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

International Journal for Electronic Crime Investigation

(IJECI)

VOL: 5
ISSUE: 4 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(4) 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(4) Year (2021)

CONTENTS

Editorial

Kaukab Jamal Zuberi
Latest Trends in Malware Attacks 01-02

Research Article

Prof Dr Aftab Ahmad Malik, Dr Mujtaba Asad, Dr Waqar Azeem
Role of Legislation, Need of Strong Legal Framework and Procedures to Contest Effectively with Cybercrime and Money Laundering 03-10

Research Article

Muhammad Taseer Suleman
Malware and their diverse characteristics related to detection and analysis: A literature survey 11-22

Research Article

Shairoze Malik and Erej Azeem
The Secrets to MIMIKATZ - The Credential Dumper 23-30

Research Article

Hafiz Burhan Ul Haq, Akifa Abbas, Muhammad Amjad Khan, Memoona, Sabreena Nawaz
Biometric Attendance Techniques in COVID-19: A Review 31-40

LGU International Journal for Electronic Crime Investigation
Volume 5(4) Year (2021)

Latest Trends in Malware Attacks

Kaukab Jamal Zuberi
Chief Editor

Increased in cyber attacks on government infrastructure calls for an immediate effort on increasing end user awareness about the potential techniques used in latest malware attacks.

Some of the malware attack trends to watch out for in 2022 are described as follows:

Use of Artificial Intelligence in Hacking:
Artificial Intelligence is a double edged sword which can be used by hackers as a weapon to design advance attacks on complex networks. White hat hackers have successfully demonstrated real-world attacks against AI-powered autonomous driving systems such as those used by Tesla cars. Researchers from Chinese e-commerce giant Tencent managed to get the car's autopilot feature to switch lanes into oncoming traffic using inconspicuous stickers on the roadway. Even without gaining the access hackers can poison data and sabotage the algorithms. "There hasn't been enough policymaker attention on the risks of AI being hacked," says Andrew Lohn, a senior fellow at the Center for Security and Emerging Technology—or CSET—a nonpartisan think tank attached to Georgetown University's Walsh School of Foreign Service. "There are people pushing for adoption of AI without fully understanding the risks that they are going to have to accept along the way.

Mobile is the new target
Cyber security trends show an increased attacks on the handheld devices. Increase in usage of mobile banking through handheld devices, reliance of various communication applications to communicate and storage of private information on the mobile device has resulted in making handheld devices a lucrative target for malware developers. Smart phones malwares will be a big challenge in 2022 for cyber security professionals.

Clouds are Vulnerable
As more organizations are moving their data to clouds, their security has become a big concern for cyber security professionals. Security measures should be taken to continuously monitor and update the software to prevent data leakages or sabotage.

Data is the prime target for hackers
Data breaches are expected to increase specially in developing countries where the quality of the software and hardware are obsolete. Safe guarding the data is prime responsibility of the cyber security teams. There is an urgent need for analyzing the existing infrastructure and take measures to close the security gaps found in this process of analyzing infrastructure. There has been several data breaches during last nine months in Pakistan. The data of very important government organizations and banks was breached, hacked, and placed on dark web.

The process of Automation and Integration
As the data grows in size and the demand for efficient and automated operations increase every day. Modern day hectic schedules pressurize professionals and engineers to deliver quick and proficient solutions. Large and complex web applications are further hard to safeguard making automation as well as cyber security to be a key concept of the software development process.

Targeted Ransomware
Critical infrastructure of organizations is being targeted with customized ransomware written for those organizations. These attacks will grow in 2022. In Pakistan, the number of such attacks have grown significantly, some of them were reported and others were kept secret by the organizations. These attacks can leak the information on dark web or encrypted critical data. Organization should develop effective Disaster Recovery Infrastructure and take steps to safeguard the critical data of the organization.

State-Sponsored Cyber Warfare
Cyber space was declared as fifth domain of war in the year 2010 by US government. Since then, state sponsored cyber warfare continues to take place discreetly and effectively. These attacks are planned and are conducted by expert operators. These attackers have all the resources available, which are required to achieve their targets.

Often, these operators collaborate with the employees of the target organizations by giving them material favors. The attacks which are supported by internal employees are hard to detect and investigate.

Measures should be taken in the critical infrastructure to have security checks on the important members of the information technology team. Periodical credit checks and background checks should be made and the management should very carefully watch the red flags in the spending patterns of these employees. In 2022, we will have redesign the cyber security policy and change the carelessness observed by the decision makers of the critical infrastructure in Pakistan. In 2022 following trends are picking up pace in global cyber security practices:

User Awareness:
As the cyber security threats have become more aggressive the organization are working to increase user awareness through seminars and trainings. What drives cybersecurity awareness forward is the growing number of people unaware of most cyberattack methods. A report by Infosec indicates that about 97% of the people in the world cannot identify a phishing email, while 1 in 25 people click such emails, thus, falling prey to cyberattacks (Infosec). Aside from this, cybercriminals now resort to more advanced and high-tech forms of phishing and malware infections. Cyber awareness among end users can prevent cyber attempts to attack the infrastructure. Organizations need to take immediate steps to create cyber awareness among employees.

Zero Trust
The zero trust model restricts network access to only those who need it. Access is granted to authorized users using patterns based on identity, time, and device based on contextual awareness, and default access is eliminated. Everything must now pass security protocols such as access control steps and user identity verification.

Security as Service
More and more companies are moving towards Managed Security Service Providers (MSSP) to ensure the cost efficient and timely availability of sisecurity solutions for the organizations. This trend is increasing and have its pros and cons.

Machine Learning:
Role of Machine Learning is growing in the field of Cyber Security. Machine Learning enables cyber security systems to analyze the threat patterns and learn the behavior of the cyber criminals. This prevents the organizations from future attacks.

GDPR Compliance
he general data protection regulation is one of the most important tools of the European Union in managing data privacy. In fact, it is extrapolated not only for inhabitants in any member state but for all companies marketing goods or services to EU residents. Therefore, the GDPR has a significant impact on global data protection requirements.

It imposes a uniform and consistent data security law, eliminating the need for each state to write its own law on personal data, which further protects consumers.

Distributed Decisions:
In the face of a potential cyberattack scenario, business cybersecurity needs, and expectations are maturing and shifting towards a more agile security model. Therefore, the scope, scale, and complexity of digital business require that cybersecurity decisions, responsibility, and accountability be distributed across organizational units, departing from a centralized function.

Therefore, the role of the CISO (Chief Information Security Officer) has shifted from that of a technical subject matter expert to that of an executive risk manager. But, as we said above, a single centralized cybersecurity function is not agile enough to meet today's business needs. CISOs must reconceptualize their roles to empower business leaders, making it easier to make their own informed risk decisions.

No one knows the future of cyber security. New risks are emerging every day. Some organizations are still trying to figure out the means and ways to secure their data, Pakistan is way behind in cyber security and intensity of the recent cyber attacks call for an immediate action to come up with a comprehensive strategy to safeguard our critical infrastructure from potential cyber attacks which may cause significant damage.

Aftab *et al.LGU (IJECI) 2020*

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

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 5 issue 4 Year 2021

Role of Legislation, Need of Strong Legal Framework and Procedures to Contest Effectively with Cybercrime and Money Laundering

Prof Dr Aftab Ahmad Malik [1], Dr Mujtaba Asad [2], Dr Waqar Azeem [3]
Ph.D (University of Kent, England);M.Phil; MSc; LL.B.
Professor, Faculty of Computer Science,
dr_aftab_malik@yahoo.com
Ph.D (Shanghai Jiao Tong University, China) Assistant Professor [2],
Ph.D.; M.Phil ; Assistant Professor [3],
[1,2,3] Lahore Garrison University

Abstract:

There is need for a robust and strong legislation to tackle white Collar-crime is stressed, which is on the rise in both the public and private sectors. The effect of immoral and unlawful actions in government, notably high-level bribes, has crippled the financial and legislative bodies in their normal functioning. The bank frauds, money laundering and cybercrimes are also on the rise, due to the widespread use of digital gadgets and the internet. The absence of strong network-security systems especially in banking sector has caused great losses indeed. The goal of this study is multidimensional; more about the importance of applying strong regulations as well as morality and ethical principles. It has been argued in this paper that morality and ethical norms have a positive influence on minimizing such crimes; if morality and ethics be coupled with strong legislation, it works as a Deterrence Force. It will undoubtedly be one of the most momentous global occurrences in recent history, having a long-term impact on culture, government operations, crime, economics, politics, and social relationships. The major role in combating the crime depends upon existence of strong legislation capable of causing reduction in crime rate, which allows the investigators vast powers and collaboration with prosecution and safeguarding the witnesses. The criminals are very well organized and using most modern technology and IT equipment, therefore, the police, investigators and prosecutors must have and be highly trained and equipped, similarly.
appropriate methods and algorithms are required. We create a new method which is a dynamic atomic shared memory for message communication. A properly stated method is proposed for message communication and then implemented. According to this method, owners can be changed dynamically and their access to read and write also changes.

1. Introduction

According to [1], the need of strong legislation has been emphasized, but most of the time times the structure of naïve cases framed by law enforcement agencies, benefits to offenders.

Similar situations have been observed in [2] and [6] for offences of bank robbery and against women and children. According to [3], the most important issue is the Standardization of forensic evidence its procurement preservation and presentation in court of using FBI techniques by FIA. The paper [3] describes deficiencies in PECA and propose amendments to facilitate investigating agencies, courts and prosecution, [4] proposes for proper use of electronic devices for effective implementation of law. Regarding Bank frauds, [5] highlights the use modern equipment as well as discuss the role and effectiveness of Business Ethics in banking sector. The crime rates fluctuations in Pandemic situation has been reviewed in [7]. A study has been presented by [8] on public perceptions of white-collar crime and punishment. Acceding to [9] and [10] , national public survey on white-collar crime. Morgantown, wv: national white collar crime center has been highlighted. The useful reports regarding happenings to crime during the pandemic is reported by BBC in [11] and [12].

2. Bank Frauds

It has been observed that in most bank frauds, the employees of banks participate in frauds and perpetrate embezzlement and illicit transitions using computers and other digital technologies. The importance of corporate ethics in the banking industry cannot be overstated. Some politicians commit misdeeds, which must be called out with a strong and iron fist. Human behavior has been deteriorated recently, because of economic slump in all countries, political instability and the rise of the Covid-19 epidemic. The digital offences, money laundering and unlawful transactions were at an all-time high even before Covid-19. Fighting such illicit professional practices is a huge task for the world specially Pakistan. Business activities are likewise expanding, necessitating the requirement for fair financial transactional activity. The consistent arguments on this issues are the most common causes of illegalities are accounts that are not working properly and people who purposefully take money from them. The majority of the crimes are performed with the aid of computer software, hacking and tracking as said earlier. The important reasons are:

- Deceptive behavior,
- Inadequacy (means: insufficiency),
- Ineffectiveness,
- Corrupt work style,
- Willful neglect and
- Dysfunction in commercial activities of the workers and employees. Particularly, when it comes to receiving and moving funds, as well as money exchange locally and internationally, auditing that is not up to par, using falsehoods to harm the market, misconduct by private and public companies, commercial, organizations and banks. The scarcity of trustworthy and well-trained bank officers is another reason.

3. White Collar Crime Frauds and Money Laundering

It is defined as a crime committed by persons of respectability and high social status in the course of the occupation. For example, it is committed for financial gains, such as securities fraud, embezzlement, corporate fraud and money laundering. In every society offender having modes-operandi of committing white-collar crime working in influential capacity in the society; either managerial positions or publically and politically powerful. They operate the offence in groups. It is defined as a crime committed by persons of respectability and high social status in the course of the occupation.

4. Naïve Cases in Cybercrime and White-Collar Crime

It has been observed that development of naïve cases and weak investigation and non-supporting witnesses sometimes lead to weaken the hands of the prosecution. Sometimes the terrorists have been set free by the courts due to reasons such as deficiencies and flaws in legislation. The Cyber and White-Collar crimes are committed by using and accessing Computers and Networks by tracking and hacking the Data and information of people and organizations. No strategy can be successful in the absence of strong legislation. The criminals involved in Cybercrime and white-collar crime keep on acquiring and hacking the data of people, government, industry, banks and business organizations by crossing security barriers of computers and networks. The occurrence of crime increased particularly in threats to attack and asking money to stop the attack

5. Threat is a new modus operando?

Nowadays it is common to threats the people and CEO's of Business organizations. The occurrences of crime increased particularly in threats to attack and asking for money to stop the attack. Stricter security measures must be adopted to safeguard the data and networks and strong encryption attained and implemented.

European Union Point of View

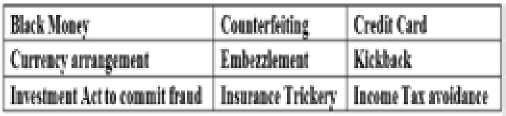
- The European Union advocates focusing on strong legal frame work.
- In addition, there exist justifications to amend the US cyber legal framework to reduce the frequency of crime.
- The present paper presents some salient legal, procedural and feasible measures.

Why deterrence force is important? Examples:

- Punishment of Theft, Dacoity, Rape and narcotics smuggling in Saudi Arabia
- Punishment of Corruption in China is death penalty
- Punishment of Terrorist Activities in Islam

Spreading disinformation to harm business

- This strategy is adopted by many criminal minded people to harm the business.
- The incorrect information is believed to be true, particularly in stock markets.
- This is achieved by floating incorrect trade data willfully by miscreants.



Black Money	Counterfeiting	Credit Card
Currency arrangement	Embezzlement	Kickback
Investment Act to commit fraud	Insurance Trickery	Income Tax avoidance

Table 1 : Selected areas of white-collar crime. Source [1]

6. Role of National Accountability Bureau (NAB)

The role of NAB is of immense impotence due to corrupt practices and recovery of the looted money. But unfortunately, due to false propaganda, this institution needs to redefine its role so that the nation and the victims of NAB know that justice is being done. It has been reported in depth in [13] about the alarm regarding the issue of 90 days detention in NAB cases; accordingly, the report says, “The controversial provision empowering the National Accountability Bureau (NAB) to detain an accused for 90 days came on the radar of the Supreme Court when on the apex court described the clause as cruel and an injustice”. The author of [13] further states that the issue concerns filing of multiple references against accused by NAB. One of the appeals concerns a former Director general of FATA Disaster Management Authority, facing allegations of granting approval and forwarding fake and bogus claims of 161 persons, embezzling Rs59.6 million from the grants which were to be distributed as compensation among the affected for the damage caused to their houses due to security operations in Mahmand Agency. On one hand the the criminal commit offences aginst the nation and on the other hand criticize the national institution NAB.

The authors of this research paper are of the opinion that all constitutional institutions must be respected i.e. all courts of law, government agencies and functionaries, They have their constitutional role prescribed under law. However, where there exists any hardship to follow a particular procedure of law, the high courts, Supreme Court, legislative assemblies and parliament may take cognizance with their jurisdiction.

Section 24 (d) of the National Accountability Ordinance (NAO) empowers NAB to detain any accused in its custody for the purpose of inquiry and investigation for a period not exceeding 90 days, but the court concerned can remand the accused to custody not exceeding 15 days at a time and for every subsequent remand the court will have to record reasons in writing, the copy of which will have to be sent to the high court concerned.

According to recommendation [13] NAB don’t harass the accused and should exercise its authority while remaining within the four corners of laws, instead of perceived notion of its authority, adding that what is needed against a suspect in white-collar crimes was on documentary evidence.

6.1 National Accountability (newly-amended) Ordinance, 2021

The promulgation of a new accountability law will affect, according to [13] nearly 100 high-profile cases involving senior bureaucrats and others. A closer look into the National Accountability (newly-amended) Ordinance, 2021 suggests that nearly 2,700 accused (60pc of total ongoing 8,272 references, investigations, inquiries and complaints) either might get relief under the newly-promulgated accountability law or their matters would be transferred to the authorities, departments and courts concerned under the respective laws. Presently, 332 high-profile/mega cases are under process at the NAB regional offices. They link to a former president, six former prime ministers, eight ex/sitting chief ministers, 126 former/sitting ministers/senators/MNAs/MPAs, 159 serving/retired bureaucrats and fake accounts cases.

According to the analysis presented in [14], the opinion of experts say that amendments made in the National Accountability Bureau (NAB) law through a presidential ordinance are a mix of good, harsh and controversial provisions.

All victims claim that they are being victimized due their no fault which is not correct.

However, points important to be adhered to and construction of strong cases are given below:

- Construction of naïve cases against criminals may not be sent to court pre-mature. The language of the cases registered (FIR) is not effective most of the times. The false propaganda is that the cases have been made as a result of political victimization, such impression may be ruled out. The cases are registered by Law enforcement agencies, but the state witnesses do not support most of the times, the prosecution and investigation officers in court.

- Further, according to [14], the eminent constitutional expert Mr Wasim Sajjad explained that giving accountability courts the power to grant bail was a fairamendment but attaching the condition of a surety bond equivalent to the alleged corruption amount was unjust. “It is always the discretion of the relevant court to fix the surety money. But in the present case, a legislative order through a presidential ordinance has been given to it to follow,” he said. “Courts determine a reasonable surety bond amount while granting bail.

Recommendations

1. There is need for reaffirmation and making currently available legislation into a stronger set of procedural and criminal law. To reduce corruption and bribery, the government must take proactive measures.

2. The public funds not to be squandered or wasted. To prevent bribery and corruption, take strong measures against public servants and place them under rigorous observation.

3. Computerization i.e. e-commerce and e-governance, be implemented in all public sector companies. Reducing rules and making the procedure simpler with appropriate tools will also help the process.

4. In every society offender having modes-operandi of committing white-collar crime working in influential capacity in the society; either managerial positions or publically and politically powerful. They operate the offence in groups.

5. The major role in combating the crime depends upon existence of strong legislation capable of causing reduction in crime rate, which allows the investigators vast powers and collaboration with prosecution and safeguarding the witnesses.

6. The criminals are very well organized and using most modern technology and IT equipment, therefore, the police, investigators and prosecutors must have and be highly trained and equipped, similarly.

7. The fair play according to the merits of the case and guilt of offenders shall bring coherence and confidence.
8. The bribe cases must be taken up sternly with iron hands particularly where national exchequer is harmed with unbearable amounts.

9. Cybersecurity threats are only going to continue to increase, so it's essential to enforce coding security best practices, like using secure coding standards. Implement most recent most effective coding security best practices and secure coding standards to help ensure that the banks' software development is secure. key coding standards to help ensure secure software development, which may include:

    - CERT
    - CWE
    - CVE
    - OWASP
    - DISA STIG
    - NVD and CVSS

10. A static code analysis or SAST tool can help ensure secure software development. The banks may secure their network using by using encryption; banks and other financial institutions can remain in control of data protection regardless of where it's located. Encrypted information is safe in transit, on the network, and even in the cloud. In cases where system security fails, encrypted data is still safe from prying eyes.

11. All concerned must possess the knowledge and awareness of security compliance standards; the security compliance management is the process of monitoring and assessing systems, devices, and networks to ensure they comply with regulatory requirements, as well as industry and local cybersecurity standards. Staying on top of compliance isn't always easy, especially for highly regulated industries and sectors.

12. The recommendations suggested in [15] are very useful, for example, the Bank Regulations and Opportunity 2022 marks a period of great regulatory change around the world for community banks, national banks, bank holding companies, credit unions, and the financial system. For that reason, it is imperative to stay up to date on the current regulatory changes and banking laws, as well as new proposals being discussed in the jurisdictions in which institutions operate. They may have a crucial impact on digital transformation initiatives.

7. Acknowledgement

The authors express their gratitude to the Chief Editor and Director Forensics Mr Kaukab Zuberi for his valuable guidance.

8. References

[1]: Dr Aftab Ahmad Malik, Mujtaba Asad and Waqar Azeem, "To Combat White Collar Crimes in Public and Private Sector and Need for Strong Legislation and Ethics", International Journal for Electronic Crimes Investigation"(IJECI); Vol 4 Issue 3, July-September 2020 PP-1-8.

[2]: Dr Aftab Ahmad Malik, Mujtaba Asad and Waqar Azeem," Promulgate Strong legal framework for child protection against offences of torturing, abusing or killing"; International Journal for Electronic Crimes Investigation"(IJECI) Volume 4 issue 2, April-June 2020 ; PP 1-10

[3]: Dr Aftab Ahmad Malik, "Standardization of forensic evidence its procurement preservation and presentation in court of using FBI techniques by FIA"; International Journal for Electronic Crimes Investigation (IJECI); Volume 4 issue 1 , Jan - March 2020 PP :1-6.

[4]: Aftab Ahmad Malik, Mujtaba Asad, Waqar Azeem, "Deficiencies In PECA and Proposed amendments to facilitate Investigating Agencies, Courts and Prosecution, Proper Use Of Electronic Devices For Effective Implementation Of Law"; "International Journal for Electronic Crimes Investigation"(IJECI) Published in October-December Issue 2019

[5]: Dr Aftab Ahmad Malik, "Bank Frauds Using Digital Devices and the Role of Business Ethics", "International Journal for Electronic Crimes Investigation"(IJECI) volume 2 issue 4, 2019

[6]: Dr Aftab Ahmad Malik "Electronic Devices to Investigate Offences of Torturing, Abusing, Molesting Assaulting or Killing the Innocent Children"; International Journal of Electronic Crime Investigation (IJECI); Volume 3, issue 2; April-June, 2019.

[7]: Ben Stickle, Marcus Felson (2020),"Crime Rates in a Pandemic: the Largest criminological Experiment in History", American Journal of Criminal Justice (2020) 45: PP 525–536https://doi.org/10.1007/s12103-020-09546-0

[8]: Holtfreter, K., Van Slyke, S., Bratton, J., and Gertz, M. (2008). Public perceptions of white-collar crime and punishment. Journal of Criminal Justice 36: 50–60.

[9]: Huff, R., Desilets, C., and Kane, J. (2010). The 2010 National Public Survey on White Collar Crime. Morgantown, WV: National White Collar Crime Center.

[10]: Syeda Marryium, et.al (2019): "Aspects of White Collar Crime", IJECI Volume 3, issue 4, October-December

[11]: Dominic Casciani & Ben Butcher (2020) Covid: What's happened to crime during the pandemic? BBC Report;

[12]: John H. Boman, Owen Gallupe (2020), " Has COVID-19 Changed Crime? Crime Rates in the United States during the Pandemic; PMCID: PMC7340780; PMID: 32837168; American Journal of Criminal Justice. Jul 8 : PP 1–9. doi: 10.1007/s12103-020-09551-3 [Epub ahead of print]

[13]: Nasir Iqbal , "SC alarm over 90-day detention of accused in NAB cases", Published in Dawn, December 4th, 2020

[14]: Tariq Butt, "Experts: NAB law amendments a combination of good, harsh provisions", October 2021, The News International; https://www.thenews.com.

pk/print/901299-experts-nab-law-amendments-a-combination-of-good-harsh-provisions

[15]:Michael Magrath, “Cybersecurity and Strong Authentication – Compliance” Top Banking Regulations & Security Compliance Requirements [2022] https://www.onespan.com/blog/top-banking-regulations-security-compliance-requirements

Suleman *et al.LGU (IJECI)* 2020

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

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 5 issue 4 Year 2021

Malware and their diverse characteristics related to detection and analysis: A literature survey

Muhammad Taseer Suleman
taseersuleman@lgu.edu.pk
Digital Forensics Research and Service Centre, Lahore Garrison University, Lahore

Abstract:

The term malware refers to a specific form of software that causes damage to the computing device through data leakage and transformation, device malfunctioning, hacking, and exploitation. A typical malware can be categorized into several categories including virus, worm, trojan, ransomware, etc. The analysis of malware helps in the categorization and behavior judgment of malware. The deep analysis of malware helps in malware detection. The current research study covers a hierarchical representation of various malware categories, different forms of detection, computing devices for malware, and a malware analysis approach. The study describes each category in detail, which helps in forming mapping of malware analysis in detail.

Keywords: malware, analysis, worms, trojans, ransomware, detection.

1. Introduction

The word Malware consists of two words: Mal means “Malicious” ware means “Software” means Malicious Software. The malware contains a set of instructions that can harm or damage your computers on the behalf of the attacker or according to the intentions of the attacker. Malware is malicious software that can harm computers or networks on a large (WAN) or small scale (LAN) [1]. The malware contains diverse types and categories. The malware consists of botnets, spyware, rootkits, backdoor, worms, viruses, spam, ransomware, scareware, and adware[2]. Due to diversity in the malware categories, these affect a variant type of devices. Nowadays, a single user can interact with several devices including a personal computer, laptop, smart phone, smart watch, etc. Several malware categories affect these devices in number of ways including hacking, data leakage, data transformation, data unavailability, device malfunctioning etc. The detection of malware is of great importance [3]. Detection can be broadly classified into central-based or peer-based. The central-based detection involves one server, to which different devices are communicated and the server scans each device for the possible matching of virus strings [4]. Moreover, peer-based detection involves any malware detection software installed in the device. The known malware can be caught through scanning of installed anti-malware applications.

The current study focused on the malware taxonomical representation in terms of its categories, detection approaches, interaction with different devices, and malware analysis types. Each category is discussed in detail. The rest of the paper presents malware taxonomy in detail with conclusive remarks at the end.

2. Malware Taxonomy

The malware taxonomy spans largely into its different types, detection capabilities, effects on different devices most importantly the behavioral analysis through which

2.1. Malware categories

2.1.1. Botnets:

Botnets allow attackers to access the system, Botnets are usually deployed on a large scale if the computers are infected with same type of botnet that it can be accessed from one C2C server (Command and Control Server). Botnets are a special kind of malware. Botnets spread like worms. Most of the botnets are made up of **IRC (Internet Relay Chats)** bots that are connected via the channel in which they accept commands for example "DDOS" means increasing the traffic on the server, "run/exploit" to open anything in the targeted system.

- **Spyware:** The main purpose of spyware is to monitor or keep track of its targets and can steal their data. It usually collects information from the target system and sends it to the attacker for example keyloggers, sniffers, spybots, etc., [5].

- **Keyloggers:** Keyloggers are used to collect your keyboard logs, can collect your sensitive information for example bank information, passwords, confidential messages, etc.

- **Sniffers:** A sniffer is a tool in software or hardware form that can be used to track/-monitor internet traffic in real-time. It can capture all that your computer sends or receive.

- **Spybots:** Spybots can enter our computer system and can collect information about us and transfer all the collected information to a third party.

2.1.2. Rootkits:

Rootkits are designed in a way to modify the Operating System to create a backdoor. They operate in a way that they cannot be detected. These are generally combined with other malware to conceal their code. They can also take advantage of different vulnerabilities to gain remote access [6]. Rootkits can also be used to modify monitoring tools, making it difficult for them to detect. In most cases when a computer is infected with a rootkit it wiped everything on the system for example backdoors to make the code fileless or undetectable for the victim [7].

2.1.3. Backdoor:

The backdoor is the type of malicious code that can be installed inside the computer system to gain unauthorized access without user permissions and gives access to the attacker, when the backdoor is open or get executed, the attacker gets connected to the target computer with no authentication it's like C2C Server (Command and Control Server)[8]. The attacker can easily execute commands on the target computer. It usually works in the Background, and it is difficult to detect.

2.1.4. Worms/Virus:

The main purpose of worms is to duplicate themselves to spread from one computer to another; they make multiple copies of themselves to consume more ram and to make the computer slow some things it gets hanged and unable to respond. Worms can be run by themselves for example **ILOVEYOU** worm is the famous one it comes with a .vbs extension, **Stuxnet** is responsible for causing damage to the **Nuclear Program of Iran**. The virus can also be programmed to bypass the AV detection most of them are spread by CDs, unusually downloading, attaching USB, etc.

2.1.5. Spam-Sending Malware:

In Spam-Sending Malware, malware enters the target system infects the system and uses that system to send spam mails. It also provides spam-email sending services, most of the users buy this for their marketing and business purpose.

2.1.6. Ransomware:

Ransomware enters into your computer system to encrypt all the files present in your computer and ask for a ransom to open or decrypt them. It changes the extension of the files, so it becomes impossible for the user to open that file without the key. Ransomware is usually spread with phishing emails it encourages the user to download the malicious file and then in this way it can affect the targets. Attackers ask for ransom in Bitcoin form. The Bitcoin address is visible to you. One of the popular ransomware attacks is **WannaCry** .

2.1.7. Scareware:

Scareware works in a way that frightens the user. It uses **scare** technique to trap the user to perform a specific action for example to buy something. Scareware usually has a GUI interface like and trusted antivirus or security program. It tells the user that there is some virus or bug in your system that can only be removed by their software in that way user buy their software. For example, when we are scrolling social media apps some advertisements come and display there is a virus in our mobile or laptop with the mobile or laptop model. In this way, scareware trapped their victim [9].

2.1.8. Adware:

Adware is designed to deliver advertisements automatically to the target. Adware is usually Web-Browser Based. It is very difficult for a normal user to ignore it when these are constantly popping on the target screen. It usually comes with spyware.

Fig 1. Shows the malware categories in detail.

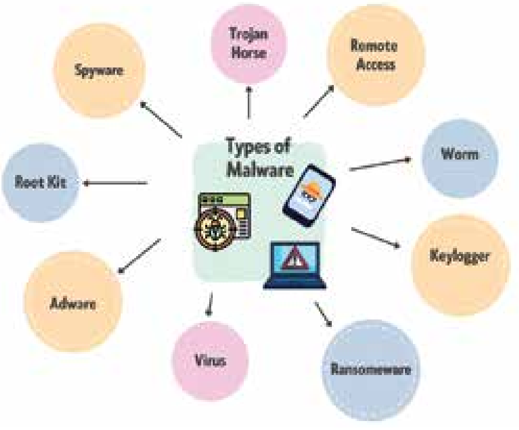


Fig 1. Malware categories

2.2. Malware Detection Approaches:

Malware detection is mainly carried out through machine learning and artificial intelligence. The malware detection techniques can be broadly categorized into signature-based, behavior-based, heuristic-based, model-learning-based, and deep-learning-based.

2.2.1. Signature-based detection:

A signature is a set of bits that uniquely identifies the structure of a program. Signatures are commonly employed in malware identification because each program's signature is unique. The static properties of executable files are first discovered during the signature extraction process. The signature generating engine then uses the extracted features to create signatures. When a suspected sample file must be classified as malicious or benign, the file's signature is retrieved and compared to previously identified signatures. The sample file is classified as harmful or benign based on the comparison. Signature-based malware detection is the term for this method. When it comes to detecting known malware, this method is quick and effective. It, on the other hand, is unable to detect zero-day malware. Furthermore, signature-based malware detection is no longer viable because it cannot detect new malware variants, is inefficient, and requires human engagement.

2.2.2. Behavior-based Detection:

The sample program's activities are tracked in a behavior-based detection approach. The sample program is classified as malicious or benign based on the observed behaviors. The three aspects of this approach are: extracting behaviors, creating attributes, and utilizing machine learning algorithms to determine whether the studied program is dangerous or benign. System calls, API calls, or changes in the file, registry, and computer network are utilized to determine behaviors. To put it another way, the order or frequency of system calls and file-registry actions is used to influence behavior [10]. Even if the source code of software changes over time, the program's behavior does not. As a result, this method can be used to identify a variety of malicious software variations. Furthermore, this technique can detect previously undiscovered novel malware. The most significant disadvantage of behavior-based detection is that malware does not exhibit all of its true characteristics in a protected environment like virtual machines or sandboxes. Using cyber threat intelligence, machine learning, and data forensics, a new hybrid approach based on dynamic analysis has been developed [11].

2.2.3. Features-Based Detection:

Heuristic-based detection is a multi-technique detection strategy. Certain guidelines and machine learning approaches are used in this experience-based approach. To produce rules, the heuristic technique can use both strings and behavior-related data [12]we investigate the stability of a susceptible-infected-susceptible epidemic model incorporated with multiple infection stages and propagation vectors to mimic malware behavior over scale-free communication networks. In particular, we derive the basic reproductive ratio (R{0}. Signatures are made by those requirements. It's mostly used to identify various types of malware, as well as malware that has never been seen before. To begin, the system is taught using specific features. First and foremost, the system is taught using certain features. Anomalies are then discovered by testing the data. Although the success rate for detecting new malware is high, because of optimization concerns, the rate of false positives (FP) and false negatives (FN) is also high.

2.2.4. Model-learning based detection:

Malicious and benign characteristics are retrieved and coded using linear temporal logic formulas to identify feature relationships, which are referred to as specifications, in the model checking-based detection approach. Flow linkages between behaviors that employ hiding, spreading, and injecting actions are used to extract program properties. The properties collected are compared to the previously determined parameters to classify the sample software file as malware or benign. The file is classified as malicious or benign based on the comparison. This method is impervious to stealth and packing techniques, and it can detect a part of new malware versions.

2.2.5. Deep-Learning Based detection:

Deep learning is a branch of AI that learns from examples and inherits from artificial neural networks (ANNs). Deep learning is widely utilized in sectors like image processing, self-driving cars, and voice control, but it isn't generally used in malware detection and categorization. The deep learning-based detection strategy works well and decreases the feature dimension significantly, but it is vulnerable to evasion assaults [13][14]. Furthermore, constructing hidden layers takes a long time, and adding more hidden layers only improves performance slightly. Because deep learning hasn't been widely employed in malware detection and classification, additional academic research is needed to accurately assess this method [15].

Fig. 2 depicts malware detection approaches in taxonomical form.

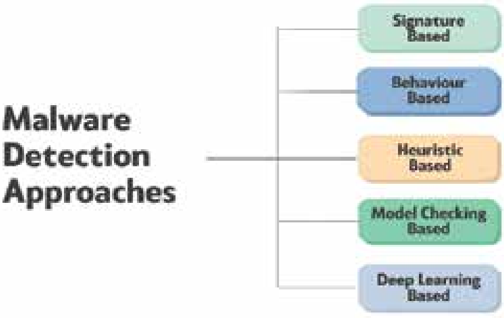


Fig. 2. Taxonomical representation of malware detection approaches

2.3. Malware Detection for various devices:

Malware Detection detects intrusions by monitoring the malware activity on different platforms and classifying it as normal or dangerous. This classification is often based on machine learning algorithms that use different types of rules to detect them instead of detecting them with signatures and patterns.

2.3.1. Malware Obfuscation Techniques:

The technique that malware researchers used to conceal their code so that it becomes difficult for the victim and AV to read or understand it this technique is called **Obfuscation Technique.**

2.3.2. Malware Detectors:

A Malware detector is a program that is used to detect malware it is largely based on rules, hashes, and signatures.

Malware Detection is Based on

- Signature-Based Detection
- Behavior-Based Detection

2.3.3. Signature-Based Detection:

The most widely used malware detection method is the detection of malware by signatures. Instead of going for behavior detection methods, malware detection has largely focused on completing the signature-based analysis. In signature-based detection, all the signatures of known malware were stored when malware tries to enter the system it checks whether its signature is stored in our database or not. If the signature matches then it is confirmed that it is malware. Signature-based rely on extraordinary raw byte examples or standard articulations, referred to as marks, made to organize the harmful document [16]. Static detection of data, for example, previous signatures are used to determine whether it is malware or not. The fundamental advantage of signature-based approaches is their depth, as they cover all possible document execution contexts [17]accurate detection is challenging due to the constantly evolving nature of the malware variants that cause concept drift. Existing malware detection solutions assume that the mapping learned from historical malware features will be valid for new and future malware. The relationship between input features and the class label has been considered stationary, which doesn't hold for the ever-evolving nature of malware variants. Malware features change dynamically due to code obfuscations, mutations, and the modification made by malware authors to change the features' distribution and thus evade the detection rendering the detection model obsolete and ineffective. This study presents an Adaptive behavioral-based Incremental Batch Learning Malware Variants Detection model using concept drift detection and sequential deep learning (AIBL-MVD.

2.3.4. Mobile-Malware Detection Techniques:

Mobile Malware Detection Techniques are divided into two categories:

- Static Techniques
- Dynamic Techniques

Fig 3. Represents a mobile computing device.

Fig. 3. A mobile computing device

2.3.5. Static Technique:

The static technique mainly relies on the source code of an application to classify it accordingly without having the application being executed. These techniques are classified into one of the following classes according to the basis they rely on for analyzing source code [18].

2.3.6. Signature-Based Detection:

A program is classified as malware or a type of malware if its signature matches the existing signatures. This is a very fast method. AV can only identify the existing malware and fails against the unseen variants of malware. It also needs an immediate update of malware signatures.

2.3.7. Dynamic Techniques:

In Dynamic analysis, an application is examined during its execution, and then it is classified according to one of the following techniques. The Classification is done according to the behavior of the detection mechanism.

2.3.8. IoT-Malware Detection Techniques:

IoT is moreover inside the midst of numerous information safety vulnerabilities and exploits. Risks of connecting networks if we tend to take below consideration the technical possibilities of devices moreover to their specific weaknesses, the benefit with those hackers will sight them, and their anticipated proliferation worldwide. And the projected global impact becomes simply evident in any elegant surroundings. Internet of Things (IoT) practice includes internet-based gadgets, internet-based cars, embedded structures, sensors, and alternative gadgets or systems that have a manner of autonomy[19]. The manner of shifting as well as aggregation understanding. IoT would possibly moreover be deployed inside aggressive ways fee the object of terrain like Security teams uses an electromagnetic field to detect malware in an IoT Device[20]. This will even work in obfuscation cases.
Fig. 4. Shows different IoT devices.

Fig 4. IoT devices and malware

The recent finding presented by security researchers from the **Research Institute of Computer Science and Random System (IRISA)** at the **Annual Computer Security Applications Conference (ACSAC)**

- Attackers use the others channel info to discover anomalies in emanations after they range from previously determined patterns and suspicious behavior in the system's normal state

- Without making any modifications in the method, this method enables detection along with the classification of rootkits that required administrative rights, ransomware, or some new malware

- The electromagnetic emanation calculated from the device is almost undetectable by the malware.

During the research Malware Researcher uses the Raspberry Pi 2B model as a target device with 1GB of Ram and 900MHZ quad-core ARM Cortex A7 processor combined with the 303 BNC preamplifier. With an accuracy of 99.82 percent and 99.61 percent, this system was able to detect three malware families.

The method involves three phases: measuring electromagnetic fields while executing 30 different malware binaries, performing benign activities to train a Convolutional Neural Network (CNN) model to classify malware samples, and instructing a Convolutional Neural Network (CNN) model to classify malware samples.

- The framework takes an executable as input and uses side-channel information to generate malware labels.

- Researchers were able to acquire useful information about the state of a monitored device by using simple neural network models.

- It works against a variety of code obfuscation/transformations, including random trash injection, hypervisor, and packaging, as well as a previously unknown transformation.

Concluding this example, we can say that IoT appliances are a lucrative target for cybercrime due to their rapid development and usage. The attack surface is much larger, making stealthy malware harder to identify. To mitigate potential security threats, researchers are required to develop malware analysis techniques.

2.3.9. Malware Detection on Computer System:

As software evolves and improves, it also develops vulnerabilities, requiring the deployment of security patches. Furthermore, Operating system security vulnerabilities are becoming increasingly significant. Older versions of operating systems receive fewer and fewer upgrades with each new release until manufacturers stop supporting them permanently. Companies that are either unable to upgrade or want to ensure compatibility with legacy software continues to employ operating systems with known vulnerabilities. As a result, the issue of legacy operating systems remains vital. Detecting malicious software, or "malware," within features extracted is widely misunderstood, and usually consists of just running an antivirus scanning application across an acquired image mounted as a volume. Malware detection is divided into four stages: analysis, categorization, detection, and eventual containment. A typical cloud computing system has been represented in Fig.5.

Fig.5. A typical cloud computing environment

Several classification strategies have been used to classify malware according to their occurrences, allowing for the recognition of a virus's type and activities, and also new types. Malware analysis entails finding malware samples using multiple classification techniques based on properties of known malware characteristics. Malware detection refers to the process of quickly detecting and detecting any instance of malware to prevent additional system damage.

- **Web Application Firewall(WAF):** The Imperva cloud PCI DSS compatible technology, which is deployed at the edge of your network, uses signature, behavior, and reputational analysis to block all malware injection attempts on your websites and online applications. Imperva Cloud WAF is available as a managed service that is supported by a security team.

- **Backdoor Protect:** On your web server, software that intercepts communication attempts using backdoor shells. The service can pinpoint the most highly obfuscated malware by monitoring these requests, even if it was installed on your web server before you signed up for

Imperva cloud protection services.

- **Login Protect:** A two-factor authentication (2FA) solution that requires no connectivity and can be deployed on any Imperva cloud-protected URL address in seconds. The service prevents cybercriminals from gaining network access and installing rootkits and backdoors on your web servers using stolen login information such as username and password.

- **Yara Rules:** The term YARA belongs to malware research and detection tool. It uses a rule-based approach to generate malware family descriptions based on textual or binary patterns. A description is just a Yara rule name, with these rules being grouped.

2.4. Types of malware analysis

Malware analysis can be broadly categorized into two categories i.e., static analysis and dynamic analysis. The static analysis refers to the analytical review of any malware through code inspection, string search, etc. However, for dynamic analysis, the malware is executed in a protected virtual environment (i.e., sandbox) for its behavior inspection. Fig. 6 represents malware analysis taxonomy.

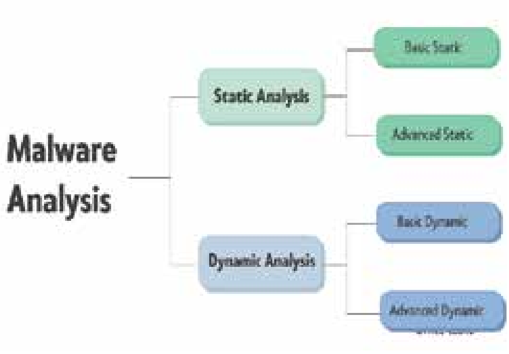


Fig. 6. Malware analysis taxonomy

2.4.1. Static analysis

Static analysis is based on the idea of examining the malicious program without executing the program. As running the malicious program can affect your system, this is a secure way to examine the malware. Static analysis shows a program or file is malicious, gives information about its functionality. Static Analysis is divided into parts: Basic static analysis and advanced static analysis. In Basic static analysis, header information, metadata such as filename, sizes are analyzed. Also, Md5 checksums and hashes are compared with the previously detected malware. Tools like BinText, PEview, MD5deep, and PEid are used to obtain this information. Basic static analysis is quick and simple, and much inaccurate for sophisticated malware. In advanced static analysis, malware code is examined in detail. One way is to reverse engineer the machine code into an assembly code using a disassembler. Various tools like IDA pro are widely used for this purpose. Assembly codes are analyzed thoroughly to discover the functionalities of malware. Also, malware headers, functions, and strings are analyzed and give much useful information about the malware. The advanced static analysis gives information about the malware's purpose, working, and functionality, however, the analysis requires deep expertise of assembly instructions and concepts of OS.

2.4.2. Dynamic Analysis

Dynamic analysis is the analyzing the instructions of malware by running it and behaviors of the malware is examined; finding what it does and changes on the hosted system, therefore it is also called malware behavior analysis.

Running the malware on the system is a risk, to save the system to get infected by the malware, the dynamic analysis must be done in close environments such as virtual machines and sandbox. Sandbox is an isolated virtual environment thus malware cannot affect the system or transmit on the network. Function calls, parameters, file path locations, the flow of information, registry changes, and network-related activities are examined. There can be two parts of dynamic analysis: basic dynamic analysis and advanced dynamic analysis. The basic dynamic analysis examines the malware's behavior with tools like API monitor, process explorer, process monitor, ApateDNS, Regshot, Wireshark, and virtual environments. In advanced dynamic, debugging tools are used to examine the behaviors; tools like WinDbg, OllyDbg, etc allow the analyst to run every instruction individually for examining the changes made by the malware. Changes can be registry keys, domain names, IP addresses, file path locations, and memory areas. Most of the functionalities can be found in advanced dynamic analysis. Performing analysis on debuggers requires good expertise and knowledge of assembly-level instructions and operating system concepts.

3. Conclusion

Malware is a typical software crafted to disrupt the normal operation of a computing device. Malware comes in wide categories including viruses, worms, trojans, ransomware, rootkits, etc. The effect of malware includes data stealing, device malfunctioning, data transformation, device hacking, and services unavailability. The analysis and detection of malware are extremely important due to their harmful effects on computing devices. The current study dealt with the malware categories, detection, and analysis types, and the mapping of malware with different computing devices. It has been concluded that the research highlights many aspects of malware in terms of its behavior.

4. References

[1] O. Aslan and R. Samet, "A Comprehensive Review on Malware Detection Approaches," IEEE Access, vol. 8, pp. 6249–6271, 2020, doi: 10.1109/ACCESS.2019.2963724.

[2] R. Gupta and S. P. Agarwal, "a Comparative Study of Cyber Threats in Emerging Economies," 2017, [Online]. Available: www.InternetLiveStats.com.

[3] K. Iwamoto and K. Wasaki, "Malware classification based on extracted API sequences using static analysis," Asian Internet Engineeering Conf. AINTEC 2012, pp. 31–38, 2012, doi: 10.1145/2402599.2402604.

[4] G. Cabau, M. Buhu, and C. P. Oprisa, "Malware classification based on dynamic behavior," Proc. - 18th Int. Symp. Symb. Numer. Algorithms Sci. Comput. SYNASC 2016, pp. 315–318, 2017, doi: 10.1109/SYNASC.2016.057.

[5] J. Donahue, A. Paturi, and S. Mukkamala, "Visualization techniques for efficient malware detection," IEEE ISI 2013 - 2013 IEEE Int. Conf. Intell. Secur. Informatics Big Data, Emergent Threat. Decis. Secur. Informatics, pp. 289–291, 2013, doi: 10.1109/ISI.2013.6578845.

[6] X. Ban, C. Li, W. Hu, and W. Qu, "Malware variant detection using similarity search over content fingerprint," 26th Chinese Control Decis. Conf. CCDC 2014, pp. 5334–5339, 2014, doi: 10.1109/CCDC.2014.6852216.

[7] L. Nataraj, S. Karthikeyan, G. Jacob, and B. S. Manjunath, "Malware images: Visualization and automatic classification," ACM Int. Conf. Proceeding Ser., 2011, doi: 10.1145/2016904.2016908.

[8] R. Komatwar and M. Kokare, "A Survey on Malware Detection and Classification," J. Appl. Secur. Res., vol. 16, no. 3, pp. 390–420, 2021, doi: 10.1080/19361610.2020.1796162.

[9] S. Sen, E. Aydogan, and A. I. Aysan, "Coevolution of Mobile Malware and Anti-Malware," IEEE Trans. Inf. Forensics Secur., vol. 13, no. 10, pp. 2563–2574, 2018, doi: 10.1109/TIFS.2018.2824250.

[10] L. Chen, C. Xia, S. Lei, and T. Wang, "Detection, Traceability, and Propagation of Mobile Malware Threats," IEEE Access, vol. 9, pp. 14576–14598, 2021, doi: 10.1109/ACCESS.2021.3049819.

[11] R. Korine and D. Hendler, "DAEMON: Dataset/Platform-Agnostic Explainable Malware Classification Using Multi-Stage Feature Mining," IEEE Access, vol. 9, pp. 78382–78399, 2021, doi: 10.1109/ACCESS.2021.3082173.

[12] A. Dadlani, M. S. Kumar, K. Kim, and K. Sohraby, "Stability and immunization analysis of a malware spread model over scale-free networks," IEEE Commun. Lett., vol. 18, no. 11, pp. 1907–1910, 2014, doi: 10.1109/LCOMM.2014.2361525.

[13] O. Aslan and A. A. Yilmaz, "A New Malware Classification Framework Based on Deep Learning Algorithms," IEEE Access, vol. 9, pp. 87936–87951, 2021, doi: 10.1109/ACCESS.2021.3089586.

[14] "Intelligent vision-based malware detection and classification using deep random forest paradigm."

[15] M. Nisa et al., "Hybrid malware classification method using segmentation-based fractal texture analysis and deep convolution neural network features," Appl. Sci., vol. 10, no. 14, 2020, doi: 10.3390/app10144966.

[16] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, "IoMT Malware Detection Approaches: Analysis and Research Challenges," IEEE Access, vol. 7, pp. 182459–182476, 2019, doi: 10.1109/ACCESS.2019.2960412.

[17] A. A. Darem, F. A. Ghaleb, A. A. Al-Hashmi, J. H. Abawajy, S. M. Alanazi, and A. Y. Al-Rezami, "An Adaptive Behavioral-Based Incremental Batch Learning Malware Variants Detection Model Using Concept Drift Detection and Sequential Deep Learning," IEEE Access, vol. 9, pp. 97180–97196, 2021, doi: 10.1109/ACCESS.2021.3093366.

[18] G. Suarez-Tangil, J. E. Tapiador, F. Lombardi, and R. Di Pietro, "Alterdroid: Differential Fault Analysis of Obfuscated

Smartphone Malware," IEEE Trans. Mob. Comput., vol. 15, no. 4, pp. 789–802, 2016, doi: 10.1109/TMC.2015.2444847.

[19] P. Faruki et al., "Android security: A survey of issues, malware penetration, and defenses," IEEE Commun. Surv. Tutorials, vol. 17, no. 2, pp. 998–1022, 2015, doi: 10.1109/COMST.2014.2386139.

[20] J. Jeon, J. H. Park, and Y. S. Jeong, "Dynamic Analysis for IoT Malware Detection with Convolution Neural Network Model," IEEE Access, vol. 8, pp. 96899–96911, 2020, doi: 10.1109/ACCESS.2020.2995887.

Shairoze Malik *et al.LGU (IJECI)* 2020

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

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 5 issue 4 Year 2021

The Secrets to MIMIKATZ - The Credential Dumper

Shairoze Malik and Erej Azeem
DFRSC - Digital Forensic Research and Service Centre,
Lahore Garrison University - Main Campus, Sector C DHA Phase 6,
Lahore – Pakistan
shairozemalik@lgu.edu.pk, erejazeem00@gmail.com

Abstract:

With the emergence of many credential dumping tools, Mimikatz has become an exceedingly dramatic tool against Windows users that allows the intruders to fetch plain text passwords. Moreover they also target memory to dump password hashes. Mimikatz capacity and potential will be briefly discussed throughout the paper. Several modules of Mimikatz to dump credentials will follow, and the paper will conclude with procedures and techniques that may be used as prevention against Mimikatz attacks that are performed.

Keywords: Mimikatz, hash dump, lsass, modules, kerberos, tickets, krbtg

1. Introduction

This well-known tool known to be as Mimikatz was initially derived in 2011 by Benjamin Delpy also known as *gentilkiwi* in, they proofed and confirmed how the protocols used for authentication of Microsoft were at severe risk to attack. Attackers make use of the vulnerability on Windows System to access internal storage. We can say that he, Benjamin Delpy- the creator of Mimikatz tool created one of the most widely are far apart used and downloaded hacker tools. There are a lot of modules provided by Mimikatz to gather and use Windows credential on targeted systemswhich basically includes recapture of passwords in clear text, LM Hashes (LAN Manager), NTLM Hashes (New Technology LAN Manager), Kerberos tickets [1] which include Golden Kerberos Ticket and Silver Kerberos Ticket. From Windows XP and forward, Mimikatz run on all Windows versions.

2. Concepts to be known

2.1 Active Directory

Active Directory that is also known as AD is a Microsoft's directory service. It is more like a database that runs on Windows server. The use of Active Directory is that is allows administrators to manage the access to resources I.e. network resources and also allows the administrators to manage the user permissions. Everything in Active Directory is stored as an object [2], whereas by object we mean any single element which could be a group, a user, an application or even a device. As said earlier, Active directory stores everything on network as objects allowing the information to be searched and used easier for the administrator.

2.2 NTDS.dit

We would not be wrong if we say that NTDS.dit fie is the heart of Active Directory that stores user accounts. It is basically a (.dit) file that is being used by AD. Because it stores the Active Directory data it is sometimes referred as a database. It comprises of information about the user-objects and multiple attributes are possessed by user objects, groups and also the group membership. Moreover, password hashes for all users in the domain are also stored in this NTDS.dit file [3].

Both LAN Manager (LM) hash and NT hash of the passwords are generated by Windows. Local Security Accounts Manager well known to be SAM database (C:\Windows\System32\config\SAM file) or in Active Directory AD (C:\Windows\NTDS\NTDS.dit file) [4] are basically the locations where these hashes are stored.

2.3 Kerberos

A well-known computer security protocol known as Kerberos authenticates the service requests across a network between two or more hosts, more likely to be across the Internet [5]. A secret key cryptography is used and also a trusted third party for client server authentication and the verification of user’s identities. Kerberos is completely designed to avoid locally storing passwords and to send to send any passwords through the internet providing mutual authentication. By this we simply mean that both the server’s and user’s authenticity is being verified.

2.4 LSASS and LSA

LSASS is the abbreviation of Local Security Authority Server Service and LSA stands for Local Security Authority. Within Windows, the LSASS.exe is an executable for preserving and saving user credentials in memory both for internal (local) and domain users. LSASS is merely an implementation of Local Security Authority. "LSA" is the idea and a conception, whereas "lsass.exe" is a procedure and an action that is implementing many of the LSA functions.

2.5 KDC

A well-known mechanism in cryptography that is a key distribution center (KDC), is in charge for giving keys to users in a network that shares sensitive or confidential data. In a network whenever a connection is established each time, KDC is requested by both for distinctive password generation which is then used for verification by end system users. KDC (a.k.a) Key Distribution Centre is a type of symmetric encryption that allows the access of even more than two systems in a network by bringing about a distinctive ticket type key for shielded connection formation over which data and information is shared or spread out, moved and even transferred. Before the communication takes place, Key Distribution Centre is the main server which is called upon. Key Distribution Centre is typically used in compact grid or networks when link requests do not overwhelm the system due to its central architecture. Instead of standard key encryption, Key Distribution Centre is used because every time the connection is requested, the key is generated each time, which decreases the possibilities of attack.

3. Mimikatz Attack Capabilities

3.1 Pass-the-Hash attack

A well-known tool for extracting hashes and passwords from memory; Mimikatz performs Pass-the-Hash attack from Active Directory user account. In other words, NTLM hash that is used by Windows to deliver passwords is obtained by Pass-the-Hash attack.

3.2 Pass-the-Ticket attack

For impersonating a user on Active Directory Domain there is a method that is well known that is called as Pass-the-Ticket. It fragments and cracks the Kerberos protocol. A Kerberos ticket is obtained for a user account and that can be used to login as that particular user on any other system.

3.3 Kerberos Golden Ticket attack

The encryption of authentication tickets is handled by a hidden root account known as KRBTGT. It is the default Microsoft Windows authentication protocol, Kerberos, which is implemented by Microsoft. The ticket for this hidden root account KRBTGT is obtained through a Kerberos Golden Ticket attack. In a Golden Ticket assault, hackers bypass the KDC and create their own TGTs to obtain access to various resources. A successful Golden Ticket assault grants the hacker near-unrestricted access to your domain's entire infrastructure, including all machines, files, directories, and domain controllers (DCs). They have the ability to impersonate anyone and perform almost any task.

3.4 Kerberos Silver Ticket attack

A faked service authentication ticket is known as a Silver Ticket. Silver Ticket is quite similar to Golden Ticket in that it involves manipulating the Kerberos protocol to gain the hacked system's credentials. An attacker using Silver Ticket can only falsify ticket-granting service (TGS) tickets for certain services. Silver Tickets are more difficult to detect than Golden Tickets because there is no connection between the service and the DC, and any logging is local to the targeted system. Hackers can use a pass-the-ticket technique to raise their access or utilize the service's privileges to gain greater access if they have a Silver Ticket.

3.5 Pass-the-Key attack

Because Pass the Hash is a combination of Pass the Hash and Pass the Ticket, it's also known as Over Pass the Hash Attack. Another variation of pass-the-hash, however this time a unique key is supplied to impersonate a user obtained from a domain controller. To put it another way, it gets a unique key that a user can use to authenticate to a domain controller. This key can be used by the attacker to impersonate the user.

3.6 Pass-the-Cache

A very well-known attack known as Pass-the-Cache attack is somewhat similar to the attack that is previously discussed in this paper called Pass-the-Ticket attack. In this case the login data that is saved, stored and encrypted is used on system that could be MAC, UNIX or even LINUX systems.

4. Mimikatz Modules

4.1 PROCESS Module:

This module of Mimikatz tool is used for dealing with the Windows processes. This module can also be used for process injection [6] and also for the parent process spoofing [7].

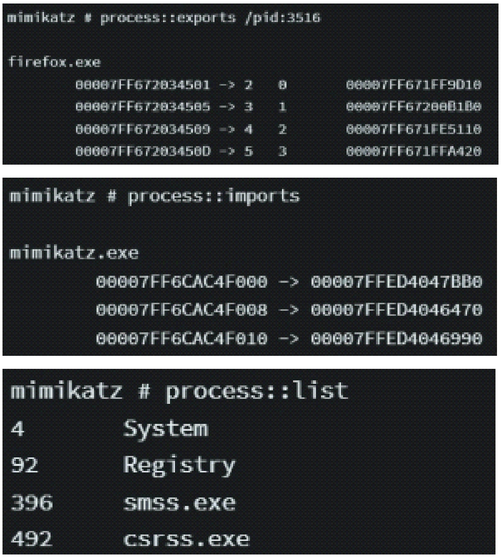
***Export**:* This command in the Mimikatz tool lists all the functions exported from Dynamic Link Libraries, which are files that contain code for commonly used programs that each running process uses. If a process ID, often known as /PID, is not given, the results displayed are mimikatz.exe exports.

Import: this command is used for listing all the functions imported from the Dynamic Link Libraries each running process is using. If a process ID that is also known as /PID is not specified, then the results displayed are the imports of mimikatz.exe.

List: This command is used for listing all running processes.

Commands:

PROCESS::*export*
PROCESS::*import*
PROCESS::*list*



```
mimikatz # process::exports /pid:3516

firefox.exe
        00007FF672034501 -> 2   0       00007FF671FF9D10
        00007FF672034505 -> 3   1       00007FF67200B1B0
        00007FF672034509 -> 4   2       00007FF671FE5110
        00007FF67203450D -> 5   3       00007FF671FFA420
```

```
mimikatz # process::imports

mimikatz.exe
        00007FF6CAC4F000 -> 00007FFED4047BB0
        00007FF6CAC4F008 -> 00007FFED4046470
        00007FF6CAC4F010 -> 00007FFED4046990
```

```
mimikatz # process::list
4       System
92      Registry
396     smss.exe
492     csrss.exe
```

Figure 1: mimikatz tool showing the use of export, import and list commands.

4.2 STANDARD Module:

In Mimikatz, the Standard module commands can be typed unaccompanied by the module name i.e. STANDARD. The purpose of Standard module do not need to be prefixed with "standard" [8]. They can easily be requested at first hand from the Mimikatz.

Commands:

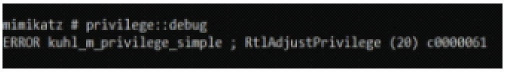
Log: This command is used for journaling steps and operations or we can even say actions and then just easily taking down the logs that is the time-stamped documentation.

Module privilege: This command contains some accommodation to work with privileges while functioning and running with Mimikatz.

Sleep: In Mimikatz, this command switches to sleep mode within the particular defined seconds.

base64: This command in the tool show or exchange the condition or state of input or output to the Base64.

Cd: Current directory is displayed or changed by this specific command.

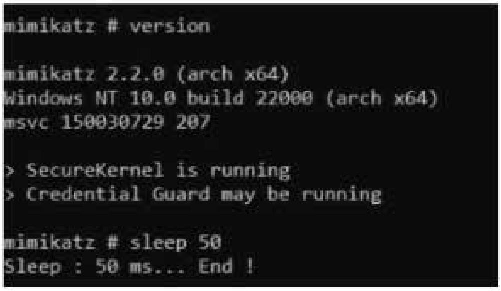


```
mimikatz # privilege::debug
ERROR kuhl_m_privilege_simple ; RtlAdjustPrivilege (20) c0000061
```

Figure 2: privilege::debug when not in root

ERROR:

kuhl_m_privilege_simple; RtlAdjustPrivilege (20) c0000061 this error exactly means that the client or user does not hold the required privileges that is mostly the case when you are not the administrator.



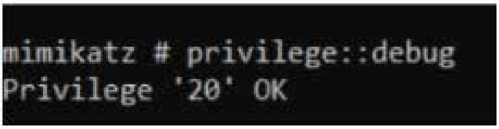
```
mimikatz # version

mimikatz 2.2.0 (arch x64)
Windows NT 10.0 build 22000 (arch x64)
msvc 150030729 207

> SecureKernel is running
> Credential Guard may be running

mimikatz # sleep 50
Sleep : 50 ms... End !
```

Figure 3 : Standard module commands

Running as Administrator:

Command: privilege::*debug*

We get the following output as shown in figure:



```
mimikatz # privilege::debug
Privilege '20' OK
```

Figure 4: privilege::debug when in root

4.3 NET Module:

NET module functionality are very much similar to the Windows net commands.

Alias: This command displays much of the information about the memberships (local groups) also including the Remote Desktop Users.

Group: This command of NET module displays the local or internal groups.

***If**:* If lists the available hostnames and the local IP addresses.

Serverinfo: serverinfo command will exhibit data about the logged in server.

Session: lists the active running sessions.

Share: available shares are displayed by this share command of NET module

Commands:

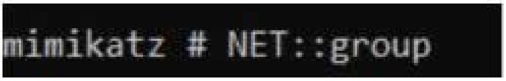
NET::*group*

NET::*if*

NET::*serverinfo*

NET::*:session*

NET::*share*



```
mimikatz # NET::group
```

Figure 5: How to utilize NET module commands

4.4 CRYPTO Module:

The CRYPTO Mimikatz module comes up with modern potential and capacity to interface with Windows cryptography functions (CryptoAPI) [9] i.e. Cryptography Application Programming Interface.

***Capi*:** This command patches Crypto API layer for the purpose of easy export.

Certificates: This command of Crypto module of Mimikatz tool is used to list and export certificate.

Hash: This command provides hash of a password with optional username that is being provided.

Keys: Key container are listed and exported by this key command.

Providers: providers of cryptography are listed by this command.

Stores: This command lists the cryptographic stores.

Commands:

CRYPTO::*CAPI*

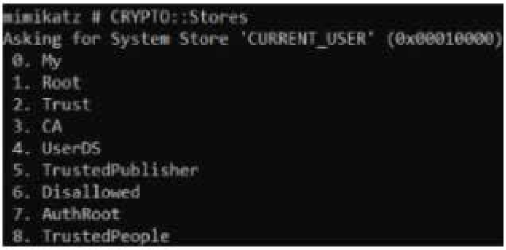
CRYPTO::*Certificates*

CRYPTO::*Hash*

CRYPTO::*Providers*

CRYPTO::*Stores*

CRYPTO::*Keys*



```
mimikatz # CRYPTO::Stores
Asking for System Store 'CURRENT_USER' (0x00010000)
 0. My
 1. Root
 2. Trust
 3. CA
 4. UserDS
 5. TrustedPublisher
 6. Disallowed
 7. AuthRoot
 8. TrustedPeople
```

Figure 6: Listing down the cryptography stores

4.5 DPAPI Module:

The (DPAPI) that stands for Data Protection API that basically helps in data protection. The DPAPI, Data Protection API Mimikatz module comes up with the proficiency for pulling out

Windows stored and saved (and even protected) credential data using DPAPI module. DPAPI is the Windows official method to preserve or encrypt local or internal data that are usually the passwords. A DPAPI blob [10] is a non-transparent binary structure, containing the private data of the applications that are encrypted using DPAPI.

Blob**:** This specific command is used to unprotect a DPAPI blob with a master key or application programming interface.

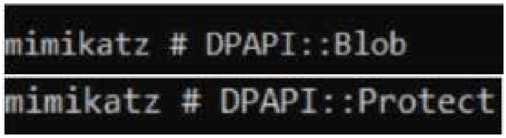
Chrome/in:"%localappdata%\Google\Chrome\UserData\Default\LoginData" /unprotect*:* This command of DPAPI module dumps credentials that are stored and also the cookies from the Chrome browser. ***Protect*** – This command protects data using DPAPI.

Commands:

DPAPI::*blob*

DPAPI::*chrome/in:"%localappdata%\Google\Chrome\UserData\Default\LoginData"/unprotect*

DPAPI::*protect*



```
mimikatz # DPAPI::Blob
mimikatz # DPAPI::Protect
```

Figure 7: DPAPI blob and protect commands

4.6 SEKURLSA Module:

Dumping the passwords from the memory is possible using the SEKURLSA module of Mimikatz tool. To use the commands of the SEKURLSA module we need to have root permissions or else we will face errors.

Logonpasswords*:* This command displays a list of all accessible provider credentials.

Krbtgt**:** This command helps in getting the password data of Domain Kerberos service account (KRBTGT).

Kerberos: For all the authenticated and verified users. this command lists Kerberos credentials.

Tickets /export: Kerberos tickets of all sessions are exported and listed by this command.

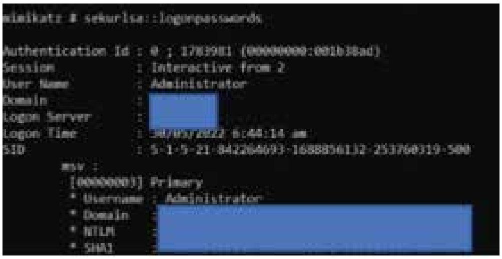
Commands:

SEKURLSA::*Logonpasswords*

SEKURLSA::*krbtgt*

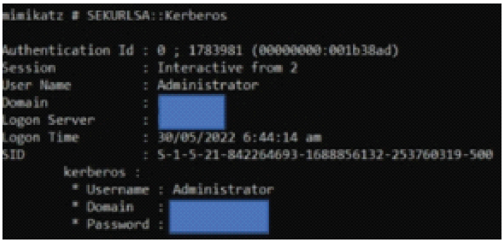
SEKURLSA::*kerberos*

SEKURLSA::*tickets /export*



```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1783981 (00000000:001b38ad)
Session           : Interactive from 2
User Name         : Administrator
Domain            : [redacted]
Logon Server      :
Logon Time        : 30/05/2022 6:44:14 am
SID               : S-1-5-21-842264693-1688856132-253760319-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : [redacted]
         * NTLM     :
         * SHA1     :
```

Figure 8: Recently logged on user credentials



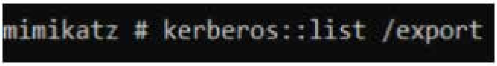
```
mimikatz # SEKURLSA::Kerberos

Authentication Id : 0 ; 1783981 (00000000:001b38ad)
Session           : Interactive from 2
User Name         : Administrator
Domain            : [redacted]
Logon Server      :
Logon Time        : 30/05/2022 6:44:14 am
SID               : S-1-5-21-842264693-1688856132-253760319-500
        kerberos :
         * Username : Administrator
         * Domain   : [redacted]
         * Password :
```

Figure 9: Listing kerberos credentials

4.7 KERBEROS Module:

It is of great interest that he Kerberos module is capable of being used without the need of any privilege or Admin rights. Microsoft Kerberos API is involved and produces and generates the Golden tickets.

Tgt: Information about the current session is displayed by this command of Kerberos module of Mimikatz tool. ***List /export:*** The Kerberos Tickets are listed by this command.



```
mimikatz # kerberos::list /export
```

Figure 10: Listing Kerberos Tickets

5. Famous Attacks Performed Using Mimikatz

5.1 Notpetya Cyber Attack

Notpetya a well-known malware whose prime target was Ukraine left multinational companies with many knocked down computer systems. In Windows devices the remaining credentials that are stored in RAM were the target of this malware called Notpetya [11]. This attack was only possible when accounts were logged on at the run time because that is when LSASS memory loads the credentials which are then hijacked by the Mimikatz tool. Notpetya spread escalated through the patched and not patched devices both without mercy with the union of Mimikatz and Eternal Blue [12]. Credentials from patched machines were withdrawn with Mimikatz whereas credentials from not patched devices were pulled out with Eternal Blue.

5.2 Bad Rabbit Ransomware

A type of Crypto Virus known as Bad Rabbit was mainly designed for a specific purpose that is to lock or encrypt files through Drive-by-Attack [13] where not secure web pages are compromised. Using the JavaScript, the Bad Rabbit ransomware is inoculated into the websites HTML code. The infected file is somehow downloaded and looks safe. It does not infects the computer system unless and until the file is opened of executed [14]. It will lock the computer showing its ransomware capacity once it is clicked. This ransomware will then gather credentials using the credential dumper well known tool called Mimikatz.

6. Defensive Approach Against Mimikatz Attacks

6.1 Updating Your Operating System On Your Windows Server

Updating your operating system on your windows server will provide more security against the Mimikatz attacks. So this prevention suggested should be in the to-do list. Many corporations security features are not available unless and until the functional level of Active Directory a.k.a AD is not updated to some present-day category version.

6.2 Debug Rights For Local Administrators To Be Disabled On All Servers And Workstations

To bypass many of the local protections, Windows has a mode known as "Debug Mode". The main purpose of this Debug Mode relates to the troubleshooting process mainly to be named as troubleshooting the device drivers and many more. In newer Operating Systems, this is a default setting and to simply disable this particular setting mode in MS Configuration, navigate to the boot/Advanced options and disable "Debug".

6.3 In Active Directory Disable The Storage Of Plain Text Passwords And Password Caching

Password decryption was back in time decided to be enabled for users which maybe sadly still remains with us. In addition, if no Domain Controller [15] is accessible, Windows will cache the up to the minute number of authentications, which includes the password hashes.

6.4 Change The KRBTGT Account Password

Administrators of Active Directory neglect changing passwords of the KRBTGT account that provides the Golden Ticket to the attackers providing the admin rights. There is one more thing to take in consideration about the Active Directory that it preserver the past and current passwords both so therefore, changing the passwords twice would be a best consideration, ensuring that the two password resets are completely synchronized in Active Directory AD.

7. Conclusion

The exceptionally impressive tool mainly invented for penetration testers now being also used by the Cyber criminals for malicious motives - Mimikatz, attacks pertinent Windows systems to gain privilege and dump credentials from the memory. This paper has covered many sections including the attack capabilities and modules of Mimikatz followed by the Prevention steps to be taken against these attacks. The Mimikatz tool keeps on updating its functionality so the defenders must take appropriate steps to protect against the attacks performed using Mimikatz.

8. References

[1] https://www.techtarget.com/searchsecurity/definition/Kerberos

[2] https://networkencyclopedia.com/object-in-active-directory/

[3] https://www.windowstechno.com/what-is-ntds-dit-and-where-its-held-what-other-folders-are-related-to-ad/

[4] https://www.elcomsoft.com/help/en/esr/esr_system.html

[5] https://web.mit.edu/kerberos/

[6] https://medium.com/csg-govtech/process-injection-techniques-used-by-malware-1a34c078612c

[7] https://www.ired.team/offensive-security/defense- evasion/parent-process-id-ppid-spoofing

[8] https://redteam.wiki/postexploitation/mimikatz/standard

[9] https://networkencyclopedia.com/cryptoapi/

[10]https://www.insecurity.be/blog/2020/12/24/dpapi-in-depth-with-tooling-standalone-dpapi/

[11] https://www.trellix.com/en-us/security awareness/ransomware/petya.html

[12] https://www.sentinelone.com/blog/eternalblue nsa-developed-exploit-just-wont-die/

[13] https://encyclopedia.kaspersky.com/glossary/drive-by-attack/

[14] https://www.proofpoint.com/us/threat reference/bad-rabbit

[15] https://www.varonis.com/blog/domain-controlle

Hafiz *et al.LGU (IJECI)* 2020

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

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 5 issue 4 Year 2021

Biometric Attendance Techniques in COVID-19: A Review

Hafiz Burhan Ul Haq[1], Akifa Abbas[2], Muhammad Amjad Khan[3], Memoona[4], Sabreena Nawaz[5]

[1]Burhanhashmi64@gmail.com, akifaabbas19@gmail.com[2],
amjad97@gmail.com[3], memoona1291@gmail.com[4] ,sabreena.nawaz02@gmail.com[5]
University of Education

Abstract:

Now a days COVID-19 is spreading everywhere that has badly affected the countries in social as well as economical perspectives. According to SOP's people have to maintain social distance, use face mask and avoid biometric devices for attendance in order to prevent the corona virus. Several techniques have been developed in order to maintain the attendance in Covid-19 pandemic by considering the precautions to reduce the spread of corona virus. This paper provides the review on the biometric techniques such as face recognition, palm recognition, face mask detection, face recognition and iris detection techniques adopted in COVID-19 to maintain/mark the attendance in an organizations/institutes. However, the challenges of the Covid-19 techniques also are part of this paper that highlights the issues in current techniques. The prime focus of this study is to differentiate biometric method for researchers or users to decide which tools are better for their requirements.

Keywords: *Covid-19, Face recognition, Palm recognition,Face mask detection, Irisdetection*

1. Introduction

Biometrics were introduced in 500 BC in Babylonian empire. In 1800s, Paris, France, first biometric identification system was recorded. Edward Henry developed the standard of fingerprinting known as Henry Classification System. This was considered the first system which can identify the unique architectures of fingerprints. However, the system was acquired by law enforcement for identifying the criminals [1].

Similarly, in 1960s, semi-automated facial recognition were developed. This recognition can be used for unlocking the phone. The law enforcement adopted fingerprint and facial recognition methods and FBI (Federal Bureau of Investigation) invested in its development. This was incentive in developing biometric sensors for capturing and extracting data. In 1991, facial detection technology was originated for real time recognition. The first iris recognition system was registered in 1994 and unique features are revealed which can be used for authentication [1]. In 1999, Southern Minnesota Beet Sugar Cooperative (SMBSC) was the first organization which used an iris based time and attendance solution. They wanted to modern and automate their punch card based time and attendance solution and they go for biometrics. They decided that hand free approach will be suitable for meeting their needs. As a solution they integrated iris based method [2]. By 2000s, hundreds of biometric authentication and recognition systems and algorithms were registered in USA. Research in biometric is still advance and continued [1].

Before biometrics, manual attendance system was used for employees and students. By using this approach, many drawbacks which include error, time consumption, ineffectiveness, inconsistency and difficulty to maintain large records has been observed. To overcome these issues, we switched to biometrics based attendance systems which included finger print scanning, thumb scanning, palm scanning, facial recognition, iris recognition and signature based systems. These systems verify the input data in database and confirm identity according to information defined by admin and mark record of authorize person. By using biometric system, users can achieve accuracy and consistency in a simplified manner. It has also enhanced user security and privacy.

In COVID-19 Pandemic, physical interaction is restricted and avoided. Biometric attendance system which includes thumb scanning or fingerprint and signature-based system involves physical touch which is risky for human health and it increases chance to be infected by corona virus. So in COVID-19 pandemic we move to those biometric systems and methods which are touch-less such method are facial recognition, touch-less fingerprint scanning and iris recognition. By adopting these touch-less technologies in any organization include schools, offices, universities and factories in order to provide safe and secure environment and to reduce the causes of spreading COVID-19. Our review is on biometric methods and techniques adopted in COVID pandemic. This will help the lay man to understand which technique is more suitable for its work or organization to prevent it-self or employee from corona virus.

2. Biometric Based Techniques Adopted in Covid-19 Pandemic

2.1. Face Recognition Systems

AI (Artificial Intelligence) has powered contactless system which is developed for marking the student attendance automatically by recognizing their faces. An attendance report has been generated which is customized. Machine Learning algorithms and neural networks are used in this system. Neural networks are composed of artificial neurons having set of algorithms. Convolutional Neural Network (CNN) applied to monitor the contact-less attendance system. Pre- trained models which are basis of computer vision are used. For faces, feature extraction is concluded and is stored separately. The proposed system method is compared with other methodologies including Radio Frequency Identification (RFID), Support Vector Machine (SVM), Linear Discriminant Analysis (LDA), Principal Component Analysis (PCA) and the resultantly achieved accuracy is 95%. [12]. A campus health information system is introduced that consist of multiple IOT devices, cloud database and personal cloud Pod. It can detect and record the identity and real-time body temperature and it sends that data to the cloud automatically. Then, the centrally managed data is distributed to the personal cloud Pod. The personal cloud Pod holds all data. To activate the decentralized data management, the decentralized data management model permit students to control the server. [10] Covert Human Intelligence Source (CHIS) and its structure is proposed. Covert Human Intelligence Source (CHIS) consist of plural face recognition and body temperature detection devices, group of decentralized personal cloud data models and two cloud databases. CHIS consist of the Face Recognition Temperature Detection Device (FRTDD) part, cloud database part and the personal cloud Pod part. The FRTDD is basically the data collection part which is constructed by Raspberry Pi camera and infrared sensor AMG8833. The main processes are initialization, Daily Processing and nightly updated. Two JSON data objects named User Data Object and IoT Data Object are created in the cloud database to run with FRTDD. The user data object saves the user information and the IoT data object saves the detected information. [13]. For the identification of faces in online attendance, web-based tool is developed. Two algorithms are used to propose this system, one is Local Binary Pattern Histogram (LBPH) and the other one is Convolutional Neural Network (CNN) for recognizing face. Also Haar cascade classifier is used for boosting the detection. LBPH visual descriptor is used for classification in computer system. In CNN, deep learning method used to input image or assign relevance make up Multiple Layers of artificial neurons. Accuracy found in CNN is 95% while in LBPH is 78% [15]

2.2. Touch-less fingerprint/Palm scanning

A device is developed which uses a method achieving contactless fingerprint scanning, precisely and enhancing the correlation factors. The proposed method consist of high precision of acquisition process of fingerprint as well as effective fingerprint architectural technique. Two proximity sensors of infrared have been used with contactless fingerprint scanner microcontroller (using Arduino IDE). It synchronize the sensors by using laser beam and the aperture of camera in scanning process. In scanning, the distance of 3.5 cm was found optimal between camera and targeted finger having correlation factor of 59.9%. Reports has revealed that the white light and other radiations having longer wavelength are absorbed by the layer of skin. So blue light is used as an alternative which is less absorbed by the skin. It results in enhancing the correlation factor and generating in high resolution fingerprint image. Then the highest correlation factor achieved is 78.12% at 280 lm [3]. Shao & Zhong [18], proposed a system for open set touch less palm print recognition. They use novel deep metric based method W2ML [34]. To improve the ability of generalization, deep metric learning feature extractor is learned in Meta way. To define query and support sets, multiple sets are sampled which then combined into Meta sets. Hard sample mining and weighting are conducted to select informative Meta sets in order to improve efficiency. The accuracy is increased by 9.11% and the EER is decreased by 2.97%.

2.3. Face recognition with mask

A smart attendance system is developed by using face recognition algorithm, deep learning techniques, open CV, python and caffe layer network. Mainly two tasks are performed by this system. Firstly, face mask detector is trained to check if the person is wearing mask or not. It will be classified as with mask or without mask. Secondly, the person identification will be identified with mask. The variability changes in human faces such as expression, mask, scarf, difficulty will be faced in this model [5]. A US health center 'Client' decided to move to the face recognition time attendance system for eliminating the spread of corona virus. The tools and technologies used in this system include pytorch, python, OpenCV, faiss, and augmentations. The main focus is to detect face with mask. The system is trained to detect the employee identity who is wearing mask by recognizing facial attributes (forehead, eye, facial hair etc). Time clock entry is also added into the system. Different experiments are concluded by using different masks with multiple people and the system accuracy achieved is 91% [6]. KENT RO Systems Limited, announced Kent Cam Attendance, a Next-Gen Touch-less Attendance System based on Facial Recognition and Artificial Intelligence (AI). This system is the extension of AI product portfolio which was introduced with KENTCamEye. The system used computer vision which is AI based for capturing and recognizing the face of an employee and attendance will be marked. The records are managed by secured cloud application. It includes extra features like inbuilt algorithm for optional mask detection and have a smart alert in case of any person not wearing a mask. Also this system include patented algorithm for real person detection. The face recognition takes less than a second achieving accuracy of 99.9 % [7]. Keshavdas, M. [8] proposed a contact less system which uses facial recognition technology for identifying the student facial features and marking attendance automatically. This system can work with cloud or on local server or can provide hybrid solution. However, this system also have features for detecting mask and thermal sensors are integrated for checking fever of the scanned person. The system can identify four thousand unique faces. Depending on the need, it can be scaled up to sixty thousand plus faces. AttendX-Net facial recognition is developed by using ResNet method, multi-layer feed forward network and faiss. The face will be scanned through face detection module then AttendX-Net API will extract the 128-d vector according to architectures (AttendXNetV1 [29], AttendXNetV2 [30], AttendXNetV3 [31]) for verification. In results, AttendXNetV1 and AttendXNetV2 are having more accuracy than AttendXNetV3 [32]. The system can also identify the human wearing mask. In the trials, 49 people are detected in which 17 were men and 32 were women. From 882 trials, when wearing mask the accuracy achieved was 56% and when not wearing mask the accuracy achieved was 79%. The correct total percentage for men was 78% of 612 trials and for women it was 77%. Therefore, the overall 68% accuracy achieved [11]. A multi granularity masked face recognition model is proposed by using three types of faced masked data sets. A system is having two applications named Face Mask Detection and Masked Faces Recognition. The Face Mask Detection check that everyone must wear the mask. The Masked Faces Recognition is an application which recognize and verify any person's face who wear the mask. Three types of datasets will used for recognition of masked faces that are following: (i) Real-World Masked Face Recognition Dataset (RMFRD) [26] (ii) Masked Faced Detection Dataset (MFDD) [25] (iii) Simulated Masked Face Recognition Dataset (SMFRD) [27, 28]. RMFRD is now the largest real world masked face dataset. The recognition accuracy of masked faces achieved is 95% [14]. Furthermore, a face mask detection is proposed that helps in identifying whether a student has worn a mask and uses Barcode/RFID tags to mark his/her attendance. To detect a face mask a combination of HAAR Cascade, ADAM classifiers are adopted. With 'no mask', the system achieved accuracy is 95% and 'valid mask' the accuracy is 88%-92% in proper surroundings. For increasing the accuracy improvement in camera quality can be made and by keeping distance of 0.7m for face mask detection [16]. For real time mask detection and face recognition, two techniques are adopted: Eigen faces and Local binary pattern histogram (LBPH). The system will capture the image, detects the face and mask and attendance will be recorded. The LBPH performance is better than Eign faces for recognizing the face. The system achieved accuracy with eigen faces is 73.3% and 100% with LBPH [17]

2.4. Iris and face recognition

In an access control system (facial or iris recognition), thermal camera is integrated for detecting the high temperature of an employee. As a fever is considered as a main symptom of COVID-19, thermal camera will detect that person who is having high temperature and he/she will be not granted for access and the process will be terminated. If the temperature is sensed normal by thermal camera, it will send green signal and control is transferred to the access control system. Then the process will be continued to match the record of a person in database. If matched, the person will grant access otherwise the person is not allowed to enter. However this method is limited in terms of accuracy [4]. The iris detection is introduced for the authentication of an employee by using the fusion of iris and face recognition. This method is highly robust and takes less than a second to identify employee with time and date. Iris time provides an android based platform which can take hundreds of time and attendance applications [9]. Iris ID's technology is also used by the number of hotels existed in Iraq. However, with the help of iris recognition technique- iris access, Iris ID's iCAM 7S biometric scanners is used to automate the attendance system [10]. Table 1 describes the brief overview of the Biometric Techniques.

TABLE 1. Overview of Biometric Techniques adopted in Covid-19 for attendance purpose

S.No.	Authors / Organizations	Methodology	Category	Remarks
1	Oduah et al. [3]	Finger print acquisition process, fingerprint architectural technique.	Contact less fingerprint scanning.	The highest fingerprint correlation factor 78.12% was achieved at 280 lm.
2	Dhawale, S. P. [5]	face recognition algorithm, deep learning techniques, open CV, python and caffe layer network	Face detection with mask.	The recognition is difficult in case of variation face expressions.
3	Kent RO [7]	Facial Recognition and Artificial Intelligence	Face recognition	Robust and achieved accuracy of 99.9%.
4	Keshavdas, M. [8]	Facial recognition technology integrated, thermal sensor	Face detection, fever detection	It can be scaled up to sixty thousand plus faces.
5	Securityinfowatch [9]	Fusion of iris and face recognition	Face and iris recognition	Highly robust model to identify the user with time and date.
6	Bist et al. [11]	ResNet method and multi-layer feed forward network and faiss	Face recognition with mask	Overall achieved accuracy is 68%. Comparatively low accuracy.
7	Rajamanogaran, M. et al., [12]	Machine Learning algorithms and neural networks	Face recognition	Achieved accuracy 95%.
8	Wu, et al., [13]	the Face Recognition Temperature Detection Device (FRTDD) part, cloud database part and the personal cloud Pod part	Face recognition and temperature detection	Wearing mask will affect the accuracy of face recognition.
9	Suhaimin, et al., [17]	Eigen faces and Local binary pattern histogram (LBPH)	Face detection with mask	The accuracy achieved for Eigen faces is 73.3% and for LBPH it is 100%
10	Indatalabs, [6]	pytorch, python, open CV, faiss, and albumentations	Face detection with mask	Accuracy achieved is 91%
11	Archana, et al. [15]	Binary Pattern Histogram (LBPH) and Convolutional Neural Network (CNN)	Face recognition	Accuracy found in CNN is 95% while in LBPH is 78%
12	Jain et al. [16]	HAAR Cascade, ADAM classifiers	Face detection with mask	'No mask', the system accuracy is 95%. 'valid mask' the accuracy is 88% to 92%
13	Gupta et al. [4]	Access control system with thermal camera integrated.	Face or iris detection	There is a need of more work on camera and it can be advanced for better results.
14	Wang, et al. [14]	Three data sets MFDD, RMFRD and SMFRD.	Masked face recognition	The recognition accuracy of masked faces achieved is 95%
15	Shao, & Zhong [18]	Deep metric learning-based feature extractor	Touch less palm print recognition	Accuracy is increased by up to 9.11%

Different techniques are overviewed and discussed which can be adopted for taking attendance in COVID-19 Pandemic. It is a major concern to reduce the spread of corona virus and to have secure attendance system. Mostly face recognition techniques are adopted for marking attendance and most of them are having good results. But face recognition with mask have not shown such good results as compared to other detections and recognitions. Touch-less fingerprint or palm recognition are considered to be moderate. For any organization, face recognition and iris detection techniques are more accurate and suitable in order to mark attendance in safe and protected environment. The accuracy in face and iris recognitions are having better results than other recognition techniques. They can be considered best and suitable approach for marking attendance and for reducing the spread of virus effectively.

3. Challenges in Techniques Adopted in Covid-19

- In contact less finger print scanning, the distance between finger and camera have affected the correlation factor. The background light intensity also assorted the correlation factor.
- By using Eigenfaces recognition, it is good for data representation but not for class discrimination in recognizing face.
- Those Face recognitions using thermal camera for detecting temperature of the person are having conditions. If one person is infected by virus and the system fail to show increase in temperature he will be allowed to enter. In other situation, if the person is not infected by virus and the system shows increase in temperature then he will be not allowed to enter.
- Wearing mask affects the accuracy of face recognition.
- Variable changes in human faces such as facial expressions, scarf and lightning conditions may cause difficulty.
- Touch-less sensors are expensive to be implemented and it might be not possible for some organizations.
- Misuse of face and iris recognition is a concern when it comes to privacy.

4. Related Work

During COVID-19 Pandemic, many challenges and opportunities and impact of this virus have been discussed in different papers. Gomez-Barrero et al. [19], discussed about the main challenges faced in COVID era on hand based and facial biometrics. The researcher also described the new opportunities by overviewing the existing systems based on iris scanners, touch-less biometric recognitions and mobile recognitions. Okereafor et al. [20], discussed the control measures for the infectious disease transmission through fingerprint recognitions which is touch based and considered the approaches to make fingerprint systems hygienic and safe in order to prevent the disease but not focused on touch-less systems. Lewis, N. [21], considered the biometric technology which include facial recognition features using thermal imaging and discussed the ethical challenges. The system focused on touch free identification and temperature screening. Srinivas, G. R. [22], discussed the challenges by using touch based attendance systems and move on to facial recognition and also considered other available technologies for biometric attendance system. Elliot, M. [23], analyzed the challenges and opportunities of incorporating emerging technologies which include Artificial Intelligence, Internet of Things and Big data used in COVID-19 pandemic. Yashaswini et al. [24], focused on the image processing and Iot technologies such as RFID (Radio Frequency Identification), Open CV and SSD (Single Shot Detector). However, these techniques are used in COVID-19 as an alternative to biometric scanners.

5. Conclusion

This work discusses and assesses the impact of COVID-19 on different biometric systems and outlines its weakness and strengths. Then we discuss evaluation of different biometric detection and recognition techniques and methods in very advanced and compared them which can be adopted in this COVID-19 Pandemic. Our focus is on the latest biometric technologies acquired during COVID. Those organizations, where wearing mask is compulsory can adopt the system which is having feature of mask detection. We proposed an Overview of biometric techniques based attendance system during COVID. Also we have seen that better results are produced by deep learning models in real time scenarios. For preventing spread of virus through physical contact, attendance system which are contact less are focused in this paper.

6. References

1. [Online]. Available: https://bioconnect.com/2021/12/08/a-brief-history-of-biometrics/#:~:text=While%20the%20earliest%20accounts%20of,classification%20and%20comparison%20of%20criminals. [Accessed 1-Jan-2022].

2. [Online]. Available: https://www.irisid.com/download/IrisID_TimeAttendance.pdf.[Accessed 1-Jan-2022]

3. Oduah, U. I., Kevin, I. F., Oluwole, D. O., & Izunobi, J. U. (2021). Towards a high-precision contactless fingerprint scanner for biometric authentication. Array, 11, 100083.

4. Gupta, A., Maurya, S., Mehra, N., & Kapil, D. (2021, January). Covid-19: Employee fever detection with thermal camera integrated with attendance management system. In 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 355-361). IEEE.

5. Dhawale, S. P., (2021). Human Face with Mask Detection and Recognition for Smart Attendance System in a Pandemic Scenario. International Journal of Research in Engineering and Science (IJRES), 9(7), 68 -70.

6. [Online]. Available: https://indatalabs.com/resources/face-recognition-time-attendance. [Accessed 12-Jan-2022]

7. [Online]. Available: https://www.business-standard.com/content/press-releases-ani/k

ent-ro-launches-zero-human-touch-attendance-system-120082700960_1.html [Accessed q5-Jan-2022]

8. [Online]. Available: Keshavdas, M., (2022), https://fleetroot.com/blog/contactless-attendance-using-facial-recognition-for-students-wearing-masks/

9. [Online].Available: https://www.securityinfowatch.com/access-identity/biometrics/biometric-time-attendance/product/21159646/iris-id-systems-inc-iristime-biometric-time-and-attendance-solution-from-iris-id . [Accessed 1-Jan-2022]

10. [Online].Available: https://www.infomet.com.tr/uploads/mediaresources/newsarchieve/20200819FindBiometrics.pdf[Accessed 1-Jan-2022]

11. Bist, A. S., Febriani, W., Lukita, C., Kosasi, S., & Rahardja, U. (2020). Design of face recognition attendX for recording student attendance data based on artificial intelligence technology. Solid State Technology, 63(2s).

12. Rajamanogaran, M., Subha, S., Priya, S. B., & Sivasamy, J. (2021). Contactless Attendance Management System using Artificial Intelligence. In Journal of Physics: Conference Series (Vol. 1714, No. 1, p. 012006). IOP Publishing.

13. Wu, H., Pan, Y., Weng, X., & Chen, H. (2021). Design of Campus Health Information System Using Face Recognition and Body Temperature Detection. In 2021 IEEE Intl Conf on Cyber Science and Technology Congress (CyberSciTech).

14. Wang, Z., Wang, G., Huang, B., Xiong, Z., Hong, Q., Wu, H., ... & Liang, J. (2020). Masked face recognition dataset and application. arXiv preprint arXiv:2003.09093.

15. Archana, M. C. P., Nitish, C. K., & Harikumar, S. (2022). Real time Face Detection and Optimal Face Mapping for Online Classes. In Journal of Physics: Conference Series (Vol. 2161, No. 1, p. 012063). IOP Publishing.

16. 16] Jain, D., Upadhyay, A., Nirban, A., Arya, M., & Mishra, R. (2021). Face Mask Detection & Attendance System. International Journal of Scientific and Research Publications (IJSRP), 11(3).

17. Suhaimin, M. S. M., Hijazi, M. H. A., Kheau, C. S., & On, C. K. (2021). Real-time mask detection and face recognition using eigenfaces and local binary pattern histogram for attendance system. Bulletin of Electrical Engineering and Informatics, 10(2), 1105-1113.

18. Shao, H., & Zhong, D. (2022). Towards open-set touchless palmprint recognition via weight-based meta metric learning. Pattern Recognition, 121, 108247.

19. Gomez-Barrero, M., Drozdowski, P., Rathgeb, C., Patino, J., Todisco, M., Nautsch, A. & Busch, C. (2021). Biometrics in the era of COVID-19: challenges and opportunities. arXiv preprint arXiv:2102.09258.

20. Okereafor K, Ekong I, Okon Markson I, Enwere K Fingerprint Biometric System

Hygiene and the Risk of COVID-19 Transmission JMIR Biomed Eng 2020;5(1):e19623 URL: https://biomedeng.jmir.org/2020/1/e19623.DOI: 10.2196/19623

21. [Online].Available: https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/biometric-technology-use-during-pandemic-can-pose-ethical-problems.aspx. [Accessed 15-Jan-2022]

22. [Online].Available: https://government.economictimes.indiatimes.com/news/technology/contact-based-biometric-attendance-system-is-dead-what-if-facial-recognition-triggers-personal-data-privacy/75368517. [Accessed 15-Jan-2022]

23. Mbunge, E. (2020). Integrating emerging technologies into COVID-19 contact tracing: Opportunities, challenges and pitfalls. Diabetes & Metabolic Syndrome: Clinical Research & Reviews, 14(6), 1631-1636.

24. Yashaswini, K. S., Harmya, T. V., Sukrutha, B., Surabhi, N., & Kumar, A. S. (2021). Prevention of COVID Spread: A Review. International Journal of Research in Engineering, Science and Management, 4(8), 92-94.

25. [Online].Available: https://zhuanlan.zhihu.com/p/107719641?utm_source=com. yinxiang. [Accessed 18-Jan-2022]

26. [Online].Available: https://tzutalin.github.io/labelImg/. [Accessed 19-Jan-2022]

27. D. Yi, Z. Lei, S. Liao, and S. Z. Li, “Learning face representation from scratch”, arXiv:1411.7923, 2014.

28. Jain, V., & Learned-Miller, E. F. A Benchmark for Face Detection in Unconstrained Settings. University of Massachusetts; Amherst, MA. USA: 2010. Technical Report, UMass Amherst Technical Report.

29. Krishnan, M. G., & Balaji, S. B. (2015). Implementation of automated attendance system using face recognition. International Journal of Scientific & Engineering Research, 6(3), 30-33..

30. Kawaguchi, Y., Shoji, T., Lin, W., Kakusho, K., & Minoh, M. (2005, October). Face recognition-based lecture attendance system. In The 3rd AEARU workshop on network education (pp. 70-75)..

31. Doctorow, C. (2012). Share or die: Voices of the Get Lost Generation in the Age of Crisis. New Society Publishers.

32. Wang, X., Han, X., Huang, W., Dong, D., & Scott, M. R. (2019). Multi-similarity loss with general pair weighting for deep metric learning. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 5022-5030).

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