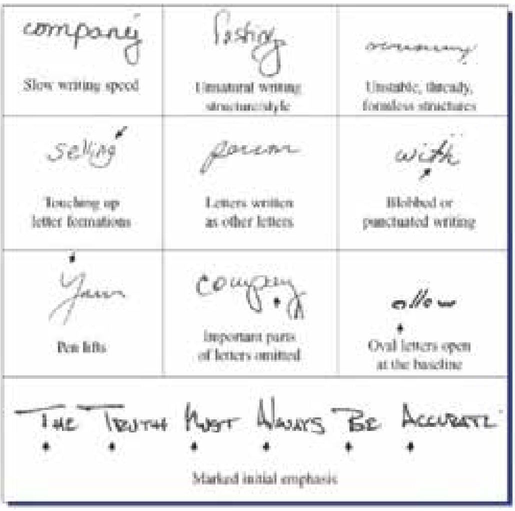

company
Slow writing speed
Unnatural writing structure/style
Unstable, threadly, formless structures
selling
Touching up letter formations
Letters written as other letters
with
Blobbed or punctuated writing
Pen lifts
Important parts of letters omitted
Oval letters open at the baseline
THE TRUTH MUST ALWAYS BE ACCURATE
Marked initial emphasis

Figure 2: Signs of dishonesty in handwriting [1].

3. Graphopathology of Psycho-Paths: Serial Killers Under the Microscope

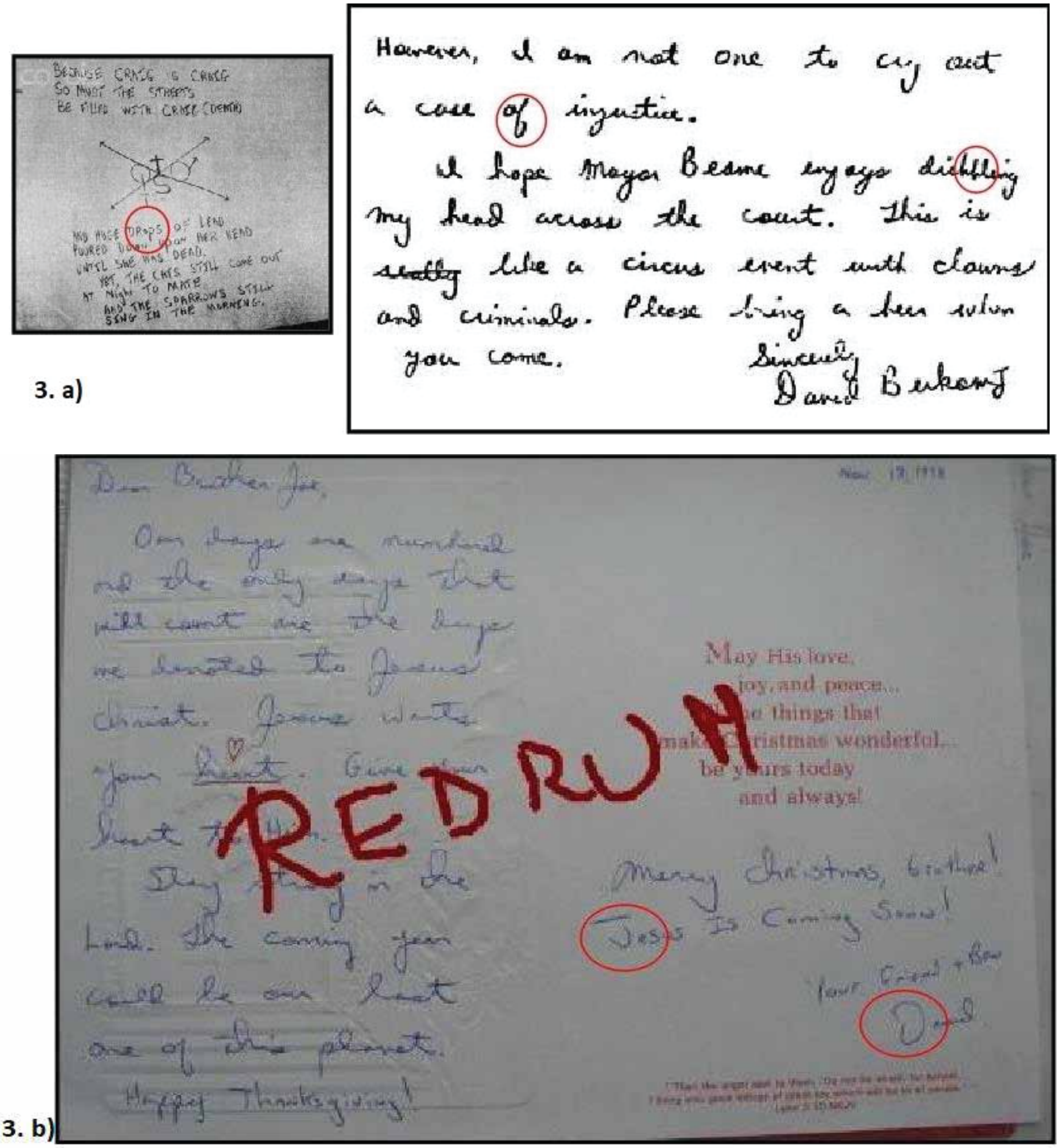
According to Wertham's theory that states that every criminal has the tendency to suffer from extreme pathological disorder and its deepened analysis should be considered to approach the essential parts of the problem. From a psychiatric perspective, schizophrenics, alcoholics, paranoiacs, rare case of neurotics or obsessive compulsives and extreme cases of hysteria are found among the most dangerous criminals. In the hierarchy of criminals, cases that can be categorized at the highest step are those that involve people mostly with schizoid personality i.e. the well-known serial killers. At this point, it is a valid question to ask about this category of perpetrators that "why the serial killers are psychopaths and why it is not listed in mentioned disorders" [21]. This statement was well explained by the scientist Florence Wittkowski who devoted her studies for the diagnosis of psychopathology through handwriting analysis. She identified that a specific symptom cannot define the psychopathy as it is not a disorder but a personality complex which is of more common classes of psychiatric diagnoses. This type of people is incapable of growing with the society, suffer from imbalance, and become psychopaths when they face rejection [28]. Hence, the serial killer is termed as psychopath as it has all signs of disorders mentioned earlier. The serial killer describes him as person who is intelligent or at times a genius with feeling of control and disobey imposition of the limits by others. They exhibit self-hatred as they suffered parent's negligence, severely abused and grown up in a violent family environment.

It would be fascinating and interesting step to analyze the criminal's handwriting where three names David Berkowitz, Ted Bundy and John Wayne Gacy represent the most important examples in behavioral analysis as followings;

Case Study No. 1: "David Berkowitz"

David Richard Berkowitz is an American serial killer and arsonist who murdered 6 people and wounded 7 others. He is also known as Son of Sam and .44 Caliber Killer, and committed crimes between July 1976 and August 1977 in New York. He is a common example of psychopathic character with disturbed childhood as he was born as a consequence of an affair marriage and was adopted by an average family. He disliked his step mother and sister who were accused of witchcraft and introducing him to punishment. He had a normal life by serving in the army and doing blue collar jobs regardless of no interest for school and obsession for minor theft and pyromania in his childhood. He claimed that he was introduced to drugs, violent crime and pornography after contacting with the occult in a cult in 1975 that involved only séances and fortune telling harmless activities [21, 29, 30].

Some letters were found throughout this period of time that proved to be useful to the investigation and to solve the puzzle. The analysis of these letters confirmed that psychiatrists described the killer as neurotic who was suffering from paranoid schizophrenia and believing that he was in possession of demon. David Berkowitz writing is vertical with horizontal lines running upwards sometimes, distance between the letters and words and line is small and normal, respectively.



3. a)

BECAUSE CRAIG IS CRAIG
SO MUST THE STREETS
BE FILLED WITH CRAIG (DEATH)

AND HUGE DROPS OF LEAD
POURED DOWN UPON HER HEAD
UNTIL SHE WAS DEAD.
YET, THE CATS STILL COME OUT
AT NIGHT TO MATE
AND THE SPARROWS STILL
SING IN THE MORNING.

However, I am not one to cry out a case of injustice.

I hope Mayor Beame enjoys dribbling my head across the court. This is really like a circus event with clowns and criminals. Please bring a beer when you come.

Sincerely
David Berkowitz

3. b)

Nov 17 1978

Dear Brother Joe,

Our days are numbered and the only days that will count are the days we devoted to Jesus Christ. Jesus wants your heart. Give your heart to Him.

Stay strong in the Lord. The coming year could be our last one of this planet.

Happy Thanksgiving!

REDRUM

May His love,
joy, and peace...
the things that
make Christmas wonderful...
be yours today
and always!

Merry Christmas, brother!
Jesus Is Coming Soon!

Your Friend + Bro
David

[illegible]

Figure 3: a) & b) Handwriting samples of David Berkowitz [21].

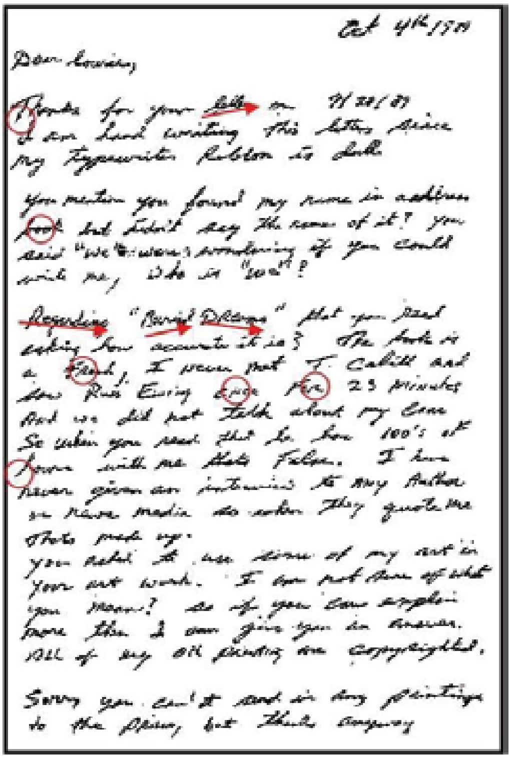
The upper zone is reduced with double loops, lower zone is ended rightward with “f”s that claims attention and zone which is best developed is the middle one. Arcades and semi angular connections is used with medium speed and pressure, keeping a bookish formation of certain letters like the “m”s and representing a 5th grader’s handwriting impression. However, some lightly peculiar appearance of “J”s and “D”s, and regressive ending traits are also detectable in this copy book writing samples [21, 29] as shown in figure 3.

The overall writing of Berkowitz represents the signs of abnormality that are deceptively subtler and important for the analysis. Nevertheless, these signs point towards a person who is disturbed, easy to be influenced, unable to maintain a healthy relationship, having a narrow concept of life and powerful inferiority complex, and incapable to associate his actions and their outcomes [21].

Case Study No. 2: “John Wayne Gacy Jr”

John Wayne Gacy was an American serial killer and rapist, also known as the Killer Clown who assaulted and murdered 33 young boys and men (1972-1978). He born in a middle class family with three children and was the only son in close affection with his mother and sisters. However, he had a difficult relationship with his abusive and alcoholic father who constantly demeaned him. He was molested by a family friend when he was 9 years old and later on after two years he suffered an accident with serious consequences that caused his father to ignore him. Similar to Berkowitz, he also had no interest in school but he succeeded in his own business and became an outstanding member of the society. He tried to hide his violent and bisexual tendencies by living a normal life but he failed to do so and as a result caused termination of his two marriages [21, 30].

During his trial, a team of psychiatrists diagnosed and described him as a person who depicts himself as a victim of hostile circumstance and denies for everything happened to him as an alibi to assure a sympathetic response. Technically some important features should be highlighted such as winding left margin and filling the page shows little space for others. The writing has rightward slant, little winding horizontal lines, letters with slightly reduced, words with large and rows with normal spacing. When considering zones, the upper zone is sharp, filled with ink, has low closed loops with hooked or clubbed debut, middle zone is thread like, lower zone has elongated with loops towards right and hooks such as “f”s. The writing is connected with semi angular inferior traits and angular arcades, achieved by medium speed and pressure [21, 29].



Oct 4th 1989

Dear Lorraine,

Thanks for your letter on 9/28/89
I am hand writing this letter since
my Typewriter Ribbon is dark

You mention you found my name in address
book but didn't say the name of it? you
said "we were wondering if you could
write me, who is "we"?

Regarding "Buried Dreams" that you read
asking how accurate it is? The book is
a Fraud, I never met T. Cahill and
saw Russ Ewing once for 23 minutes
And we did not talk about my case
So when you read that he has 100's of
hours with me thats False. I have
never given an interview to any Author
or News media so when they quote me
thats made up.
You asked to use some of my art in
your art work. I am not sure of what
you mean? So if you can explain
more then I can give you an answer.
All of my oil painting are copyrighted.

Sorry you can't send in any paintings
to the Prison, but thanks anyway

Figure 4: Handwriting sample of John Wayne Gacy [21].

According to professionals, Gacy's handwriting analysis represents a smudged writing with many signs of confusion, unpleasant pastosity, letters with clubbed or hooked debuts, using of capital letters within or at the beginning of words and displaying certain letters formation in awkward manner. The graphological interpretation represents a person with considerable issues when obeying the rules of society but he behaved as a proper individual when living through such rules. Other than this, he is discovered to be a confused and disturbed person with an explosive temper who struggles to fulfil his strong desires and to repress his anger that lead him into a violent human being [21, 29, 31].

Case Study No. 3: Theodore Robert "Ted" Bundy

Theodore Robert Ted Bundy is the most publicized psychopath serial killer, rapist, kidnaper and necrophiliac who was convicted for 30 murders and many other atrocious deeds between 1974 and 1978. The birth certificate of Ted Bundy clearly recognized his paternity but he was suspected to be the son of his own abusive and violent grandfather who pretended to be his parents and representing his mother as his older sister. He raised up in a violent environment and went through spotting traumatic electroconvulsive therapy of his grandmother for depression. These factors caused a young boy to show a vicious and disturbing behavior that accumulated with the passage of time into a large collection of pornography and establishing attraction towards knives. However, he claimed that these were the results of observing a suspicious ritual at the age of three when he found his aunt sleeping and surrounded by knives in her bed [21]. Though his mother's new husband adopted and loved him, he always felt isolated from him but found his support in reading various detective magazines, crime novels and documentaries, getting appeal towards people involved in sexual violence and displaying photos of mutilated or dead bodies. The main triggering event that led to his criminal development was his separation from his university sweetheart and it was a strong enough experience to discover the truth for a man who admitted and shown no interest in interpersonal relationships. Distress and rejection caused him to change his area of interest to psychology and started working at a suicide hotline emergency center. Later on, he commenced law classes and participated in a local reelection operation that led to the beginning of his horrifying violence acts [21, 29, 30].

After his arrest, the psychiatric diagnose found him a very kind, charming and caring person who can decide between wright and wrong but his apparent behavior shows little guilt or sorrow, narcissism, scheming behavior and a weak decision maker. His extremely thorough research and skills of minimizing physical evidence increased his personal charm, and his caring ability led to difficult, frustrating and a longer investigation that unfortunately suggested a large number of victims.

As compared to previous samples explained, Ted Bundy has a more structured handwriting with paragraphs that show interest for his writing appearance. His writing has winding right margin and linear left margin with considerably narrow and tall rightward slant. The writing represents dominant middle zone, low upper zone possessing loops or sharp booklets and more developed lower zone with rounded and big loops. The slightly arising and horizontal lines with reduced space between letters, varying space between words while small between lines shows embarrassments on various events. The writing is connected with semi angular traits and arcades follows by good speed and even pressure, representing a writing effort. However, a display of crooked letters or artistic interpretation of letters such as “f, l, h” was also found in this writing sample by constant use of long and hooked debut that shows beginning of a curious trait [21] as shown in following figure;

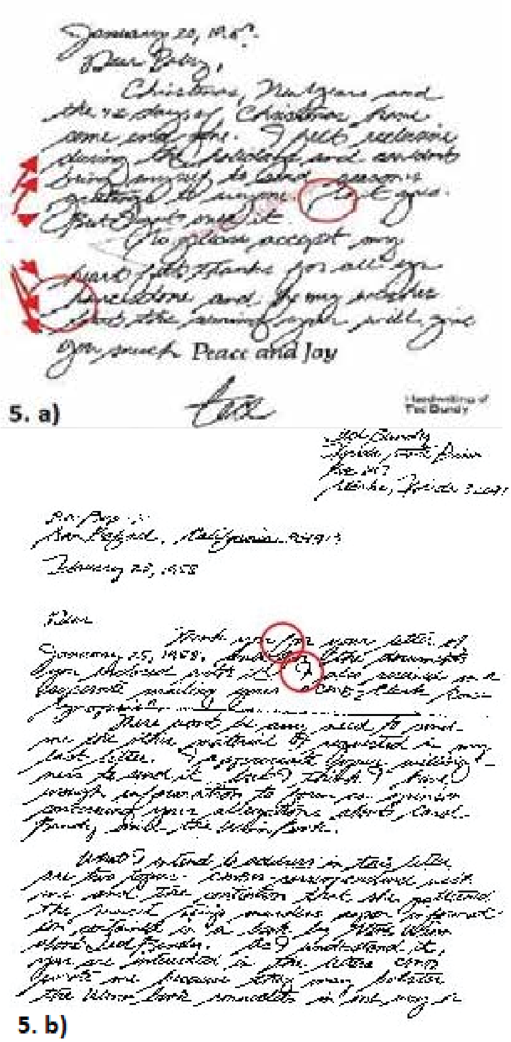

Peace and Joy
5. a)
Handwriting of Ted Bundy
5. b)

Figure 5: a) & b) Handwriting sample of “Ted” Bundy [21]

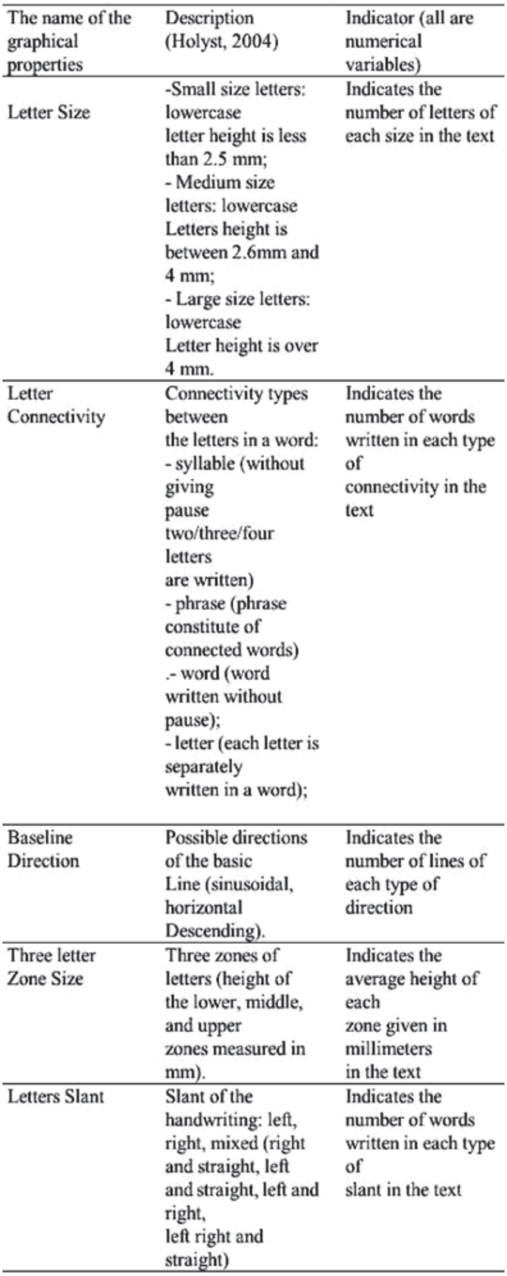
Handwriting features of Ted Bundy represents a graceful, charming and seductive, and creative person who is smart, educated, logical, thorough, determined and resourceful. However, the writing also shows the sign of pride, parsimony, arrogance and intellectual adoration. The presence of inner conflicts and absence of feeling liberty led to the emotional instability, personal wildness, and gives the sign of aggressive, malicious sexuality, willful and brutal tendencies [21, 31].

The above three examples only give a general idea of graphology that can be used as a viable method of investigation for criminal profiling and understanding a criminal’s mind. Therefore, graphologists with respect to specific criminal investigation should be involved in the judicial process prior to the suspect identification or during the interrogations as they can deliver useful information regarding the culprit and the best questioning methods.

4. Handwriting Feature Selection & Proposed Process

Significant features present in handwriting can help to distinguish writers and violent behavior in their personality. Automated approach such as machine learning techniques for the analysis of handwriting has gain a vital role for forensics, biometrics and data science etc. Most of the research predicted personality by analyzing handwriting features but few of them considered the hidden personality traits like signs of aggression and violent nature. A recent research [1] has explored some of the main handwriting features such as baseline, spacing between letters, words and lines, writing speed and pressure, word slant and stroke connectivity to study violence and aggression in an individual personality. These features and their types with examples as explained in the research can be observed in following table [12];

Table 1: Extracted Features [1].



The name of the graphical properties	Description (Holyst, 2004)	Indicator (all are numerical variables)
Letter Size	-Small size letters: lowercase letter height is less than 2.5 mm; - Medium size letters: lowercase Letters height is between 2.6mm and 4 mm; - Large size letters: lowercase Letter height is over 4 mm.	Indicates the number of letters of each size in the text
Letter Connectivity	Connectivity types between the letters in a word: - syllable (without giving pause two/three/four letters are written) - phrase (phrase constitute of connected words) .- word (word written without pause); - letter (each letter is separately written in a word);	Indicates the number of words written in each type of connectivity in the text
Baseline Direction	Possible directions of the basic Line (sinusoidal, horizontal Descending).	Indicates the number of lines of each type of direction
Three letter Zone Size	Three zones of letters (height of the lower, middle, and upper zones measured in mm).	Indicates the average height of each zone given in millimeters in the text
Letters Slant	Slant of the handwriting: left, right, mixed (right and straight, left and straight, left and right, left right and straight)	Indicates the number of words written in each type of slant in the text

4.1 Image Feature Extraction Techniques

Image analysis is required to extract the desired features from handwriting samples that predict the violent and aggressive behavior. It involves the conversion of features and objects into image data and then quantitative information followed by some basic steps. Multiple image processing steps are required for the extraction of meaningful quantitative information as developed images are noisy, composite and artifact –laden as outlined in following steps;

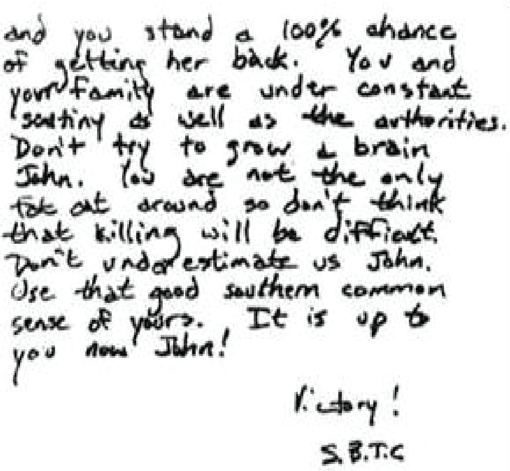
- Normalization: The first step is to read the digital image by removing or correcting imperfections such as noise formation due to low level light, uneven illumination and defective pixels etc. acquired during image acquisition steps. The features of interest in the image is highlighted through enhancing the image contrast by using various spatial filters and image transformation techniques. Second step also known as pre-processing step involves conversion of image to gray scale that follows bitwise not process for converting black pixels to white ones.
- Noise Reduction: Three filters are used to remove noise and unwanted points or lines disconnected strokes from the scanned image that cause distortion and thresh holding operation is performed to remove the blur effect from the image. For example, Boolean filters are preferred over other morphological methods to remove the textured background as they provide better processing time and accuracy. Similarly, edge sharpening is removed by using ramp width reduction filter and

image contrast is adjusted by using Adaptive un-sharp masking as a common method.

- **Contour Smoothing:** Optimal local weighted averaging method is preferred for reducing possible errors by filtering out unwanted glitches and strokes in handwriting sample because this method provides accurate estimation of essential contour point positions, deviation angles and tangent slopes for handwriting analysis [1]. This step also identifies the contours and medium handwriting should have alphabets between 2.5 to 3.5mm. Contours height between 5 and 50 were selected as standard for all images. Hence, average height of letters present in image is retrieved by calculating height of each contour [25].
- **Compression:** Compression techniques such as global threshold is used to convert the color images to binary as this provides better performance and regulated by modified histogram. As handwriting analysis requires only handwritten sample, so white space thinning method is used as it is fast and simple.
- **Row Segmentation:** Vertical Projection Profile (VPP) method is used for row segmentation because it gives best classification accuracy. Sum of pixels for each row in the image were analyzed by calculating highest pixel sum and considering pixel sum lower than 7.5% of threshold value which was obtained by using trial and error method. Leave-one-out approach was used for conducting test on handwriting samples with average accuracy of 97.2% for correct row segmentation. This step was followed to make a corresponding bounding rectangle in each row of the handwriting script.
- **Spacing Between Lines Feature:** Bounding rectangles determine the amount of overlap between two succeeding rows by delimiting each rows. The rows are considered evenly spaced if the overlap value is lower than 12% of the sum of both row bounding rectangles and crowded if it is higher than 12% [1].
- **Baseline Features:** Baseline features for each row can be determined by method discussed in [32] that studies the pixel density of each segmented row rectangle which is rotated within the angle thresholds of -30; +30. This process is repeated to obtain a horizontally centered highest pixel density. This method is broadly used for extraction of baseline features because this method as compared to other state-of-the-art methods gives faster convergence and higher classification accuracy. Rotation within -6; +6 angle threshold considered to give align highest pixel density, leveled and ascending baseline within -31; -6, and descending baseline within +6; +31 [1].

4.2. Handwriting Sample's Simulation

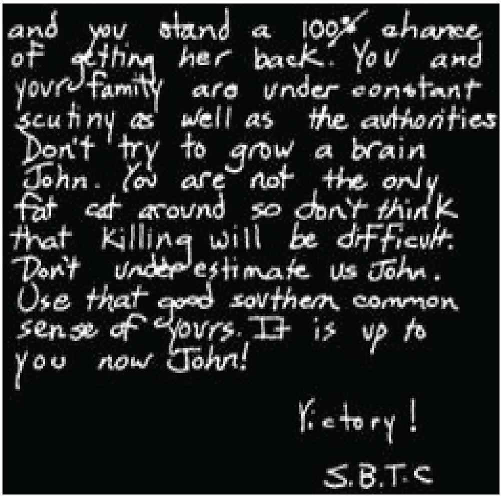
Proposing the basic idea of handwriting analysis can facilitate the process of identifying and recognizing hidden signs of aggression and violent behavior in an individual handwriting which are associated with some types of personality disorders or psychopathy. Different researches have been conducted to study one of the psychopathy by speech samples and social media service analysis [27, 33]. However, forensic psychologists and graphologists evaluate the psychopathic behavior and handwriting samples through tedious processes. Considering sensitivity and shortage of data, publically available handwriting samples have been collected from authenticated graphologists who have handwriting samples of serial killers and anti-social people [34]. It involves reading and pre-processing of original image as shown in figure 6, follows by grey-scaling, applying threshold and high contrast to the image as shown in following figure 7;



and you stand a 100% chance
of getting her back. You and
your family are under constant
scutiny as well as the authorities.
Don't try to grow a brain
John. You are not the only
fat cat around so don't think
that killing will be difficult.
Don't underestimate us John.
Use that good southern common
sense of yours. It is up to
you now John!

Victory!
S.B.T.C

Figure 6: Original Image [1].

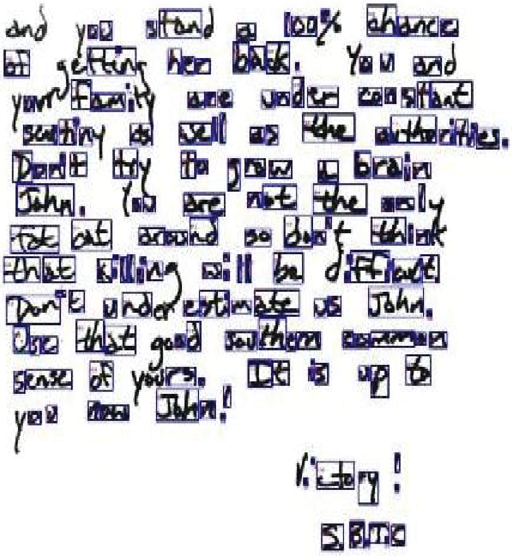


and you stand a 100% chance
of getting her back. You and
your family are under constant
scutiny as well as the authorities
Don't try to grow a brain
John. You are not the only
fat cat around so don't think
that killing will be difficult.
Don't underestimate us John.
Use that good southern common
sense of yours. It is up to
you now John!

Victory!
S.B.T.C

Figure 7: Image after pre-processing [1].

Polygonization is used as the main technique for finding the baseline slant and formed the closed polygon around one of the lines that further coordinates to form the slop. Threshold algorithm is used to calculate writing pressure by converting the image into a binary one. Grey level threshold is used to determine a particular threshold that maps the eyelevel pixel values present in the image. Pixel value is mapped to pure black (foreground) if it is below the set threshold and to pure white (background) if it is above the threshold. The threshold value calculates the writing pressure e.g. light pressure was indicated by higher threshold. The number of the black pixels counts the number of foreground pixels and indicates the writing size, pressure and stroke thickness. The contours of texts plotted on the image as rectangles are detected from the image that intern calculates size of the letters as shown in figure 8;

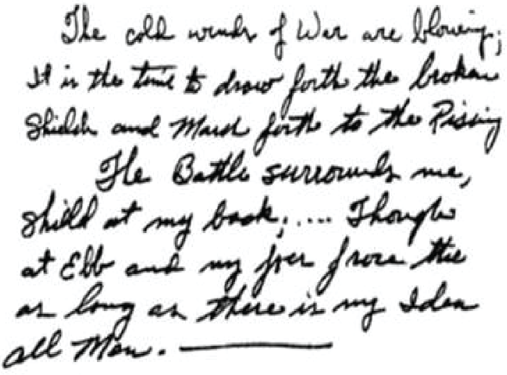


and you stand a 100% chance
of getting her back. You and
your family are under constant
scutiny as well as the authorities.
Don't try to grow a brain
John. You are not the only
fat cat around so don't think
that killing will be difficult.
Don't underestimate us John.
Use that good southern common
sense of yours. It is up to
you now John!

Victory!
S.B.T.C

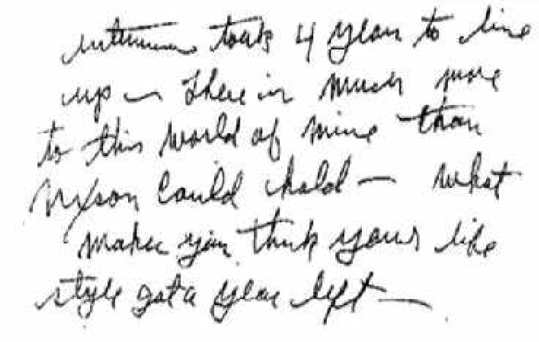
Figure 8: Image after Contour plot [1].

Height of words is calculated when these contours of texts are highlighted and gives an average height of all the contours. Features like zones including upper, middle and lower zones, lowercase letter size and connectivity, leftward and mixed slant, loops in ovals and writing pressure were extracted from following processed images of violent and normal handwritten [1] samples;



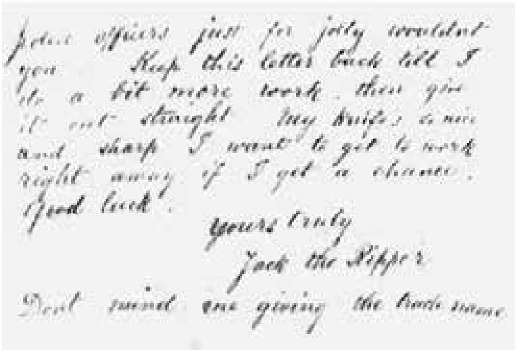
The cold winds of War are blowing;
It is the time to draw forth the broken
Shield and March forth to the Rising
The Battle surrounds me,
shield at my back;.... Though
at Ebb and my foes from the
as long as there is my Idea
all Man. ——

Figure 9: Violent handwriting sample image



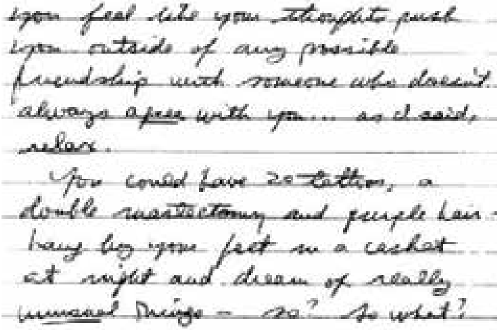
Autumn took 4 years to line
up — there is much more
to this world of mine — than
anyone could behold — what
makes you think your life
style got a year left —

Figure 10: Violent handwriting sample [1]



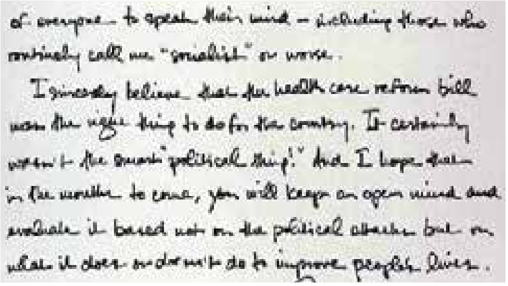
your officers just for jolly wouldn't
you. Keep this letter back till I
do a bit more work, then give
it out straight. My knife's so nice
and sharp I want to get to work
right away if I get a chance.
Good luck.
yours truly
Jack the Ripper
Dont mind me giving the trade name

Figure 11: Violent handwriting [1].



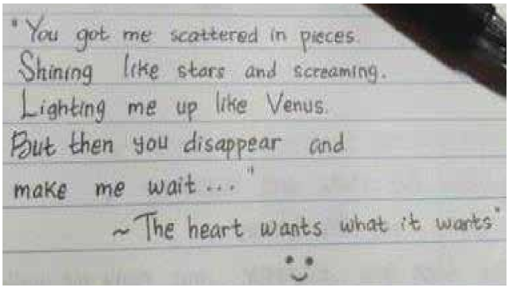
you feel like you thoughts push
you outside of any possible
friendship with someone who doesn't
always agree with you... as I said,
relax.
You could have 20 tattoos, a
double mastectomy and people hair
hang by your feet in a casket
at night and dream of really
unusual things — so? So what?

Figure 12: Violent handwriting [1].



of everyone to speak their mind — including those who
routinely call me "socialist" or worse.
I sincerely believe that the health care reform bill
was the right thing to do for the country. It certainly
wasn't the "smart" political thing!" And I hope that
in the months to come, you will keep an open mind and
evaluate it based not on the political attacks but on
what it does or doesn't do to improve people's lives.

Figure 13: Normal handwriting sample [1].



"You got me scattered in pieces.
Shining like stars and screaming.
Lighting me up like Venus.
But then you disappear and
make me wait..."
~The heart wants what it wants"
:)

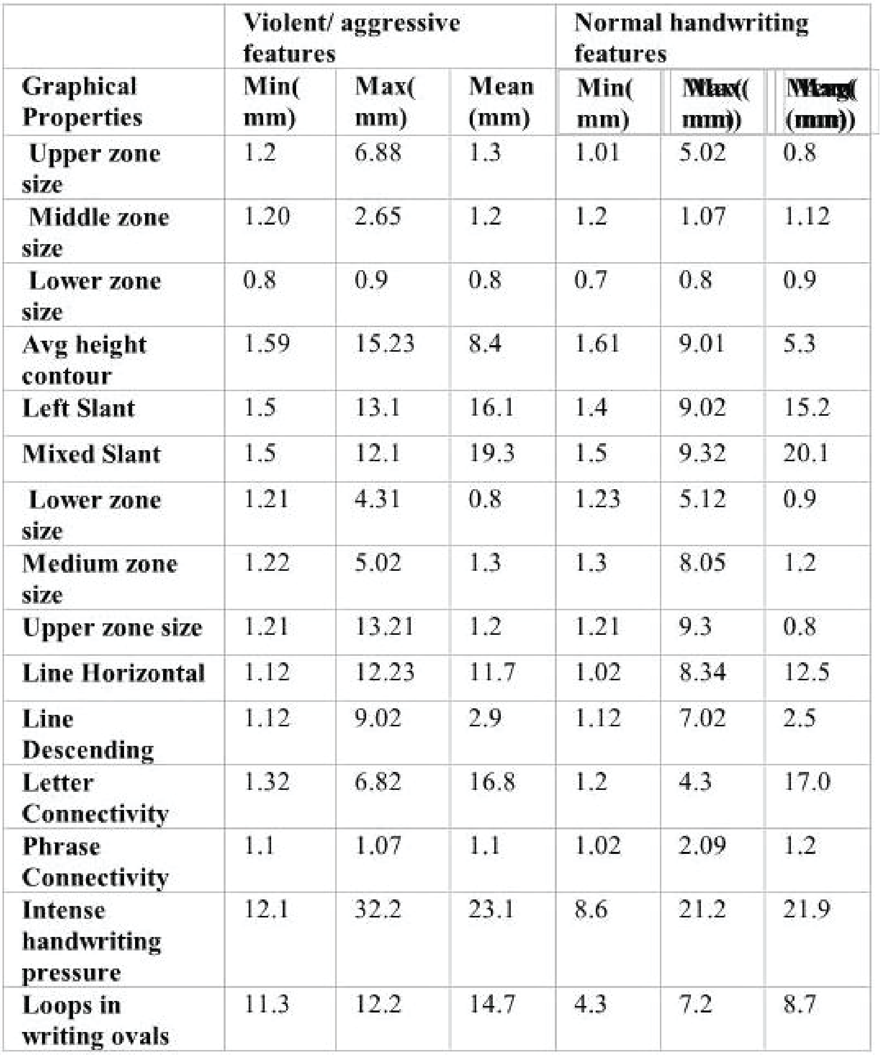
Figure 14: Normal handwriting sample [1]

4.2.1. Simulation Results

Above images are some examples of processed samples of violent and normal handwriting samples that were cleaned and processed to extract graphical features. Results obtained from calculation of various features were formalized [1] as shown in table 2.

The given table shows the comparison between violent/aggressive and normal handwriting features. The processed images of violent handwriting have lower zone with 0.8mm size and upper zone with 6.88mm on average. It is noticed that violent handwriting as compared to an average person, has much larger height of contours with 8.4mm. Some letters were observed to drop below the baseline that indicates the sign of dangerousness as depicted with supporting facts in figure 1 and table 1. Violent people have tendency to make loops in writing ovals as discussed in above literature and depicted maximum value of 14.7mm on higher side in table 2. Greater leftward slants were observed in some of the handwriting samples presenting distorted handwriting with signs of anxiety and violence [25, 35]. Some of the handwriting samples shown intense writing pressure with maximum value of 23.1mm that supports and predicts sign of dangerousness presented [1] in figure 1.

Table 2: Comparison of features extracted in handwritten image [1].

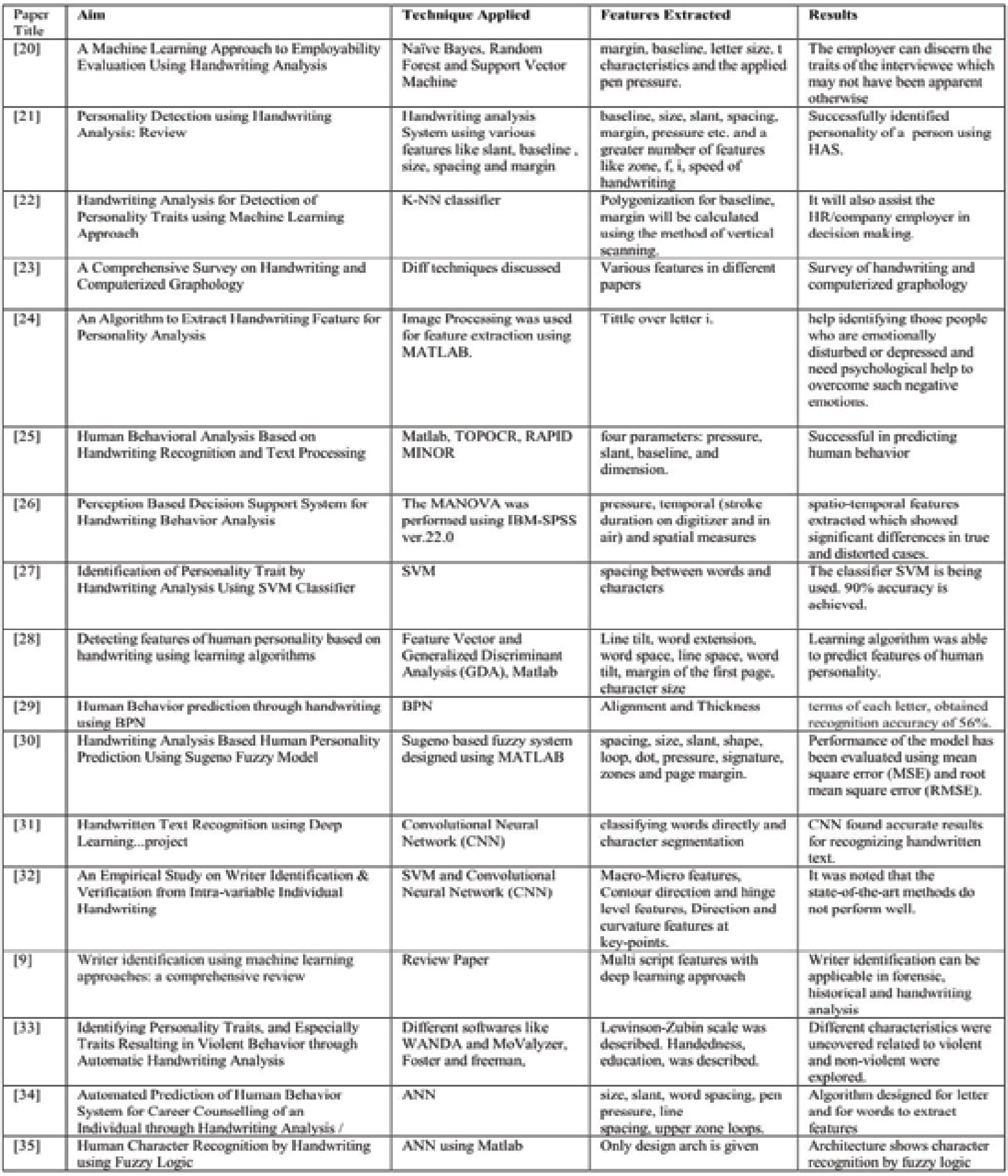


	Violent/ aggressive features			Normal handwriting features		
Graphical Properties	**Min(mm)**	**Max(mm)**	**Mean (mm)**	**Min(mm)**	**Max(mm)**	**Mean (mm)**
Upper zone size	1.2	6.88	1.3	1.01	5.02	0.8
Middle zone size	1.20	2.65	1.2	1.2	1.07	1.12
Lower zone size	0.8	0.9	0.8	0.7	0.8	0.9
Avg height contour	1.59	15.23	8.4	1.61	9.01	5.3
Left Slant	1.5	13.1	16.1	1.4	9.02	15.2
Mixed Slant	1.5	12.1	19.3	1.5	9.32	20.1
Lower zone size	1.21	4.31	0.8	1.23	5.12	0.9
Medium zone size	1.22	5.02	1.3	1.3	8.05	1.2
Upper zone size	1.21	13.21	1.2	1.21	9.3	0.8
Line Horizontal	1.12	12.23	11.7	1.02	8.34	12.5
Line Descending	1.12	9.02	2.9	1.12	7.02	2.5
Letter Connectivity	1.32	6.82	16.8	1.2	4.3	17.0
Phrase Connectivity	1.1	1.07	1.1	1.02	2.09	1.2
Intense handwriting pressure	12.1	32.2	23.1	8.6	21.2	21.9
Loops in writing ovals	11.3	12.2	14.7	4.3	7.2	8.7

5. Other Relevant Research Work

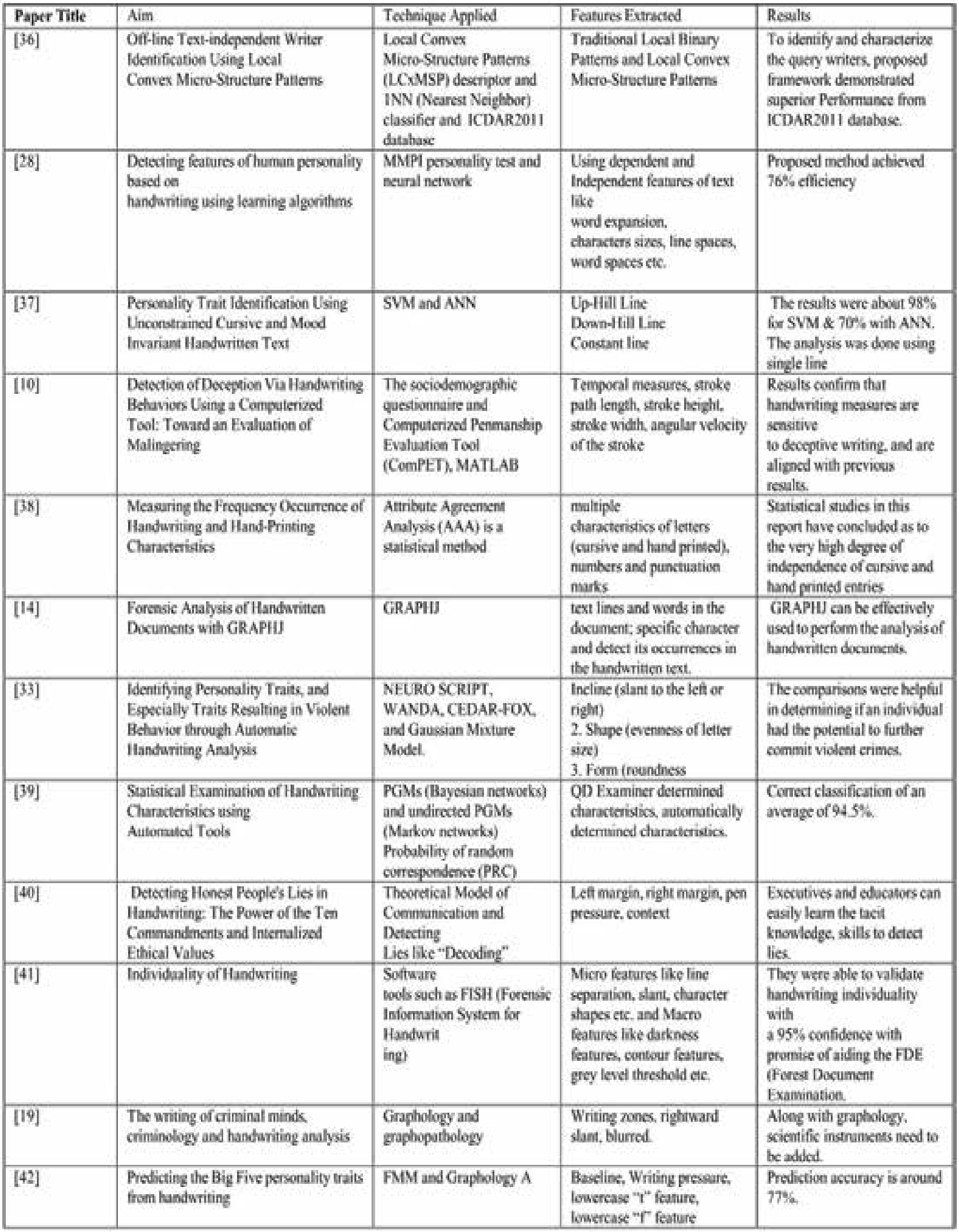
Most of the handwriting analysis carried out by graphologists involves identification of personality traits and behavior through set of questionnaires and its result review. Several state-of-art research and studies on handwriting analysis are presented that describe psychological and personality traits, mental status and behavior of an individual [1] as listed in following table 3 and 4;

Table 3: List of relevant research work [1].



Paper Title	Aim	Technique Applied	Features Extracted	Results
[20]	A Machine Learning Approach to Employability Evaluation Using Handwriting Analysis	Naïve Bayes, Random Forest and Support Vector Machine	margin, baseline, letter size, t characteristics and the applied pen pressure.	The employer can discern the traits of the interviewee which may not have been apparent otherwise
[21]	Personality Detection using Handwriting Analysis: Review	Handwriting analysis System using various features like slant, baseline , size, spacing and margin	baseline, size, slant, spacing, margin, pressure etc. and a greater number of features like zone, f, i, speed of handwriting	Successfully identified personality of a person using HAS.
[22]	Handwriting Analysis for Detection of Personality Traits using Machine Learning Approach	K-NN classifier	Polygonization for baseline, margin will be calculated using the method of vertical scanning.	It will also assist the HR/company employer in decision making.
[23]	A Comprehensive Survey on Handwriting and Computerized Graphology	Diff techniques discussed	Various features in different papers	Survey of handwriting and computerized graphology
[24]	An Algorithm to Extract Handwriting Feature for Personality Analysis	Image Processing was used for feature extraction using MATLAB.	Tittle over letter i.	help identifying those people who are emotionally disturbed or depressed and need psychological help to overcome such negative emotions.
[25]	Human Behavioral Analysis Based on Handwriting Recognition and Text Processing	Matlab, TOPOCR, RAPID MINOR	four parameters: pressure, slant, baseline, and dimension.	Successful in predicting human behavior
[26]	Perception Based Decision Support System for Handwriting Behavior Analysis	The MANOVA was performed using IBM-SPSS ver.22.0	pressure, temporal (stroke duration on digitizer and in air) and spatial measures	spatio-temporal features extracted which showed significant differences in true and distorted cases.
[27]	Identification of Personality Trait by Handwriting Analysis Using SVM Classifier	SVM	spacing between words and characters	The classifier SVM is being used. 90% accuracy is achieved.
[28]	Detecting features of human personality based on handwriting using learning algorithms	Feature Vector and Generalized Discriminant Analysis (GDA), Matlab	Line tilt, word extension, word space, line space, word tilt, margin of the first page, character size	Learning algorithm was able to predict features of human personality.
[29]	Human Behavior prediction through handwriting using BPN	BPN	Alignment and Thickness	terms of each letter, obtained recognition accuracy of 56%.
[30]	Handwriting Analysis Based Human Personality Prediction Using Sugeno Fuzzy Model	Sugeno based fuzzy system designed using MATLAB	spacing, size, slant, shape, loop, dot, pressure, signature, zones and page margin.	Performance of the model has been evaluated using mean square error (MSE) and root mean square error (RMSE).
[31]	Handwritten Text Recognition using Deep Learning...project	Convolutional Neural Network (CNN)	classifying words directly and character segmentation	CNN found accurate results for recognizing handwritten text.
[32]	An Empirical Study on Writer Identification & Verification from Intra-variable Individual Handwriting	SVM and Convolutional Neural Network (CNN)	Macro-Micro features, Contour direction and hinge level features, Direction and curvature features at key-points.	It was noted that the state-of-the-art methods do not perform well.
[9]	Writer identification using machine learning approaches: a comprehensive review	Review Paper	Multi script features with deep learning approach	Writer identification can be applicable in forensic, historical and handwriting analysis
[33]	Identifying Personality Traits, and Especially Traits Resulting in Violent Behavior through Automatic Handwriting Analysis	Different softwares like WANDA and MoValyzer, Foster and freeman,	Lewinson-Zubin scale was described. Handedness, education, was described.	Different characteristics were uncovered related to violent and non-violent were explored.
[34]	Automated Prediction of Human Behavior System for Career Counselling of an Individual through Handwriting Analysis /	ANN	size, slant, word spacing, pen pressure, line spacing, upper zone loops.	Algorithm designed for letter and for words to extract features
[35]	Human Character Recognition by Handwriting using Fuzzy Logic	ANN using Matlab	Only design arch is given	Architecture shows character recognition by fuzzy logic

Table 4: List of relevant research work [1].



Paper Title	Aim	Technique Applied	Features Extracted	Results
[36]	Off-line Text-independent Writer Identification Using Local Convex Micro-Structure Patterns	Local Convex Micro-Structure Patterns (LCxMSP) descriptor and 1NN (Nearest Neighbor) classifier and ICDAR2011 database	Traditional Local Binary Patterns and Local Convex Micro-Structure Patterns	To identify and characterize the query writers, proposed framework demonstrated superior Performance from ICDAR2011 database.
[28]	Detecting features of human personality based on handwriting using learning algorithms	MMPI personality test and neural network	Using dependent and Independent features of text like word expansion, characters sizes, line spaces, word spaces etc.	Proposed method achieved 76% efficiency
[37]	Personality Trait Identification Using Unconstrained Cursive and Mood Invariant Handwritten Text	SVM and ANN	Up-Hill Line Down-Hill Line Constant line	The results were about 98% for SVM & 70% with ANN. The analysis was done using single line
[10]	Detection of Deception Via Handwriting Behaviors Using a Computerized Tool: Toward an Evaluation of Malingering	The sociodemographic questionnaire and Computerized Penmanship Evaluation Tool (ComPET), MATLAB	Temporal measures, stroke path length, stroke height, stroke width, angular velocity of the stroke	Results confirm that handwriting measures are sensitive to deceptive writing, and are aligned with previous results.
[38]	Measuring the Frequency Occurrence of Handwriting and Hand-Printing Characteristics	Attribute Agreement Analysis (AAA) is a statistical method	multiple characteristics of letters (cursive and hand printed), numbers and punctuation marks	Statistical studies in this report have concluded as to the very high degree of independence of cursive and hand printed entries
[14]	Forensic Analysis of Handwritten Documents with GRAPHJ	GRAPHJ	text lines and words in the document; specific character and detect its occurrences in the handwritten text.	GRAPHJ can be effectively used to perform the analysis of handwritten documents.
[33]	Identifying Personality Traits, and Especially Traits Resulting in Violent Behavior through Automatic Handwriting Analysis	NEURO SCRIPT, WANDA, CEDAR-FOX, and Gaussian Mixture Model.	Incline (slant to the left or right) 2. Shape (evenness of letter size) 3. Form (roundness	The comparisons were helpful in determining if an individual had the potential to further commit violent crimes.
[39]	Statistical Examination of Handwriting Characteristics using Automated Tools	PGMs (Bayesian networks) and undirected PGMs (Markov networks) Probability of random correspondence (PRC)	QD Examiner determined characteristics, automatically determined characteristics.	Correct classification of an average of 94.5%.
[40]	Detecting Honest People's Lies in Handwriting: The Power of the Ten Commandments and Internalized Ethical Values	Theoretical Model of Communication and Detecting Lies like "Decoding"	Left margin, right margin, pen pressure, context	Executives and educators can easily learn the tacit knowledge, skills to detect lies.
[41]	Individuality of Handwriting	Software tools such as FISH (Forensic Information System for Handwrit ing)	Micro features like line separation, slant, character shapes etc. and Macro features like darkness features, contour features, grey level threshold etc.	They were able to validate handwriting individuality with a 95% confidence with promise of aiding the FDE (Forest Document Examination.
[19]	The writing of criminal minds, criminology and handwriting analysis	Graphology and graphopathology	Writing zones, rightward slant, blurred.	Along with graphology, scientific instruments need to be added.
[42]	Predicting the Big Five personality traits from handwriting	FMM and Graphology A	Baseline, Writing pressure, lowercase "t" feature, lowercase "f" feature	Prediction accuracy is around 77%.

6. Conclusion

This paper reviews the signs of dangerousness and violent tendencies reflected in one's personality and its identification through handwriting analysis. Certain features like presence of loops, connectivity, space and zone size, slant and baseline direction, speed and pressure obtained from handwriting samples were studied to identify the red flags. It is highly challenging to identify violence and aggressive behavior from handwriting due to vast areas of graphology. It is very difficult but more interesting for graphologists to solve crimes because of the influence of their actions. Graphologist's opinion should be considered during an investigation to avoid prolonged, delayed and a slow interrogation process that mainly lacks the correlation between strategies and personality of the target suspect or victim or witness. One should know the limits and errors of this instrument resulted from insufficient knowledge of the specialist or illegal management of given data, however, this method is inspired scientifically and its remarkable results strongly recommend its usage in complex criminal investigation. It is authoritative to promote this scientific method with its advantages on a wider scale in professional as well as in academic environment. Further research studies and development can be accomplished by discovering wide range of graphical structures and patterns, perfecting programs and training new specialists. Hence, handwriting can become a valuable tool to identify violent signs in one's personality.

7. Referencing

[1] D. Jain, Dr. S. Arora, Dr. C.K. Jha. (2020, August). "Identification of violent behavior using Handwriting." International Journal of Advanced Trends in Computer Science and Engineering. vol. 9(4), pp. 6238 – 6250.

[2] India Today. Ryan school murder case [Online] vol. 8, no. 9.

[3] Outlook Magzin. (2007, January). Devil in flesh [Online].

[6] R. Hare. (2013, January). Psychopathy Check List," vol. 53, no. 9.

[5] D. S. Kowal, P. K. Gupta. (2021, March). "Handwriting analysis: A psychopathic viewpoint." The International Journal of Indian Psychology. Vol. 9(1).

[6] S. Lambe, C. H. Giachritsis, E. Garner, J. Walker (2018). "The Role of Narcissism in Aggression and Violence: A Systematic Review." Trauma, Violence, Abus. vol. 19(2), pp. 209–230.

[7] D. Gallardo-Pujol, N. Pereda. (2013). "Person-environment transactions: persionality traits moderate and mediate the effects." Personal. Ment. Health. vol. 7, pp. 102–113.

[8] R. Howard. (2015). "Personality disorders and violence: what is the link." Borderline Personal. Disord. Emot. Dysregulation. vol. 2(1), pp. 1–11.

[9] R. Yu, J. R. Geddes, S. Fazel. (2012). "Personality disorders, violence, and antisocial behavior: A systematic review and meta-regresion analysis." J. Pers. Disord. vol. 26(5), pp. 775–792.

[10] A. Rehman, S. Naz, M. I. Razzak. (2019,

April). “Writer identification using machine learning approaches: a comprehensive review.” Multimed. Tools Appl. vol. 78(8), pp. 10889–10931.

[11] G. Luria, A. Kahana, S. Rosenblum. (2014). “Detection of Deception Via Handwriting Behaviors Using a Computerized Tool: Toward an Evaluation of Malingering.” Cognit. Comput. vol. 6(4), pp. 849–855.

[12] K. Amend, M. S. Ruiz. 91980). Handwriting Analysis:The Complete Basic Book [Online]. Available: https://www.amazon.com/Handwriting-Analysis-Complete-Basic Book/dp/0878 77050X

[13] D. J. Antony. (2008). “Personality Profile Through Handwriting Analysis.” pp. 1–118.

[14] R. Plamondon. (2011). “Neuromuscular Studies of Handwriting Generation and Representation.” pp. 261–261.

[15] L. Guarnera, G. M. Farinella, A. Furnari, A. Salici, C. Ciampini, V. Matranga, et al., (2018). “Forensic analysis of handwritten documents with GRAPHJ.” J. Electron. Imaging. vol. 27(05), p. 1.

[16] G. H. Singh, R. J. Mehta, N. D. Shah, R. Y. Mehta, et al., (2016). “Handwriting Change as a Psychiatric Symptom.” Int. J. Med. Dent. Sci. vol. 5(1), p. 1075.

[17] H. Jantan, A. Z. M. Jamil. (2019). “Association Rule Mining Based Crime Analysis using Apriori Algorithm,” International Journal of Advanced Trends in Computer Science and Engineering. Vol 8(1.5). Available: https://doi.org/10.30534/ijatcse/2019/0581.5201.

[18] B. Identification, C. N. Networks, D. Examination, and Q. Documents, Behavioral Identification based on Heterogeneous Handwritten Aided by Deep Learning on a Novel Standard Dataset.

[19] C. Iulia. (1962). “The Writings of criminal minds criminilogy and handwriting analysis.” Crineanu Iulia forensic expert, România. vol. 1(4), pp. 163–175.

[20] L. Guarnera, G. M. Farinella, A. Furnari, A. Salici, C. Ciampini, V. Matranga, et al., (2017). “GRAPHJ: A Forensics Tool for Handwriting Analysis.” Lect. Notes Comput. Sci. vol. 10485, pp. 591–601.

[21] C. Iulia. (1962). “The Writings of criminal minds criminilogy and handwriting analysis.” Crineanu Iulia forensic expert, România. vol. 1(4), pp. 163–175.

[22] H. N. Champa, K. R. A. Kumar. “Automated human behavior prediction through handwriting analysis,” Proc. - 1st Int. Conf. Integr. Intell. Comput. ICIIC, 2010, pp. 160–165.

[23] R. N. M. Ron Morris. (2020, November). Forensic Handwriting Identification: Fundamental Concepts and Principles[Online]. Available: https://www.elsevier.com/books/forensic-handwriting-identification/morris/978-0-12-409602-8.

[24] C. Rush. (2019, December). Forensic Document Examination Fraudulent

Documents [Online]. Available: https://www.coursehero.com/file/65825737/Handwritting-Fraud-Doc9-2016pdf/

[25] I. Marcuse. (1971). Guide to Personality Through Your Handwriting Paperback [Online]. Available: https://www.amazon.com/Guide-Perso-nality-Through-Your-Handwriting/dp/B0084VKVH4.

[26] American Psychiatric Association. (2013). Diagnostic and statistical manual of mental disorders (DSM-5®). American Psychiatric Pub.

[27] D. Jain, S. Arora, C. K. Jha. (2019). “Diagnosis of Psychopathic Personality Disorder with Speech Patterns.” Commun. Comput. Inf. Sci. vol. 1075, pp. 411–421.

[28] A. McNichol. “Handwriting Analysis. Putting It to Work for You,” Ed. Jaico Publishing House, 2003.

[29] Anna Koren. Handwriting analysis of serial killers [Online]. Anna Koren Graphology Center Ltd. Available: http://www.annakoren.com/handwriting-analysis-of-serial-killers.html

[30] A. Taylor. (2019). Psycho Killers [Online]. Available: https://www.ranker.com/list/serial-killer-handwriting/april-a-taylor

[31] A. Howard. (2018). Can handwriting show serial killer tendencies? [Online]. Available: https://jhvonline.com/canhandwriting-show-serial-killer-tendencies-p2 4055-89.htm

[32] H. E. S. Said, K. D. Baker, T. N. Tan. (2002). “Personal identification based on handwriting.” vol. 33, pp. 1761–1764.

[33] U. Hani, H. Zaki, R. Ibrahim, S. A. Halim. (2019). "A Social Media Services Analysis." International Journal of Advanced Trends in Computer Science and Engineering. Vol 8(1.6).

[34] H. Y. Kueh, E. Marco, M. Springer, S. Sivaramakrishnan, D. Images. (2008). “Image analysis for biology - Cross-correlation.” pp. 1–52.

[35] P. E. CRONJE, “thesis,” 2009

Taseer Suleman *et al.LGU (IJECI)* 2021

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

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 5 issue 2 Year 2021

A Survey On Web Phishing Detection Techniques: A Taxonomy-based Approach

Taseer Suleman
taseer.suleman11@gmail.com
University of Management and Technology

Abstract:

The primary goal of website phishing is to obtain secret information i.e. passwords, account numbers, credit card details, etc. Web-phishing is used to deceive users, normally carried out through sending links using spoofed emails, instant messages etc. However, web-phishing detection is a challenging task. A number of techniques and mechanisms has been proposed for the detection of web-phishing. The aim of this study is to analyze different web-phishing detection techniques. Web-phishing techniques are characterized into machine-learning (ML) based, Heuristics-based, Blacklist/whitelist based and visual-based. A comparative analysis of these aforementioned categories has been done in this research based on their detection accuracy, performance, usability, and scalability. The research also identifies the advantages and limitations of web-phishing detection techniques.

Keywords: Web-phishing, Machine-Learning based, Heuristics-based, Blacklist-based

1. Introduction

Web-phishing is an online crime for obtaining personal information like banking details, credit card numbers, and social security numbers. Phishing was actually started in 1995 with America Online (AOL) users [1]. Attackers lure users by sending spoofed emails to them. Rogue links can also be sent through online social media and other messaging services [2]. Victims are redirected to the illegitimate websites when they click on those rogue links. These websites are usually the clone of a legitimate website. A careless user can give personal details on these rogue websites without checking the webpage legitimacy or Uniform Resource Locator (URL). Hackers then use these details for malicious purpose. The choice of victim and the amount of benefit are important parameters in the web-phishing attack. Web-phishing strategies include SQL injection, Tab-nabbing, Typo-Squatting, content-injection, malware-based and DNS-based attack [3]. Statistics from Anti Phishing Working Group (APWG) 2018 report shows the increase of web-phishing attacks in the previous year 2018. The report has also shown that most of these fake websites are using Hyper Text Transfer Protocol – Secure (HTTPS) services. The use of HTTPs hosted websites is to gain the trust of victims.

Many web-phishing detection solutions are proposed that can be categorized into Heuristics-based, Blacklist/Whitelist based, Machine learning based and Visuality-similarity based [4]. In this article, various techniques and mechanisms on web-phishing detection solutions are discussed. These techniques and mechanism are generally revolved around the aforementioned categories. In addition, a comparison analysis has been done to evaluate more about web-phishing detection techniques. It would help researchers in understanding the advantages and limitation of these anti-phishing techniques. In the end, we concluded our research based on the detailed analysis of the web-phishing detection techniques. In Figure 1, the taxonomy of web phishing and its detection is given.

The rest of the paper is organized as follows: In the next section, the web-phishing life cycle is discussed. In section III, phishing statistics are shown according to most recent research reports. Section IV highlights web-phishing strategies. In Section V, a detailed analysis of web-phishing detection techniques is given. Section VI concludes our research.

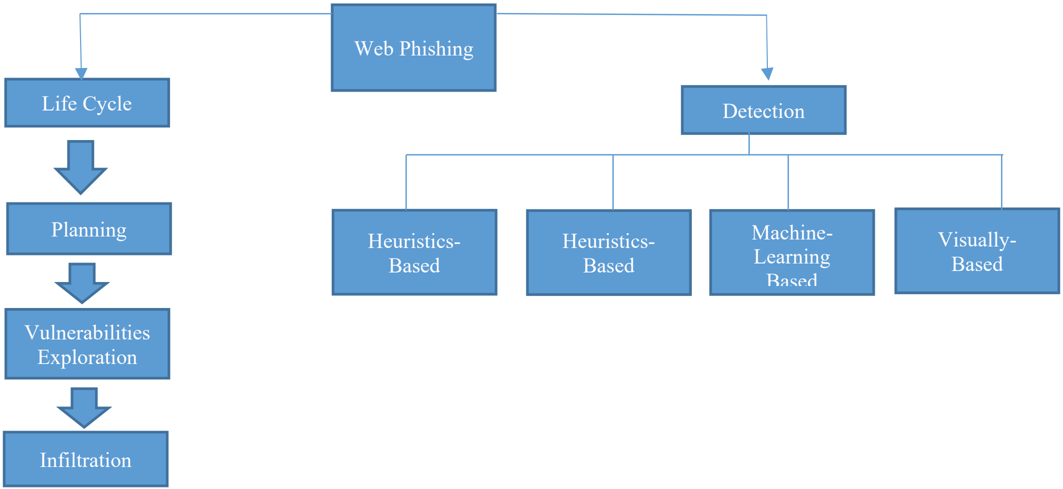


Figure 1. Taxonomy of web-phishing and its detection

2. Web-Phishing Life Cycle

A typical web-phishing life cycle comprises of few stages like planning and setup, vulnerabilities identification, infiltration and information accumulation [5]. We go through these stages in detail.

A. Planning and Setup

In the first stage, the phisher determines the objective association, an individual or a country to be targeted for malicious purpose. They uncover sensitive information with respect to their objective and its system. Normally phishing starts by sending spoofed emails or messages to the victims [6]. Victims are supposed to send required information via replying to the email. However, most of the users do not reveal their information through email. Another phishing technique can be adopted through the creation of phishing websites.

B. Finding system vulnerabilities

The target, purpose, and motivation of web-phishing is well defined. Web-phishing carried out by utilizing browsers vulnerabilities, web link manipulation, malicious use of scripting languages, spoofing website text and images.

C. Break-In or Infiltration

At this stage, the attacker penetrates into the system, takes control of the system, and perform malicious activities. This penetration may be caused through a vulnerability in the victim's system.

D. Information Accumulation

After the successful infiltration, the attacker does the information collection. Information may contain passwords, user identity number, contact lists, private images, and credit card information. The whole web-phishing life cycle is shown in Figure 2. An active attacker sends a link of the fake webpage via email to the victim. The victim is redirected towards the fakewebsite when click on this link. This fake website seems to be original to the victim. In this way, the victim gets compromised.

3. Web-phishing Statistics

According to the Anti-Phishing Working Group (APWG) 2018 report, there is an increase in web-phishing attacks. In September, 53,546 unique phishing websites detected which show a drastic increase than the month of July and August [7]. The APWG report also states the increase in the usage of phishing websites hosted on Hyper Text Transfer Protocol –Secure (HTTPS). Figure 3 shows an increase in websites using Secure Socket Layer (SSL) services. APWG 3rd quarter 2018 report reveals the most targeted industry is the online payment service. Webmail services and cloud service were also remain affected by phishing

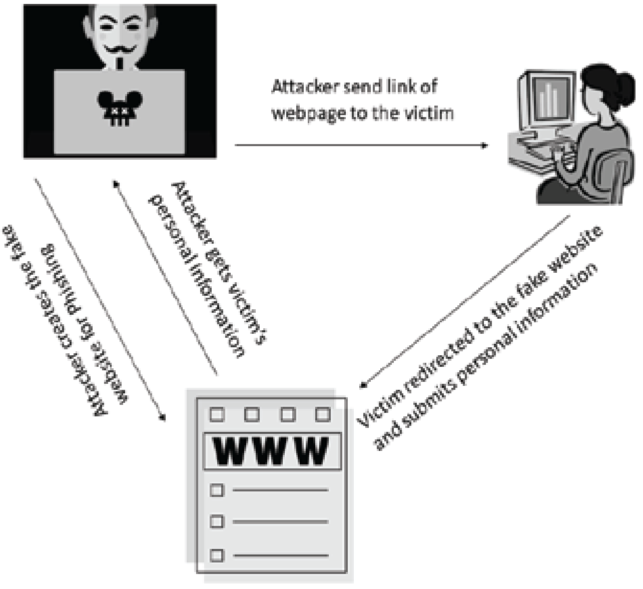

Attacker send link of webpage to the victim
Attacker creates the fake website for Phishing
Attacker gets victim's personal information
Victim redirected to the fake website and submits personal information
WWW

Figure 2. A typical Web-phishing Life Cycle

attacks in 2018. Kaspersky 3rd quarter report [8] figured out that web-phishing involved the compromise of personal data, malicious attacks against the banking sector, universities and job searching platforms. The report also revealed the phishing attacks has been increased against cryptocurrency.

4. Web-phishing Strategies

Attackers used many ways to carry out the website phishing attack. Few are the most common web-phishing strategies.

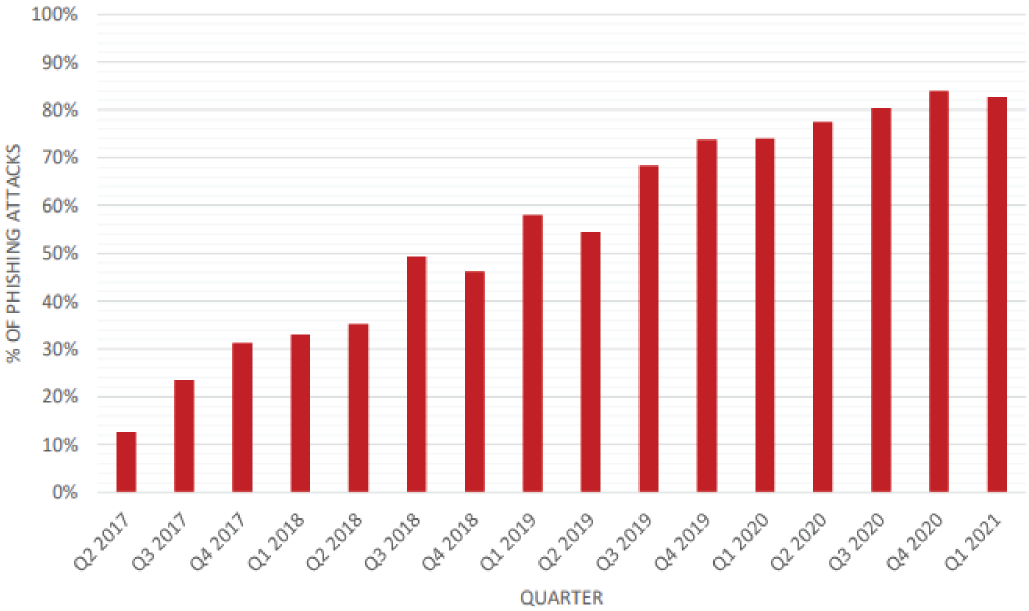


Figure 3. Phishing websites hosted on HTTPS [APWG report]

A. Spear Phishing:

It is a kind of phishing, which targets specific individual or a specific company. This technique is carried out by attackers usually by sending spoofed email or messages to the victims [9].

B. Tabnabbing:

The inactive tab of the browser replaced with the malicious webpage in this website phishing variant [10]. When the user switches back to the tab, it looks legitimate to the user. These tactics used for getting sensitive credentials from the users.

C. URL manipulation:

Website phishing is successfully achieved through the manipulating of URL [11]. Changing, adding, deleting, editing in the URL parts are very common tactics adopted by the attackers. Other techniques include exploiting browsers vulnerabilities, rogue scripts, spoofing websites etc. Figure 4 highlights some of the most common strategies used by the attackers.

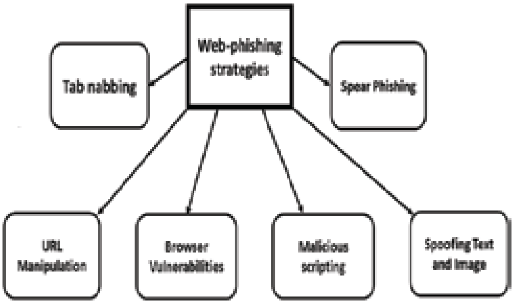


Figure 4. Web-phishing strategies

5. Web-Phishing Detection Techniques

There is a number of mechanisms developed for the detection of phishing websites [12]. These can be categorized into Heuristics-based approaches, Blacklist/Whitelist based mechanisms, Machine-Learning (ML) techniques, and visual similarity based mechanisms [13]. Heuristics-based mechanisms use unique features for the detection of illegitimate websites [14]. Based on these features, algorithms trained up to some threshold for possible detection of wrong websites. Blacklist contains the list of illegal websites as reported by the anti-phishing groups. Google had introduced this blacklist feature in its google chrome browser that checks each URL against the google blacklist [15]. The visual similarity based techniques used to compare the two web pages in terms of their appearance and layout. If it seems to be similar then the system check for URL authenticity and then the fake webpage is marked as phish webpage [16]. Different features of URL are marked for possible detection of phished webpages. Machine-learning algorithms trained on these features, in order to, automate the detection process [17].

In this section, we present a major detection mechanism for phishing websites. A detailed analysis of these mechanisms is discussed, in order to; create deep understanding for the researchers.

A. Heuristics-Based Detection Mechanism:

The heuristic-based approach used different features of the website, in order, to differentiate between phishing and non-phishing webpage. Jaydeep et al. [18] have used some features related to a webpage i.e. URL, source code etc. for phishing webpage detection. Lee et al. [19] proposed a heuristic-based approach for phishing detection using 3000 phishing websites and 3000 non-phishing websites. Their proposed method shows a good response to web-phishing detection.

Gastellier-prevost et al. [20] developed an anti-phishing toolbar named "Phishshark". This tool uses 20 heuristics for the identification of legal and illegal web pages.

Nguyen [21] applied a heuristics-based mechanism using URL features. They used a dataset of 11,660 phishing websites and 5,000 true websites. The proposed technique success rate is 97%.

1) Limitation in using Heuristics based detection mechanism:

Heuristics based mechanisms improved detection accuracy. However, implementation is difficult due to the complexity in the implementation and cost overhead.

B. Blacklist/Whitelist based mechanism:

Li et al. [22] developed an anti-phishing tool for the browser. This tool manages two lists named as white list and blacklist of web pages. When the user clicks on a link containing

URL, it then checked against these two lists. If the URL saved in blacklist the browser prevented from redirecting to that specific webpage.

Krishnamurthy et al. [23] also adopted the mechanism of blacklist/whitelist for possible phishing website detection. At first, the URL is searched in the white list. If no match found, the same URL is compared in the blacklist.

1) Limitation in Blacklist/White list based mechanisms:
Both lists should be updated, in order to, detect new URLs for phishing websites. Moreover, with the regular update on the client side it can create storage issues as well. On the server side, storage can create a delay in accessing the updated list for possible detection of phishing websites.

C. Machine Learning based mechanism:

Abu-Nimeh et al. [24] applied machine-learning algorithms to detect phishing emails. These algorithms are then compared in terms of accuracy in detecting phishing emails.

Le et al. [25] used ML techniques for the classification of websites. The algorithms used URL-based features such as URL length, a special character in URL and domain name etc. This technique improved accuracy but also increased the overhead for processing.

Tan et al. [26] developed ‘PhishWho’, an anti-phishing system, for the detection of possible phishing websites. This system works in three stages starting from the identification of keywords from a website to the decision of website legitimacy. Websites features also play a pivotal role in the identification of phishing websites.

Mohammad et al. [27] developed an anti-phishing system using neural networks for classification. The system used 17 features for classification.

Moghimi and Varjini [28] used Support Vector Machine (SVM) along with Levenshtein Distance for phishing detection. They used 25 features for classification. However, sophisticated website design by phishers remains undetected by the system.

Mohammad et al. [29] used data mining methods, in order to, detect phishing. They performed different data mining algorithms and proved C4.5 to be much better in terms of detection.

Tuan et al. used a dataset of almost 11660 phishing websites for the extraction of features for illegitimate websites [30]. They narrow down these features to six important features with a detection accuracy of 98% approximately.

Feng et al. [31] proposed a method for the detection of phishing web pages using neural networks based classification methods. Their proposed system shows 98% detection accuracy approximately.

Wewei et al. [32] used the results of trained classifiers along with the categorization of phishing websites using hierarchical clustering algorithms. Kausar et al. [33] used a combination of both heuristics mechanism and naïve Bayes classifier, in order to, improve accuracy for phishing detection.

Burber et al. [34] in their research used Natural Language Processing (NLP) for the extraction of URL-based features. They used three machine-learning algorithms for possible detection of phishing websites. The proposed methodology improved detection accuracy.

Jain et al. [35] proposed a client-side solution for the detection of website phishing. They used 2141 phishing websites from PhishTank [36] and applied machine-learning approaches. Rao and Pais [37] used a hybrid methodology for the possible detection of phishing websites. Hybrid approach includes machine-learning approaches and image checking as well.

James et al. [38] connected distinctive sorts of machine learning based arrangement calculations, including Naive Bayes (NB), Support Vector Machine (SVM), Neural Net (NN), Random Forest (RF), IBK relaxed classifier and Decision Tree (J48). Performance of all these aforementioned algorithms is compared and accuracy was determined against each algorithm.

1) Limitation in using machine-learning based detection mechanism:
Machine-learning based detection mechanism contains computational overheads. The slow processing of datasets for algorithms learning increase the latency of website phishing detection. These kinds of techniques are difficult to apply on the client side in terms of browsers extensions or add-ons due to computational cost. In order to improve detection results, a lightweight solution is required. Moreover, a hybrid approach can also be used to make detection accuracy better.

D. Visual similarity based mechanism:
This technique based on the visual features extracted from the websites. These features are later used in the comparison of legitimate website visuals with illegal website visuals.

Chiew et al. [39] proposed a method of extracting a website logo for the detection of phishing websites. They used machine-learning algorithms for possible detection.

Philippe et al. [40] proposed "tab shows", a mechanism that takes the screenshot of the tabs. Whenever a tab is opened again, the screenshot is again saved. Match analysis is performed with the current screenshot and the previous one. It alerts the user in case of any difference in both screenshots.

Lam et al. [41], the author performed a similarity analysis of layout instead of webpage content analysis. In this scheme, image processing techniques are highly involved, in order to, carry out detection.

1) Limitation in visual similarity based mechanism:
These techniques require huge computational resources for processing of images. Complexity computational overhead is always involved in such a mechanism. A lightweight solution might be helping in such a case if that is implemented on the client side.

In Table 1, we have given a comparison of the most common used web-phishing detection techniques, in detail. It would help in the deep understanding of the detection of phishing websites techniques in a comparative analysis. Four major mechanisms are targeted in the analysis that includes Heuristics-based, ML-based, Blacklist/Whitelist based and Visual-based.

Table 1. Comparative analysis of web-phishing detection mechanisms

Detectaion Mechanism	**Technique Used**	**Pros**	**Cons**
Heuristics-Based [18]	Collecting URL Features	The good approach towards detection	Minimal features were used
Heuristics-Based [19]	Using dataset of Phishing and Non-Phishing websites	Improved detection accuracy	The dataset contains fewer samples
Heuristics-Based [20]	Anti-phish toolbar developed using 20 Heuristics	Much heuristics for differentiation	Client-side requires many computational resources.
Blacklist/Whitelist Based [22]	Maintain lists in the browser for anti-phishing	Check both lists for the legal or illegal webpage	Regular list updating issue, client-side list storage issues
Blacklist/Whitelist Based [23]	Improved scheme than in [22], First check whitelist for the legal webpage	Maintains both list i.e. Blacklist and Whitelist	Computational overhead, Processing slow
ML-Based [24]	Applied ML algorithms to detect Phishing emails	Novel approach as emails are a primary source for phishing	Applied more ML algorithms with feature-selection capability might improve results
ML-Based [25]	Applied ML algorithms using URL-based features	Improvement in detection accuracy	Processing overhead, Need more URL-based features to get better results
ML-Based [26]	Worked in 3 stages using website features	Use keywords for matching	Can incorporate more features to improve results
ML-Based [28]	Used SVM along with Levenshtein distance	Used 25 unique feature to detect fake website	A careful-designed website might remain undetected
ML-Based [29]	Used Data-Mining approach	Proved C4.5 to give better accuracy	The small dataset used, the Hybrid approach might produce a better result
ML-Based [30]	Used Dataset of 11660 phishing websites	Applied feature selection (up to 6 features)	Dataset can be increased for a better result.
ML-Based [31]	Neural networks applied	Accuracy detection up to 98%	Much beneficial if applied on a lightweight technique on client-side
ML-Based [33]	A combined approach for detection using heuristics and Naïve Bayes	Improve detection accuracy	More ML algorithms can be applied for performance checking
ML-Based [37]	A hybrid approach of ML algorithms along image-check	Improved detection accuracy	Makes detection processing slow, Computational overhead
ML-Based [38]	Applied six ML algorithms for training	Improved mechanism than in [33]	Can be improved if feature selection algorithms also used
Visuals-Based [39]	Used website logo for detection of phishing webpage	The logo is compared to the real website logo stored in the database	A spoofed website detection is difficult, can be improved incorporating more features
Visuals-Based [41]	Used website layout for detection of websites	Much improved method than [39]	Highly image processing required

6. Conclusions

In this research, we have focused on the web-phishing problem. The aim of this study is to conduct a deep analysis of web-phishing detection techniques. The research focused on these detection techniques in terms of accuracy, performance, scalability, usability, and applicability. A comparative analysis of these detection techniques is discussed. It has been concluded that there is a need for a lightweight approach for web-phishing detection. A hybrid mechanism can also be helpful that can use different web-phishing detection techniques for better detection accuracy. Along with the improvement of these techniques, end user awareness is an important parameter to avoid web-phishing attacks.

7. References

[1] James, L., 2006. Banking on phishing. In: Phishing Exposed. Elsevier Inc., Ch. 1, pp. 1–35

[2] Shraddha, P., Dhwanil, P., Srushti, K., Smita, S., "A new method for Detection of Phishing Websites: URL Detection," Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018)

[3] V. Suganya, "A Review on Phishing Attacks and Various Anti PhishingTechniques", International Journal of Computer Applications (0975 – 8887) Volume 139 – No.1, April 2016

[4] R. Gotham., I, Krishnamurthi, "A comprehensive and efficacious architecture for detecting phishing webpages," Computers and Security, Elsevier, 2014.

[5] Anjum N. Sheikh, Antesar M. Shabut, M.A. Hossain, "A Literature Review on Phishing Crime, Prevention Review and Investigation of Gaps", 2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)

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

[7] Anti Phishing Working Group (AWPG). Phishing Activity Trends Report, 3rd Quarter 2018. https://www.antiphishing.org/resources/apwg-reports/

[8] Kaspersky, https://securelist.com/spam-and-phishing-in-q3-2018/88686/, Retrieved February 08, 2019.

[9] Kaspersky report spear Phishing, https://www.kaspersky.com/resource-center/definitions/spear-phishing, Retrieved December 28, 2018.

[10] Rableen, Kaur, S., Deepak, Singh, T., and Divya, Rishi, S., "An Approach to Perceive Tabnabbing Attack," International Journal of Scientific & Technology Research Vol 1, Issue 6, July 2012.

[11] Jain A.K., Gupta B.B. (2018) PHISH-SAFE: URL Features-Based Phishing Detection System Using Machine Learning. In: Bokhari M., Agrawal N., Saini D. (eds) Cyber Security. Advances in Intelligent Systems and Computing, vol 729. Springer, Singapore

[12] Gaurav, V., Manoj, M., and Pardeep, K.A., “A survey and classification of web phishing detection schemes,” Security Comm. Networks 2016; 9:6266–6284

[13] Ozgur, koray, S., Ebubekir, B., Onder, D., Banu, D.,” Machine learning based phishing detection from URLs”, Elsevier, September 2018.

[14] Luong Anh Tuan N, Ba Lam T, Huu Khuong N, Minh Hoang N. A novel approach for phishing detection using URL-based heuristic. In Computing, Management and Telecommunications (ComManTel), 2014 International Conference on, 2014; 298–303

[15] Developers G. Safe browsing API-developer guide V3. 2014; https://developers.google.com/safe browsing/developers_guide_v3, Retrieved on December 28, 2018

[16] Jian M, Pei L, Kun L, Tao W, Zhenkai L. BaitAlarm: detecting phishing sites using similarity in fundamental visual features. In Intelligent Networking and Collaborative Systems (INCoS), 2013 5th International Conference on, 2013; 790–795

[17] Nirmala Suryavanshi, Anurag Jain , “A Review of Various Techniques for Detection and Prevention for Phishing Attack”, International Journal of Advanced Computer Technology (IJACT). Vol 4 No.03.

[18] Jaydeep, S., Rupesh, G.V., “Website Phishing Detection using Heuristic Based Approach,” International Research Journal of Engineering and Technology (IRJET), Vol 03, Issue 05, May 2016.

[19] Jin-Lee, L., Dong-Hyun, K., Chang-Hoon and Lee” Heuristic-based Approach for Phishing Site, Detection Using URL Features,” Proc. of the Third Intl. Conf. on Advances in Computing, Electronics and Electrical Technology - CEET 2015

[20] Gastellier-Prevost Sophie, Granadillo Gustavo Gonzalez, Laurent Maryline. Decisive heuristics to differentiate legitimate from phishing sites. La Rochelle, France. In: Proc. Of conference on network and information systems security (SAR-SSI); May 2011. p. 1e9.

[21] Nguyen, Luong Anh Tuan, et al. "A novel approach for phishing detection using URL-based heuristic." Computing, Management and Telecommunications (ComManTel), 2014 International Conference on. IEEE, 2014.

[22] Li L, Berki E, Helenius M, Ovaska S. Towards a contingency approach with whitelist- and blacklist-based anti-phishing applications: what do usability tests indicate? Behaviour & Information Technology 2014; 33(11):1136–1147.

[23] Krishnamurthy B, Spatscheck O, Van Der Merwe J, Ramachandran A. Method and apparatus for identifying phishing websites in network traffic using generated regular expressions, to Google Patents, 2009.

[24] Abu-Nimeh S, Nappa D, Wang X, Nai S. A comparison of machine learning techniques for phishing detection. In: APWG ecrime researchers summit (eCRS), Pittsburgh, PA; October 2007.

[25] Le, A., Markopoulou, A., & Faloutsos, M. (2011). Phishdef: URL names say it all. In 2011 Proceedings IEEE INFOCOM, 2011 (pp. 191–195).

[26] Tan, C. L., Chiew, K. L., Wong, K., & Sze, S. N. (2016). Phishwho: Phishing webpage detection via identity keywords extraction and target domain name finder. Decision Support Systems, 88, 18–27

[27] Mohammad, R. M., Thabtah, F., & McCluskey, L. (2014). Predicting phishing websites based on self-structuring neural network. Neural Computing and Applications, 25(2), 443–458.

[28] Moghimi M, Varjani AY. New rule-based phishing detection method. Expert Systems with Applications 2016; 53:231–242.

[29] Mohammad RM, Thabtah F, McCluskey L. Intelligent rule-based phishing websites classification. IET Information Security 2014; 8(3):153–160.

[30] Luong Anh Tuan N, Ba Lam T, Huu Khuong N, Minh Hoang N. A novel approach for phishing detection using URL-based heuristic. In Computing, Management and Telecommunications (ComManTel), 2014 International Conference on, 2014; 298–303

[31] Feng, F., Zhou, Q., Shen, Z., Yang, X., Han, L., & Wang, J. (2018). The application of a novel neural network in the detection of phishing websites. Journal of Ambient Intelligence and Humanized Computing.

[32] Weiwei Z, Qingshan J, Tengke X. An intelligent antiphishing strategy model for phishing website detection. In Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on, 2012; 51–56.

[33] Kausar F, Al-Otaibi B, Al-Qadi A, Al-Dossari N. Hybrid client side phishing websites detection approach.International Journal of Advanced Computer Science and Applications (IJACSA) 2014; 5(7):132–140.

[34] Buber, E., Diri, B., & Sahingoz, O. K. (2017). NLP based phishing attack detection from URLs. In A. Abraham, P. K. Muhuri, A. K. Muda, & N. Gandhi (Eds.), Intelligent systems design and Applications, springer international Publishing, cham (pp. 608–618)

[35] Jain, A. K., & Gupta, B. B. (2016). A novel approach to protect against phishing attacks at client side using autoupdated white-list. EURASIP Journal on Information Security.

[36] https://www.phishtank.com, Retrieved January 02, 2019.

[37] Rao, R. S. &, & Pais, A. R. (2018). Detection of phishing websites using an efficient feature-based machine learning framework. Neural Computing and Applications.

[38] James, Joby & L, Sandhya & Thomas, Ciza, (2013) ”Detection of phishing URLs using machine learning techniques,” 304-309. 10.1109/ICCC.2013.6731669.

[39] Chiew KL, Chang EH, Sze SN, Tiong WK. Utilisation of website logo for phishing detection. Computers & Security 2015; 54:16–26.

[40] Philippe De R, Nick N, Lieven D, Wouter J. TabShots: client-side detection of tabnabbing attacks. In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, Hangzhou, China, 2013

[41] Lam I-F, Xiao W-C, Wang S-C, Chen K-T. Counteracting phishing page polymorphism: an image layout analysis approach. Advances in Information Security and Assurance. Springer: Seoul, Korea, 2009; 270–279.

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

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 5 issue 2 Year 2021

Cyber Security and COVID-19 Pandemic

Muhammad Shairoze Malik*
13beemmalik@seecs.edu.pk
National University of Science and Technology Islamabad

Abstract:
This paper investigates the issues arisen as a result of COVID-19 pandemic in the domain of cyber security. Vulnerable people and systems have become a target of cyber criminals due to pandemic. This paper discusses an increase in cyber-attacks due to pandemic. Furthermore, the rate of cyber-attacks has been increased due to an increase in fear and anxiety caused by the pandemic. Healthcare organizations have become the primary targets of cyber-attacks during the pandemic. Many companies are expecting employees to work from home (WFH), which has also prompted concerns about cybersecurity and the risk of state-sponsored assaults, and a rise in ransomware and phishing attacks. This paper also offers many practical ways to minimize the dangers of cyber-attacks, while working from home. And also discusses mitigation of healthcare security concerns. It is critical that healthcare companies establish a comprehensive cybersecurity strategy to strengthen the security of their critical data and assets.

Keyword: Pandemic, Cyber-Security, Phishing, Scamming, Malware Attacks, Denial of Service.

1. Introduction

The COVID-19 epidemic has resulted in major problems and has significantly changed our way of life. Organizations have had to adapt by focusing on the remote working of employees on a massive scale and at a rapid speed. Many businesses have been required to update their working environments as well as take decisions that were made in a rush to allow workers to operate from home with no basic preparation or arrangements. A large number of these organizations and groups have no plans in place to deal with such an issue in a short period of time [1]. In actuality, just 38% of organizations have an internet security plan [1]. Organizations and associations all over the globe have recognized the work-from-home (WFH) strategy by switching to a decent web-based environment which generally increases dangers to business data with increasing attack vectors. It is important to emphasize that WFH must become the new standard for people from one end of the planet to the other. Frequently, this entails asking employees to use their own devices and home WiFi-networks, which are usually unsafe due to the absence of critical company standard security defenses. Organizations that currently provide devices to their employees do so with little or no administrative rights, which leads to problems when the user is required to install the needed software. As a result, companies should provide substantially more fair arrangements in addition to giving workers stronger rights, implying significantly higher possible security concerns. Network security during the COVID-19 is a particularly worrisome issue because of growing cyber-treats targeting network frameworks and vulnerable people all over the world [2]. This article focuses on network security concerns that may have arisen due to this global crisis.

2. Literature Review

Online crimes such as fraud provide the highest profits while posing the least danger to the perpetrators under typical circumstances. Examining the facts, it is apparent that more individuals are currently unemployed, spending more time at home, and utilizing the internet for both work and socializing. Furthermore, government officials have provided monetary incentives to residents as well as other companies trying to recruit or retain customers. Because the world is waiting for a feasible solution to prevent the spread of COVID-19, any material pertaining to "COVID-19" will undoubtedly get the attention of normal internet users. Scammers are using this route to transmit harmful online attacks to internet users by impersonating government employees, tax authorities, and so on, as well as links to seek help with COVID-19 [3].

In a recent study, World Economic Forum emphasized that phishing and hacking have become a new normal as it continues to effect systems even after the viruses have been wiped off [4]. Because vulnerable people are more anxious and awaiting emails, text messages, phone calls, and other contacts from authorities over COVID-19 due to which these scams are far more successful now because of pandemic. It has much easier for cybercriminals to create fake websites or messages that appear to be from familiar and relevant authorities, incorporating urgency to capitalize on the widely felt fear factor due to their increasing awareness of people vulnerabilities. As a result, the effectiveness of phishing attacks has gotten a huge boost. It can take various forms, including internal and external updates, personal investments and charities. In a recent F-Secure study, spam is categorized as one of the most common methods for malware to spread. It also highlighted how epidemic is being utilized by attackers to entice users to click, particularly by disguising the executable in organize files systems such as .zip files [5]. It must be considered that criminal actors may use genuine publications as bait to attract people to perform a high-risk activity, such as clicking on a website link or opening a large file. Before proceeding, users should investigate the sender of an email as well as any links contained within it. Cybercriminals regularly employ impersonation methods, such as posing as the WHO (World Health Organization), the UN (United Nations), or a well-known organization, such as Zoom or Microsoft to trick victims into opening infected material or clicking on links.

The whole world has been placed under lockdown due to COVID-19. The shift to a new way of working in which employees frequently work from home, mostly utilizing home equipment protected by their corporate employers, has generated numerous concerns in the sector. As a consequence of this unique mass quarantine agreement, new concerns about the resilience of scientific solutions to various ecosystems are critical; particularly, the strength of current technology within employers' current cyberinfrastructures.

3. Cyber Security Concerns Associated with the COVID-19 Pandemic

3.1 Types of Cyber-Attacks:

Malwares, distributed denial-of-service and Scams & Phishing attacks are the three types of cyber-attacks that occurred during the pandemic (DDoS). Table 1 shows several examples of cyber-attacks during this crisis. APT (Advanced Persistent Threat) groups and Cyber-criminals [6, 7] are using COVID-19 related frauds and phishing to launch cyber-attacks on vulnerable persons and businesses for a variety of reasons, including financial gain or the collection of information about COVID-19 vaccinations. Hades, APT-C-09 Patchwork (aka Dropping Elephant), Hades, APT29 [9] and TA505 [8] are examples of APT activity during the epidemic.

- ✓ Scams and phishing: These are the most successful and most common attacks used in COVID-19 [10, 11]. These attacks have a success rate of 30 percent or more. This is significant because an attacker just need a small number of clicks to get financial or other benefits. As a result, sending millions of email messages to victims requesting financial assistance from the federal government, their businesses, banks, and so on will yield rapid and significant results. There are several phishing attempts (email, SMS, and voice) that target susceptible persons and systems and utilize the term coronavirus or COVID-19 to entice victims [10, 11]. There was a 600 percent rise in coronavirus-related phishing email attacks in the first quarter of 2020 [12]. Cybercriminals are also using more sophisticated techniques to lure victims, such as the use of HTTPS encryption technologies on their websites. SSL is often associated with around 73% of phishing websites [11]. SaaS (Software as a Service) users and webmail users are the most commonly phished [11].

- ✓ Viruses, Trojans, RATs, spyware, worms and ransomware are collectively known as Malwares [13]. Throughout the outbreak, APT groups and cybercriminals took advantage of the crisis by disseminating various forms of malware to vulnerable persons and systems via email messages and websites. In reality, 94 percent of malware-infected PCs were targeted via e-mail. Specific forms of adware and spyware [14], like ransomware, will undoubtedly be more effective for pandemic response groups (Table 1).

- ✓ DDoS (Distributed-Denial-of-Service) Attack: Due to ease of launch and its effect on victim, DDoS is often regarded as the most indefensible cyber-attack. A DDoS attack employs many attack sources to launch a coordinated DoS attack on one or more targets, therefore boosting attack power and complicating countermeasures [15]. During the pandemic, UK's university students and staff were unable to access university's services and the internet due to a DDoS attack on JISC, the UK's university's Web service provider. Furthermore, it is critical to note that healthcare organizations all around the world are being undermined by DDoS attacks (see Table 1).

Type of Attack	Country	Date	Details of Attack
Distributed Denial-of-Service	France	March	A network of hospitals in Paris were affected by DDoS attacks as they were unable to connect to data and email servers [18].
Distributed Denial-of-Service	US	March	DDoS attacks were conducted on US Department of Health and Human Services [18].
Ransomware	UK	March	Medical and personal information of former patients of a medical research firm based in London were leaked by Maze Ransomware Gang [17].
Ransomware	Czech Republic	March	The whole IT network of The Brno University Hospital was forced to shut down by cyber-attacks [16].
Phishing	Taiwan	May	Emails containing RAT (Remote Access Tools) urged public to get tested for COVID-19 by impersonating Taiwan’s senior Infection-Disease Control official [19].
Ransomware	US	June	Cybercriminals known as Netwalker forced The University of California, San Francisco (UCSF), which was working on the COVID-19 vaccine, to pay $1.14 million with the help of ransomware attack [20].
Phishing	Germany	June	Emails with intent to sell PPEs (Personal Protective Equipment) were sent to top officials at a firm, which included phishing URLs that took them to fake login sites to steal their credentials [20].
Ransomware	Canada	June	CryCryptor ransomware in form of COVID-19 Contact tracing App were deployed on Android smartphones [22].

TABLE 1: Cyber-attacks in year 2020 during COVID-19)

3.2 Effects on Healthcare Organizations

During the pandemic, one of the primary targets of attacks was the healthcare industry. The attacks against healthcare institutions have highlighted the issues with cybersecurity infrastructure in the healthcare industry. These include pharmaceutical businesses, and research groups as well. WannaCry ransomware assault that rendered the National Health Service (NHS) inoperable in 2017 is one example of cyber-attacks on health service providers. One of the primary reasons is that owing to restricted resources, these organizations must defend their IT systems since they are financed by cities or nations that generally have extremely stringent financial constraints. Obsolete no longer supported software and operating systems such as Windows 7 or Windows XP are being used throughout hospitals to control medical devices. According to Europol, healthcare facilities have become profitable target for ransomware as it is easily accessible. IoT (Internet of Things) devices and computers are widely used to monitor and store patient data in modern hospitals as well as to operate ventilators and ICUs (Intensive Care Units).

CISA, United States DHS and UK's NCSC issued a joint advisory paper and guidelines which discusses concerns such as malwares, phishing, WFH tools such as Zoom, and so on [10]. APT organizations are expected to continue targeting healthcare and vital services throughout the world [23]. Canada's CSE (Communications Security Establishment) and NCSC, in a recent joint report, suggested that the APT29 (aka "Cozy Bear") cyber-attacks being conducted on various organizations which are involved in the development of a COVID-19 vaccine in Canada, US and UK, are done by Russian Intelligence Services with the goal of stealing information related to vaccines [9]. To accomplish its objectives, APT29 employs a variety of tactics, including vulnerability scanning, public exploits, and phishing to obtain access to the target network, as well as proprietary malware known as ‘WellMess' and ‘WellMail' [9].

3.3 Techniques for Mitigation

There are practical measures that may be used to decrease the danger of cyber-attacks when working from home, but mitigating and avoiding cyber-attacks is not an easy process. Some mitigation techniques are as follows [1, 10, 23]:

- Virtual-Private-Network (VPN): It is an encrypted communication channel to ensure secure data transmission between two places on the internet. VPNs are being widely used to access internet these days. It provides integrity and secrecy, and it enables companies to extend security standards to WFH employees.

- Educating Users: Many security systems consider people to be the weakest link. As a result, raising awareness about cyber-attacks among users through ongoing training is critical to reducing the risks. Just 11% of firms have offered cybersecurity training to non-cybersecurity staff in the last year, according to a recent survey [24].

- Two-Factor-Authentication: It provides increased security by requiring an OTP (One Time Password) code given to your mobile phone through SMS or an authentication app along with login username and password. It helps in preventing brute force attacks as well as password guessing and theft, as well as. Two factor authentication should be implemented between organization's network and an employee working from remote location to verify their identity.

- Anti-Malware Software’s: Cybercriminals use numerous forms of malware to attack susceptible victims. Because millions of new malware and strains are created each year, using frequent and up-to-date anti-malware may minimize the danger of malware-based cyber-attacks.

- Firmware Updates: All devices' and equipment's firmware/OS should be up-to-date with the most recent security patches. It may decrease the danger of a latest vulnerabilities and zero-day assaults.

- Segmentation and Separation: Divide a network into trustworthy zones such as the Internet zone (untrusted), the entertainment network (low trust level), the home office network (high trust level) and avoid using a single network for all types of communication. A separate Wi-Fi should be implemented for the working of IoT devices which can help in limiting the security exposure of the network infrastructure and can help in containing breaches.

- Robust Corporate Online Policy: To safeguard data and prevent cyber-attacks, a robust and comprehensive policy is required as organizations have had little or no time to prepare for the remote working situations. Strong WFH rules include not having critical business discussions in public, only using company approved audio and video conference lines, and so on. A recent research found that 46% of organizations only test their recovery and backup strategies once a year or less, so a proper recovery plan and backup method should also be included in the policies and it is also critical to evaluate these plans on a regular basis [25].

- Physical-Security: It is critical to secure home office electronics physically. Measures include not leaving work computers alone, locking the laptop or using a lock screen, always logging-off after usage, and so on.

4. Discussion

Primary focus of on-gong cyber-attacks have been the healthcare organizations, which are working to resolve COVID-19. It is critical that these companies should strengthen their defenses against cyber-attacks in order to safeguard their important data and assets. Security Incident and Event Management along with a proper Intrusion Detection Systems (IDS) are two critical components for identifying hostile conduct that might make a network vulnerable to cyber-attacks. An IDS normally use three types of techniques to make an evaluation of cyber-threats: Signature matching, Anomaly detection, Deep packet inspection. Or it uses a mixture of all three approaches to create a hybrid system. IDS which make use of Artificial Intelligence (AI) is becoming increasingly popular as they have the ability to identify zero-day assaults more precisely. It is also critical for healthcare companies to have a holistic approach to cybersecurity, seeing security not only from a technology standpoint, but also within the context of procedures [26]. Risk Management, CERT-RMM (CERT Resilience Management Model) [27] and making cybersecurity a part of strategic planning and allocating a proper budget to it [26] are all examples of comprehensive approaches to cybersecurity.

5. Conclusion

The cybersecurity problems encountered during the COVID-19 outbreak have been explored and examined in this article. The most significant cyber-attacks and vulnerabilities are identified and summarized. Potential mitigating techniques and ways to reducing the dangers of cyber threats are also explored. APT-groups and cyber criminals have been attacking vulnerable individuals and systems by taking advantage of the epidemic. This scenario is unlikely to alter in the near future. Healthcare companies have been among the most targeted by cybercriminals during the epidemic for a variety of reasons. As a result, it is critical that healthcare companies enhance their defenses against cyber-threats such as implementing a holistic strategy to cybersecurity.

6. References

[1] Furnell S, Shah JN. Home working and cyber security–an outbreak of unpreparedness? Comput Fraud Secur. 2020; 2020(8): 6- 12.

[2] Hakak S, Khan WZ, Imran M, Choo KKR, Shoaib M. Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies. IEEE Access. 2020; 8: 124134- 124144.

[3] Aleroud A, Zhou L. Phishing environments, techniques, and countermeasures: a survey. Comput Secur. 2017; 68: 160- 196.

[4] Anti-Phishing Working Group. The APWG phishing activity trends report 1st quarter 2020. https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf. Accessed July 9, 2020.

[5] Sattler J. COVID-19 scams — how to spot and stop coronavirus email attacks. https://blog.f-secure.com/re-covid-19-scams-how-to-spot-and-stop-coronavirus-email-attacks/. Accessed June 24, 2020.

[6] Alshamrani A, Myneni S, Chowdhary A, Huang D. A survey on advanced persistent threats: techniques, solutions, challenges, and research opportunities. IEEE Commun Surv Tutor. 2019; 21(2): 1851- 1877.

[7] Xiao L, Xu D, Mandayam NB, Poor HV. Attacker-centric view of a detection game against advanced persistent threats. IEEE Trans Mobile Comput. 2018; 17(11): 2512- 2523.

[8] Malwarebytes. APTs and COVID-19: how advanced persistent threats use the coronavirus as a lure. https://resources.malwarebytes.com/files/2020/04/200407-MWB-COVID-White-Paper_Final.pdf. Accessed August 27, 2020.

[9] National Cyber Security Centre (NCSC) and Communications Security Establishment (CSE). Advisory: APT29 targets COVID-19 vaccine development. https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf. Accessed July 17, 2020.

[10] National Cyber Security Centre (NCSC) and Cybersecurity and Infrastructure

Security Agency (CISA). Advisory: COVID-19 exploited by malicious cyber actors. https://www.ncsc.gov.uk/news/-covid-19-exploited-by-cyber-actors-advisory;. Accessed June 4, 2020.

[11] World Economic Forum. COVID-19 risks outlook - a preliminary mapping and its implications. http://www3.weforum.org/docs/WEF_COVID_19_Risks_Outlook_Special_Edition_Pages.pdf. Accessed June 9, 2020.

[12] Sjouwerman S. Q1 2020 coronavirus-related phishing email attacks are up 600%. https://blog.knowbe4.com/q1-2020-coronavirus-related-phishing-email-attacks-are-up-600. Accessed August 30, 2020.

[13] Crown Prosecution Service. Cybercrime - prosecution guidance. https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance. Accessed: July 11, 2020.

[14] Arabo A, Pranggono B. Mobile malware and smart device security: trends, challenges and solutions. Proceeding of the 19th international conference on control systems and computer science. New Jersey: IEEE; 2013: 526- 531.

[15] Asri S, Pranggono B. Impact of distributed denial-of-service attack on advanced metering infrastructure. Wireless Pers Commun. 2015; 83(3): 2211-2223.

[16] Cimpanu C. Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak. https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/. Accessed July 20, 2020.

[17] Goodwin B. Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack. https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus. Accessed July 20, 2020.

[18] Hale G. DDoS attacks on rise due to COVID-19. https://www.controleng.com/articles/ddos-attacks-on-rise-due-to-covid-19/. Accessed July 20, 2020.

[19] Lyngaas S. ‘Vendetta’ hackers are posing as Taiwan's CDC in data-theft campaign. https://www.cyberscoop.com/vendetta-taiwan-coronavirus-telefonica/. Accessed July 20, 2020.

[20] Lyngaas S. Hackers target senior executives at German company procuring PPE. https://www.cyberscoop.com/germany-ppe-coronavirus-hackers-ibm/. Accessed July 20, 2020.

[21] Tidy J. How hackers extorted $1.14m from University of California, San Francisco. https://www.bbc.com/news/technology-53214783. Accessed July 20, 2020.

[22] Osborne C. New ransomware masquerades as COVID-19 contact-tracing app on your Android device. https://www.zdnet.com/article/new-crycryptor-ransomware-masquerades-as- covid-19-contact-tracing-app-on-your-device/. Accessed July 20, 2020.

[23] National Cyber Security Centre (NCSC) and Cybersecurity and Infrastructure Security Agency (CISA). Advisory: APT groups target healthcare and essential services. https://www.ncsc.gov.uk/news/apt-groups-target-healthcare-essential-services-advisory. Accessed June 4, 2020.

[24] Pedley D, Borges T, Bollen A, et al. Cyber security skills in the UK labour market 2020–Findings report. Department for Digital, Culture, Media and Sport. 2020. https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020

[25] Malecki F. Overcoming the security risks of remote working. Comput Fraud Secur. 2020; 2020(7): 10- 12.

[26] Bhuyan SS, Kabir UY, Escareno JM, et al. Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. J Med Syst. 2020; 44: 1- 9.

[27] Caralli R, Allen J, White D, Young L, Curtis P. CERT Resilience Management Model Version 1.2. https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf. Accessed August 28, 2020.

Hafiz Burhan Ul Haq *et al.LGU (IJECI)* 2021

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

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 5 issue 2 Year 2021

Role of Internet of Medical Things (IoMT) and Block Chain Technology for the Prevention of COVID-19 Pandemic Effect

Hafiz Burhan Ul Haq[1], Akifa Abbas[2], Sadia Zafar[3], Kashaf Ud Doja[4]
burhanhashmi64@gmail.com, akifaabbas19@gmail.com, zafarsadia73@gmail.com,
kashaf.cs@hotmail.com
University of Education, Lahore, Pakistan

Abstract:

Now a days, COVID-19 spreads everywhere and has severely affected across the globe. As COVID-19 spread in a fast manner, it creates an alarming situation all over the world. The health sector has faced more problems as compared to other sectors due to thousands of people reported per day, so the demand for oxygen pumps, masks, and sanitizers has also increased. In this situation both public and private sectors plays an important role to make the country COVID-19 free. Both private and public sectors worked hard and developed a number of IoT and Blockchain technologies, adopting different methodologies to deal with COVID-19. This paper presents the number of IoT and Blockchain technologies like (IoT Buttons, Robots, Reporting and testing ways, telemedicine) are used in COVID-19. Furthermore, it is also elaborated that how these techniques are useful with the help of case studies.

Keywords: Telemedicines, Disinfectant, COVID-19, IoT, Blockchain

1. Introduction

Coronavirus disease-19 has not only affected the health care system but also affect the Economic, Educational, and Public Sectors.COVID-19 is continuously attacking or increasing worldwide, the Environment is falling down under the weight of collapsing economic system and stacked up fatalities[1]. Regretfully many individuals are still fear of contamination. The condition which seems today is unlikely to improve. A wide range of technological methods to resolve the effect of COVID-19 worldwide are emerging [2]. Digital automation Internet of Things (IoT), IoMT telecommunication networks such as 5G were among those at the forefront. According to the WHO and the CDC, digital automation has an important part in enhancing medical care due to the COVID-19[3]. This paper presents the several aforementioned techniques that play important role in reducing the devastating effects of the COVID-19 worldwide [4].

The Internet of medical things (IoMT), also known as health care IoT, is a combination of medical devices and software applications that provide comprehensive health care services related to healthcare IT systems. There is a huge increase in IoT and IoMT applications now a days [5]. This increase is because of growing the number of mobile devices that are configured by the use of Near Field Communication (NFC) that allow these devices to communicate with IT systems. Different types of applications has been developed such as observing patients from a distant area, Utilization of wearable devices to transmit medical information to the concerned experts, etc. [6]. Resultantly, these devices store, observed, break down, and transmit health information efficiently.[7].However, the number of IoMT techniques have been developed to prevent the COVID-19 pandemic situation. Furthermore, these techniques are utilized by various technologists, clinical associations, and government agencies to reduce the load of the health care system [8].Following are the IoT and IoMT technologies that have a wide range of contributions to tracking and ultimately managing the effect of COVID-19 pandemic.

2. Smart Thermometer

Eight years ago, a US health technology company named Kinsa had distributed internet connect smart thermometers to household peoples for high fever[9]. A smart thermometer is a medical thermometer that ables to transmit readings, that can be gathered, stored, and observed. These smart thermometers are initially designed to monitor flu. Now a days, it is used in the detection of COVID-19 concentration throughout the United States. Due to the COVID-19 eruption Kinsa Health Technology Company has distributed a wide range of technological thermostats to the household in many regions of the United States [10]. That smart instrument is connected to a cell phone device, that enables them to automatically send their data to the application, so the users easily check their report online via phone. However, by using this application, users can also check their medical history. Once this data has been received Kinsa adapts this data and develops a daily graph that shows which of the US region has a high fever rate [11]. Over a couple of years, Kinsa communicating maps have shown itself to be highly accurate in predicting the quick breaking out flu around the United States [12].

3. Robots

While government and medical institutions around the world are struggling to control the COVID-19 outbreak, robots are being introduced to support patient recovery, thus reducing the burden of healthcare workers. They worked as a nurse in the health system. Robot-based non-contact UV surface decontamination techniques are also used to reduce the virus transfer via infected surfaces [13]. On the other hand, manual workout can also increase and spread the infection, also requires the deployment of disinfecting workers that may cause the risk of getting the disease. Integrated decontamination robots can cause quick and efficient disinfection. However, the number of robots are deployed worldwide to manage the effect of COVID-19 and reduce the stress of People work in healthcare institutes [14].

As the COVID-19 worldwide continues to

spread, Asimov Robotics a Kerala based company has built up three-wheel robots that are used to support patients staying in isolation. The three-wheeled robot is capable of doing different functions such as carrying food and services to the patient as well as giving medication and clinical equipment [15]. A trained medical researchers of US Company also created automatic robots to reduce the number of Healthcare-associated Infections (HAIs). These are Light Strike Disease-Zapping UV robots that can rapidly kill all diseased or germs like viruses and bacteria [16]. Danish Robotic Company, also introduced UVD Robots that can be served as a worldwide in healthcare institute. UVD robots are distributed among various regions of China, several in Asia and the US. These robots release strong UV rays to sanitize the external surface by breaking the virus strains. These robots can also run on a single charge for around 2.5 hours and about to sanitize the nine or ten rooms [17].

4. IOT Buttons

Several healthcare organizations in Vancouver have installed several battery powered IoT controller to measure the condition of healthcare. These buttons are also know Wanda Quick touch that can be used in any risk of alarming situation and also able to deploy at any private as well as public premises.

5. Autonomous Vehicles

Autonomous vehicles (AVs) use to reduce the burden on current medical methods and also reduce the risk of transmission of viruses. China takes responsibility for using autonomous vehicles (AVs) in a pandemic situation. China is the only country in the world that develops AVs in COVID-19 to mitigate the effect of COVID-19[19]. White Rhino Auto Company based in Beijing in association with the (ITPO) of UNIDO has deployed two AVs in China healthcare centers. These AVs are extremely helpful for performing many tasks such as services of healthcare and food. These vehicles decreased the burden of workers and also minimize the threat of contamination of viruses.

6. Telemedicine:

Telemedicine is a technique of using IoMT automation to enable remote monitoring of patients. This approach helps physicians to diagnose, identify, and treat the patients without physical communication. However, there is a rapid increase in the development of IoMT software and telemedicine platforms after infectious COVID-19. The US (CMS) has to revoke many healthcare rules that allow physicians to provide remotely check their patients via telehealth platforms [20].

Following are the advantages of implementing telehealth strategies:

1) It reduces the pressure on the healthcare worker.

2) It reduces the spreading rate of infection.
Some of the aspects in which telemedicine is used to control the COVID-19 effect are listed below:

- Many telemedicine techniques, involving video calls and live Facebook webinars have been introduced in the United States to offer remote medical professionals to a number of peoples [21].

- In India government has established telemedicine equipment to allow rapid COVID-19 patients to communicate remotely with medical professionals.
- Israel's healthcare center used number of telehealth care technologies to track 12 Israeli travelers who were quarantined in japan for many weeks. Similarly, the Sheba healthcare center used telemedicine techniques to make sure limited human interaction.

Many telemedicine devices such as telemedicine cart, tele-discussion app, and handheld medicine have gained importance against COVID-19 in recent months. Telemedicine systems are also much helpful by integrating with IoT technologies such as 5G networks will the high speed of telemedicine [22]. A large number of use cases that are aforementioned showing the importance of IoT and IoMT's regarding COVID-19[23]. The number of IoT automation technologies that plays an essential role in Covid 19 are discussed below:

7. Drone Technology

At the moment of public health emergencies, such as COVID-19 around the globe, Uncrewed Aerial Vehicle (UAV) usually referred to as a drone which is an airplane without a human pilot. It includes a ground base administrator and a way of communication between devices. It can bring many benefits; they can not only ensure reduced human contact but can also be used to enter the remoteness area[24].Firstly the Chine inspect the region of COVID-19 with the help of drone technology to overcome the epidemic of COVID-19. Inspired by this, many regions over the global environment have combined their forces with various analyzers and developers to find innovative ways to use drones to combat COVID-19[25]. Some of case studies regarding usage of drone technology in COVID-19.

7. Case Study 1: Crowd Surveillance

In an attempt to reduce the spreading of COVID-19, governments across the world are adopting all the required actions to make sure social distancing. Toward this end, several countries across the world involving China and India, have used drone technology for community surveillance and to track the unwarranted regions [26]. MicroMulticopter, the global manufacturer of drones based in Shenzhen, China, has implemented more than 100 drones in many regions of China to observe regions and effectively analyze crowds. Drones configured with sky speakers can also be used to give information to people who do not comply with the regulations provided by the Chinese Government. In India, a leading global technology company called Cyient has offered an autonomous unmanned aerial spectrum with monitoring technology that helps and control the COVID-19 lockdown [27].

8. Case Study 2: Screening Crowd

Below are the following COVID-19 epidemic, the Chinese government has agreed to identify COVID-19 cases as quickly as possible. For this reason, they used drones fitted with thermal sensors to conduct large-scale temperature measurements in many populated regions [28]. In India, the New Delhi authority deployed a multi-functional drone to control the outspread of this COVID-19. Drone termed as “corona weapon”, it is configured with thermodynamic and scotopic vision cameras, with compact healthcare devices for important medical supplies, an advertising speaker system, and 10-liter antibacterial pumps for sterilizing public regions [29].

Apart from infrared sensors that test only person temperature. In contrast to these actions, analysts at the USA, in collaboration with Canada Commercial UAV developed dragonfly, are creating a “pandemic drone” for automatically tracing and detecting people with contagious respiratory disease. These drones shall be fitted with a sophisticated detector and digital sensor system capable of tracking the temperature and heart rate of humans. These drones are also supposed to be able to identify breathing problems in public sectors [30].

9. Case Study 3: Scattering Disinfectant:

Drones can be used to penetrate the coronavirus in infected areas, spray antiseptics, and mitigating the risk of more disease transmission while also reduce forefront employee’s exposure to the virus. Although many regions have regularly deployed drones when the coronavirus at the initial stage like Spain [31].

10. Distribution of Healthcare Supplies and Other Essentials

Experts at the National University of Ireland (NUI) were enable to use a UAV in September 2019 to send Galway’s diabetic medicine to a distant region on the Aran Islands. This was the first effective above visual range of sight drone operation for diabetic, and it proved to the world that how drones can efficiently bring healthcare supplies[32]. Throughout the present situation of problems, this versatility will tend to be especially useful in reducing the load of medical centers and healthcare employees. Drones may be used for quick distribution of medicine and equipment 1) with one healthcare enter to other healthcare center or 2) from healthcare enter to patient cared for at home (in case of mild form of COVID-19). In China used a drone to transport healthcare equipment from the Xingchang County Infection Control Panel to the public healthcare centers in Xingchang without leading humans to contamination[33]. Marut Drones, a company established in Hyderabad managed by an alumni team from the Indian Institute of Technology (IIT), has early started a whole range of drones to counter the COVID-19 pandemic in India. The organization has drones for sterilizing, distributing medication, temperature analysis, activity tracking, and public monitoring[34]. In the United States the destructive effect of COVID-19, many US peoples are taking numerous measure to bring drone techniques into the region [35]. Zipline, a healthcare device provides services to develop an appropriate healthcare supply chain network. Aside from becoming a secure way to distribute healthcare equipment, drones can enable the provision of food stuff, as observed in few regions of world [36]. In the meantime, Google Corporation has seen a major rise in the number of suppliers that produced automated drone distribution systems called Wing in the United States. Although drone technologies hold tremendous effort for medical assistance, many countries have not utilized full capacity during the COVID-19 pandemic. At this end, policy agencies will gather and review information on current UAV programs closely, and bring further resources into design and technology in UAV [37].

11. Blockchain

In recent years Blockchain technology and IoT has been under intense research among analysts and manufacturer. The Blockchain is expanding its existence in many fields such as banking, traveling, drone communication, and healthcare sectors [38]. Now a days, health issues regarding COVID-19 are neither regional nor autonomous. The COVID-19 pandemic spread all over the world, so people need to stand together and take the action on it. The essence of the pandemic itself is centralized, so centralized technologies such as Blockchain and IoT are much helpful during this situation. Blockchain technology is described as a decentralized distributed system that records the origin of a digital commodity. Similarly, IoT includes computing devices with unique identifiers can also transfer information all over the networks. Blockchain technology and IoT allow people and institutions to be a part of a common integrated system that enables them to exchange and transfer data safely. The Blockchain reduces the vulnerabilities as well as reduces the risk for fake data distribution and information [39]. Blockchain-based software can be used for remote tracking and supervision of Coronavirus-infected people, to alleviate the pressure on workers in the healthcare sector.

Some of the Blockchain and IoT-based helpful key points to deal with the COVID-19 are discussed below:

- Improved monitoring and documentation should be provided.
- Properly reported the infected patients.
- Lockdown Policies.
- Avoid sharing fake news.
- Authorized Donation platform.
- Reduce Supply chain interruptions.

12. Testing and Reporting

Many countries such as America, China, Italy, Pakistan, etc. are focused on curbing COVID-19. However to make the world COVID-19 free, experiments need to be conducted smartly and reliable records must be preserved on the number of tests performed[40]. An IoT and Blockchain technologies are required that help set up checkup websites to monitor the patient with COVID-19 related symptoms, tracking the area highly affected areas, reduce the stress of healthcare sectors and workers, reduce the contamination of virus from the COVID-19 patient to worker. In Blockchain technology the healthcare centers coordinate as the nodes within the distributed Blockchain networks. These nodes continuously monitor the number of tests conducted on specific networks and also indicated the confirmed cases along with checkup time. These reviews can also assist healthcare sectors to make a strategy to reduce disease in specific regions according to the number of positive COVID-19 cases [41]. Blockchain technology act as a source for updating and retrieving data by all users. IoT also plays an important role during this critical outbreak of COVID-19. It can provide vital support to the healthcare sector.

12. Recording Patient Details

Blockchain and IoT technologies that are also viable approach for storing details of COVID-19 patients. Once a person has tested positive for COVID-19 all details of the patient must be recorded including their age, health condition, the intensity of the disease, the side effects of the disease, and standard medical line may be available[42]. Apart from this, a Cloud-based database is required that stores all the patient details safely.

13. Managing the Lockdown Implementation

Staying under lockdown situations is an enormous condition for people in many regions all over the world. The people basic need to explicitly observe the prohibitions on lockdowns by staying at home. People from high authorities, NGOs, to work in tandem with the government to effectively reach the expected results of lockdown [43]. Now there is numerous example of people that are living in readily accessible regions using various services while people living in rural areas are deprived of essentials things. Towards this Blockchain and IoT technology can help governmental and non-governmental monitor peoples that need in various sectors of the country and effectively lead the enactment of lockdown. All mandated persons aligned with enacting the lockdown may act as nodes in the Blockchain technology and may enroll the community needs on the network within their specified place [44]. All the network devices in the Blockchain can view the requirements listed by the nodes according to their regions. Similarly, many IoT devices are used in homes, buildings that are capable to sense and transmit warnings in regards to a critical situation in a building or home [45]. These devices are also useful in COVID-19 situations and perform very well with little modification like automatically sense the temperature and condition of the patient, in case of having affected inform it via message or in case the number of affected people beyond the defined limit then produce alarm.

14. Conclusion

The COVID-19 has affected globally not just only the health sector but industrial and business sectors as well. However, entire world is facing such issue and also try to reduce the effects of COVID-19. The number of IoT and Blockchain devices have been developed to reduce the pressure of worker and also to reduces the human intervention. This paper discussed these technologies and also explained their effectiveness in health sector. Also these indicated how these technologies can reduces the pressure of worker in current situation and makes the environment more secure, smooth, safe and reliable.

15. Reference

[1] T. Singhal, “A Review of Coronavirus Disease-2019 (COVID-19),” *Indian J. Pediatr.*, vol. 87, no. 4, pp. 281–286, 2020.

[2] J. Ren, A. Zhang, and X. Wang, “Jo ur na l P re,” *Pharmacol. Res.*, p. 104743, 2020.

[3] D. S. W. Ting, L. Carin, V. Dzau, and T. Y. Wong, “Digital technology and

COVID-19," *Nat. Med.*, vol. 26, no. 4, pp. 459–461, 2020.

[4] N. Yadav, Y. Jin, and L. J. Stevano, "AR-IoMT Mental Health Rehabilitation Applications for Smart Cities," *HONET-ICT 2019 - IEEE 16th Int. Conf. Smart Cities Improv. Qual. Life using ICT, IoT AI*, pp. 166–170, 2019.

[5] F. Shi *et al.*, "Review of Artificial Intelligence Techniques in Imaging Data Acquisition, Segmentation and Diagnosis for COVID-19," *IEEE Rev. Biomed. Eng.*, vol. 3333, no. c, pp. 1–13, 2020.

[6] D. Soldani, "Fighting COVID-19 with 5G enabled Technologies," pp. 1–14, 2020.

[7] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[8] C. J. Wang, C. Y. Ng, and R. H. Brook, "Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing," *JAMA - J. Am. Med. Assoc.*, vol. 323, no. 14, pp. 1341–1342, 2020.

[9] U. Gasser1, M. Ienca2, J. Scheibner2, J. Sleigh2, and E. Vayena2, "Digital tools against COVID-19: Framing the ethical challenges and how to address them," *Arxiv.Org*.

[10] R. Vaishya, A. Haleem, A. Vaish, and M. Javaid, "Emerging Technologies to Combat the COVID-19 Pandemic," *J. Clin. Exp. Hepatol.*, vol. xxx, no. xxx, pp. 2–4, 2020.

[11] C. Jinadatha, R. Quezada, T. W. Huber, J. B. Williams, J. E. Zeber, and L. A. Copeland, "Evaluation of a pulsed-xenon ultraviolet room disinfection device for impact on contamination levels of methicillin-resistant Staphylococcus aureus," *BMC Infect. Dis.*, vol. 14, no. 1, pp. 286–288, 2014.

[12] S. D. Chamberlain, I. Singh, C. A. Ariza, A. L. Daitch, P. B. Philips, and B. D. Dalziel, "Real-time detection of COVID-19 epicenters within the United States using a network of smart thermometers," *medRxiv*, p. 2020.04.06.20039909, 2020.

[13] I. Z. A. D. P. No and W. Naudé, "DISCUSSION PAPER SERIES Artificial Intelligence against COVID-19 : An Early Review Artificial Intelligence against COVID-19 : An Early Review," no. 13110, 2020.

[14] D. Soldani and A. Manzalini, "Horizon 2020 and beyond: On the 5G operating system for a true digital society," *IEEE Veh. Technol. Mag.*, vol. 10, no. 1, pp. 32–42, 2015.

[15] A. Sepehrinezhad, A. Shahbazi, and S. S. Negah, "COVID-19 virus may have neuroinvasive potential and cause neurological complications: a perspective review," *J. Neurovirol.*, 2020.

[16] J. J. P. C. Rodrigues *et al.*, "Enabling Technologies for the Internet of Health Things," *IEEE Access*, vol. 6, no. 1, pp.

13129–13141, 2018.

[17] Q. Pham, D. C. Nguyen, T. Huynh-the, W. Hwang, and P. N. Pathirana, “Artificial Intelligence (AI) and Big Data for Coronavirus (COVID-19) Pandemic : A Survey on the State-of-the-Arts,” no. April, pp. 1–17, 2020.

[18] B. McCall, “COVID-19 and artificial intelligence: protecting health-care workers and curbing the spread,” *Lancet Digit. Heal.*, vol. 2, no. 4, pp. e166–e167, 2020.

[19] A. Alimadadi, S. Aryal, I. Manandhar, P. B. Munroe, B. Joe, and X. Cheng, “Artificial intelligence and machine learning to fight covid-19,” *Physiol. Genomics*, vol. 52, no. 4, pp. 200–202, 2020.

[20] S. Koven, “Engla, Journal - 2010 - New engla nd journal,” *N. Engl. J. Med.*, pp. 1–2, 2020.

[21] A. E. Loeb, S. S. Rao, J. R. Ficke, C. D. Morris, L. H. Riley, and A. S. Levin, “Departmental Experience and Lessons Learned With Accelerated Introduction of Telemedicine During the COVID-19 Crisis,” *J. Am. Acad. Orthop. Surg.*, vol. 28, no. 11, pp. 469–476, 2020.

[22] C. M. Contreras, G. A. Metzger, J. D. Beane, P. H. Dedhia, A. Ejaz, and T. M. Pawlik, “Telemedicine: Patient-Provider Clinical Engagement During the COVID-19 Pandemic and Beyond,” *J. Gastrointest. Surg.*, 2020.

[23] A. C. Smith *et al.*, “Telehealth for global emergencies: Implications for coronavirus disease 2019 (COVID-19),” *J. Telemed. Telecare*, vol. 2019, 2020.

[24] X. Zhou *et al.*, “The Role of Telehealth in Reducing the Mental Health Burden from COVID-19,” *Telemed. e-Health*, vol. 26, no. 4, pp. 377–379, 2020.

[25] B. Skorup and C. Haaland, “How Drones Can Help Fight the Coronavirus,” *SSRN Electron. J.*, 2020.

[26] R. Madurai Elavarasan and R. Pugazhendhi, “Restructured society and environment: A review on potential technological strategies to control the COVID-19 pandemic,” *Sci. Total Environ.*, vol. 725, p. 138858, 2020.

[27] M. A. Ruiz Estrada, “The Uses of Drones in Case of Massive Epidemics Contagious Diseases Relief Humanitarian Aid: Wuhan-COVID-19 Crisis,” *SSRN Electron. J.*, 2020.

[28] U. G. C. Care, L. Journal, and C. Engineering, “Drone Technology - Game Changer to Fight Against COVID-19,” no. 6, 2020.

[29] P. Vaishnavi *et al.*, “Artificial Intelligence and Drones to combat COVID - 19,” vol. XII, no. Vi, pp. 125–135, 2020.

[30] S. L. Roberts, “Tracking Covid-19 using big data and big tech: a digital Pandora’s Box | British Politics and Policy at LSE,” *LSE Blog*, 2020.

[31] Z. Hu, Q. Ge, S. Li, L. Jin, and M. Xiong, “Artificial Intelligence Forecasting of Covid-19 in China,” pp. 1–20, 2020.

[32] O. Gozes, M. Frid, H. Greenspan, and D. Patrick, “Title : Rapid AI Development

Cycle for the Coronavirus (COVID-19) Pandemic : Initial Results for Automated Detection & Patient Monitoring using Deep Learning CT Image Analysis Article Type : Authors : Summary Statement : Key Results : List of abbreviati," 2020.

[33] M. Torky and A. E. Hassanien, "COVID-19 Blockchain Framework: Innovative Approach," 2020.

[34] J. J. Jordan and D. G. Rand, "Electronic copy available at : https://ssrn.com/abstract=1618202 Electronic copy available at," vol. 1, pp. 1–18, 2019.

[35] M. Gupta, M. Abdelsalam, and S. Mittal, "Enabling and Enforcing Social Distancing Measures using Smart City and ITS Infrastructures: A COVID-19 Use Case," pp. 1–5, 2020.

[36] M. Javaid, A. Haleem, R. Vaishya, S. Bahl, R. Suman, and A. Vaish, "Industry 4.0 technologies and their applications in fighting COVID-19 pandemic," *Diabetes Metab. Syndr. Clin. Res. Rev.*, vol. 14, no. 4, pp. 419–422, 2020.

[37] M. M. M. ΘΕΟΔΩΡΟΥ, "Δομή και Λειτουργία του Ελληνικού Συστήματος Υγείας(Διοικητικές και Νομικές Διαστάσεις)No Title."

[38] U. Rahardja, A. S. Bist, M. Hardini, Q. Aini, and E. P. Harahap, "Authentication of Covid-19 Patient Certification with Blockchain Protocol," vol. 29, no. 8, pp. 4015–4024, 2020.

[39] D. C. Nguyen, M. Ding, P. N. Pathirana, and A. Seneviratne, "Blockchain and AI-based Solutions to Combat Coronavirus (COVID-19) -like Epidemics : A Survey," pp. 1–15, 2020.

[40] M. C. Chang and D. Park, "How Can Blockchain Help People in the Event of Pandemics Such as the COVID-19?," *J. Med. Syst.*, vol. 44, no. 5, 2020.

[41] T. P. Mashamba-Thompson and E. D. Crayton, "Blockchain and artificial intelligence technology for novel coronavirus disease-19 self-testing," *Diagnostics*, vol. 10, no. 4, pp. 8–11, 2020.

[42] N. L. Bragazzi, H. Dai, G. Damiani, M. Behzadifar, M. Martini, and J. Wu, "How big data and artificial intelligence can help better manage the covid-19 pandemic," *Int. J. Environ. Res. Public Health*, vol. 17, no. 9, pp. 4–11, 2020.

[43] H. Hou *et al.*, "Pr es s In Pr," *Appl. Intell.*, vol. 2019, pp. 1–5, 2020.

[44] G. Z. Yang *et al.*, "Combating COVID-19-The role of robotics in managing public health and infectious diseases," *Sci. Robot.*, vol. 5, no. 40, pp. 1–3, 2020.

[45] G. Halegoua, "Smart City Technologies," *Smart Cities*, 2020.

Editorial Policy and Guidelines for Authors

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

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

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

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

LAHORE GARRISON UNIVERSITY

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

VISION

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

MISSION

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

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

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