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

International Journal for Electronic Crime Investigation

(IJECI)

VOL: 7
ISSUE: 1 Year 2023

Email ID: ijeci@lgu.edu.pk

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

International Journal for Electronic Crime Investigation
Volume 7(1) Year (2023)

SCOPE OF THE JOURNAL

The International Journal for Crime Investigation IJECI is an innovative forum for researchers, scientists and engineers in all the domains of computer science, white Collar Crimes, Digital Forensics, Nano Forensics, Toxicology and related technology, Criminology, Criminal Justice and Criminal Behaviour Analysis. Moreover, the scope of the journal includes algorithm, high performance, Criminal Data Communication and Networks, pattern recognition, image processing, artificial intelligence, VHDL along with emerging domains like quantum computing, IoT, Hacking. The journal aims to provide an academic medium for emerging research trends in the general domain of crime investigation.

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.

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

International Journal for Electronic Crime Investigation
Volume 7(1) Year (2023)

CONTENTS

International Journal for Electronic Crime Investigation
Volume 7(1) Year (2023)

Aftab *et al. (IJECI)* 2023

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

International Journal for
Electronic Crime Investigation

DOI: https://doi.org/10.54692/ijeci.2023.0701124

Research Article

Vol. 7 issue 1 Year 2023

Detection and Control over the offences of White Collar Crimes, Frauds and Hacking of information, by using effectively the relevant Software and Electronic Devices

Aftab Ahamd Malik[1], Mujtaba Asad[2] and Waqar Azeem[3]
University of Kent, England [1]
Department of Criminology and forensic Sciences, Lahore Garrison University, Lahore [1]
Shanghai Jiao Tong University, China [2]
South Eastern Regional College, Downpatrick, Ireland UK [3]
Corresponding author: dr_aftab_malik@yahoo.com
Received: November 21, 2022; **Accepted**: December 30, 2022; **Published**: March 03, 2023

Abstract

In both developed and emerging nations, fraud, white collar crime and malpractices in small and medium-sized businesses, banking, and other sectors are on the rise. The criminals are carrying out their fraud-related offence by using the most up-to-date information technology structures and similar electronic media to create unjust loss and harm in the fields of white collar crimes, banking, business, and to persons. The goal of this research paper is to make these businesses understand the need of utilizing the most up-to-date, trustworthy, and legitimate software and the necessity of making their networks more secure from external threats. The thieves are able to accomplish their goals thanks to the usage of sophisticated features for tracking and hacking private information utilizing software and information technology resources. In essence, their tactics rely on deceit and dishonesty to harm others. In essence, their methods of operation rely on deceit and dishonesty to commit the crime. Employees of the affected organisations are frequently complicit in banking and white collar scams, aiding and abetting outside criminals by transferring sensitive information. Parody, distortion, misrepresentation, twisting of the fact or truth, and concealing of actual information that is harmful to another person are all examples of fraud. The legislation's attempt to punish fraudsters seems extremely naive. There are many reasons why criminals flee, including the fact that their identities are frequently kept a secret. The criminals are able to move toward exoneration and freedom due to a lack of evidence, shoddy investigation, and naive prosecuting tactics. The fraudsters possess high quality Software Engineering Tools and Electronic Equipment to commit offences of such to harm entrepreneurs, financial organizations, commercial banks by depriving and extravtinf information and money from the concerned accounts, Technically and operationally feasible and valuable suggestions for implementation are presented in this paper to safeguard the Networks of organisations.

Keywords: Cyber Crime, Frauds, White Collar Crimes, hacking of information, Financial Crimes

1. Introduction

Mostly the malpractices occur in marketing and buying securities, hacking valuable personal information of consumers and customers and then extracting money from their bank accounts. Just only the legislation cannot help the victims. Fraudulent activity includes elements like outwardly apparent, superficial financial necessity and justification for validation and justification. Legally, the court defines fraud as a situation in which a false representation is made in order to carry out fraudulent action. Fraudulently obtaining money or "services" with the purpose to defraud is a crime. Essential components of frauds include deception, illicit gain, opportunity, purpose, and opportunity. Law enforcement organizations had not been operating at a satisfactory level. The area of frauds, particularly in accounting, society, organizations, and public, private, autonomous, and semi-autonomous bodies, has a vast amount of room for research.

Over the past eight decades, white-collar crime research has changed. The nature of “white collar crime” has also changed. Due to high-Tech and improvements are one change in the offices that has probably had an impact on white-collar crime. Particularly with the invention of the computer, both inside and outside of the office, there have been more opportunities for crime to occur. However, very few studies have looked at cybercrime from the perspective of such offences. White-Collar Crime and Cybercrime: Differences. Even if there are two distinct cancer types, this does not imply that they are the same. For instance, skin cancer and colon cancer are both types of cancers, but they have different causes, effects, and treatments.

International issues are more prevalent in cybercrime. Younger criminals are more likely to commit cybercrimes. A national threat has been created around cybersecurity. The two sorts of crime show different signs of trust. White-collar crime and cybercrime criminals' educational backgrounds might vary. It is observed that normally goals of banks similar, though they may excel more in certain specialized areas and achieve their goal and objectives. The Investment banks concentrate on attracting investors who want to invest money in the stock market and expand their financial holdings by buying and selling shares. The management of the money supply for an entire nation or set of nations is assisted by central banks. The central bank of a nation influences monetary movement, interest rates, and financial policy. Due the reputation and the measures taken by the banks, they become popular and trust worthy. In United States, the following banks are famous and considered to be safe, for their reputation:

Table 1 : Safe Banks

AgriBank	Citibank	Capital One	JPMorgan Chase
M&T Bank Corporation	PNC Bank	U.S. Bank	Wells Fargo

2. Cybercrime And White Collar Crime

According to [1] and [2[, there is difference among Cybercrime & White-Collar Crime and the papers give useful discussion on the differences also; while [3] has emphasized area of Cyber Security for Banks at great length regarding banks, industrial banks and industry itself. The paper [4] highlights very important tools used by the hackers and Fraudsters. There are indeed a dozen useful to tools used against the banks given in tables 2. Because, the gangsters are after the following information to damage the victim such as Account number, Birthdate, Location, Mother's name and other information about the account and account holder. Most of he financial crimes become easy to handle using personal confidential information. Regarding computer aided facilities available to criminal [4] presents discussion at depth and [5] speaks openly about the Cybersecurity. If difficult circumstances are encountered, the highlights have made the web a success; nevertheless, its support for modernization and free-form may be at jeopardy due to its scatter and client-controlled nature. If the lacklustre support for web features is seen as a success in and of itself, that opinion is highly subjective and influenced by the users. Even while this approach, which gives the client authority, supports the innovation paradigm, it might nevertheless pose risks to the wider public. Corruption, illegal activity, civil crime, and terrorist activity are examples of traditional ways that appear in our environment and result in bodily harm.

Information is a powerful tool. Today, government has made cyber security on top priority and a fundamental requirement. Demand for cyber security for saving foundation has significantly increased, to the point that the government has made it a priority to manage cyber risks by enhancing cyber security. Cybersecurity is essential for enhancing national security, increasing consumer confidence, and ensuring the reliability of systems that support our economy. Cybersecurity accomplishments must be carefully adjusted in order to protect privacy, freedom, alteration, and the motivating nature of the Internet. To create an effective and equitable cyber security plan, each component of the nation's essential framework must be taken into account separately.

Table 2: Toolkits of gangsters and fraudster Ref: [8]

Computer pop-ups	Fake claims	Fake entities	Fake names, credentials, numbers
Fake photos	Fake profiles	Lead lists	Persuasion
Robocalls	Phishing	Secrecy	Spoofing

3. Banking Software

Banks are confronting with different applications in their normal routine work and hence require differe nt types of software, especially related to online running the system. Today, the mainstream of people and organizations have some kind of financial account in banks. The

banking system software is indeed very complicated and sometimes is naïve and needs updated versions. The formal utilities, debugging software and usual operating systems require repairing and revamping in order to standardize the functionality and its ability cope up with new requirements. On the other hand, the banks and customer's company, both use Computerized Management Control and Information Systems which requires compatible software for storage, processing and retrieval purposes.

The famous firms, who develop sophisticated banking encryption software are given in Table 3 and Table 4 provides a few best banking software. In Table 5. we list some important Encryption Algorithms, where, AES is "Advanced Encryption Standard", also considered to be the best for US-banking and other entrepreneurs. There are several best banking software available in market for various applications for Computer Systems, Management, Corporate Banking, handling Bank Administration, and daily banking application systems. JIRA is one of the best Banking Software System to perform various important banking tasks such as Project Management, works as a tool for management, portfolio, product-management, for local configuration systems ,Portfolio and asset-management tool and also as testing-tool. Originally, it was developed by an Australian famous company. Table 6 provides the best "Software names" for online and other Banking applications.

3.1. Online Banking Software

The users may be benefited by several reliable software in the area of on-line banking. One of the trusted software, which is cloud based, can be used for "accounting Management"; it is helpful to program and automate the payable processes. Tipalti is one of the cloud based software. Some other effective and useful software are given in Tables 8. There is another cloud based software known as Fraud.net; which is used for risk management platform. It provides tools for fraud prevention.

Table 3 Encryption software developing companies for banks

IBM Corporation	Avaloq	Trend Micro Sophos	Thales Group

Table 4 Best Software for banking applications

Avaloq banking suite	CGI open finance	Core banking	Flexcube
Oracle	SAP for banking	Symphony™	TCS bancs
Temenos transact	TurnKey Lender	Validis	Mambu

Table 5: Best Banking Encryption Algorithms

AES	Blowfish	Tripple DES	Twofish	Rivest-Shamir Adleman (RSA)

Table 6: Best Software names for online and other Banking applications

Bank Account opening	Bank Account Tracking	Bank Account Management	Bank Budgeting
Bank Compliance	Banking Contract Management	Cash Management for Banks	Electronic Banking
Gnucash Online Banking	Home Banking	Kmymoney Online	Mobile Banking
Online Account Opening	Quickbooks Online Banking	Quicken Banking	Quicken Online Banking

Table 7: Suitable Software for Core Banking System

CBC Core Banking System	Cloud based core	Equation core	Finacle	Flexcube	HSBC

Table 8: Software for Online Banking

Centrex	Cyberbank	FinCell	Fraud.net
Origins	Plaid	The Nortridge Loan System	Tipalti

4. Protective Measures To Safeguard Banking Information From Fraudsters

With fast developments in Information Technology and recent research in Software Engineering, the entrepreneurs and financial organizations may choose a most suitable and feasible solution to safeguard their precious data and applications as well as the "System Software" from outside attacks. It is important to adopt preventive security measures before the damage occurs. Most obvious source of problems and criminal activities is the "Internet". Now most of the companies have their own dedicated intranets and extranets. By an intranet, the outsider is allowed to moderately access the company's network in secured manner. Mainly the intranets are used by the employees of the organization; whereas the extranets allow the outside business associates or customers having stakes in the organization. According to [5], there several protective measures to protect the banks from hackers and criminal gangsters. The Cybercrime are committed online by breaching the personal information of customers, what is termed as "Identity Theft'. It is well known that the terrorists are frequent user of internet; particularly the "mobile-terrorists". The terrorist's feat and take advantage of the weaknesses and bugs in the software. The use of digital devices by criminals have been described at length in [6]. The authors of [6] recommend for the implementation of stronger electronic devices to combat with Cybercrimes and white Collar Crimes. The paper [7] strongly recommends the use of a "Demilitarized Zone" in Network

to provides a protective measure to the network by using a "hardware fire wall", a "software firewall" with routers so that the signals from outside hackers are identified and killed on the spot. In Table 9, there is a list of a few Internet Security Software, which have been found useful:

Table 9: Internet Security Software

Avast Premium Security 2020
Kaspersky Total Security 2020
McAfee Total Protection
Symantec Norton Security Deluxe
Webroot Internet Security Complete with Antivirus Protection
Webroot Internet Security Plus with Antivirus Protection

5. Recommendations

Banks now confront new security issues as a result of the rapid expansion of their attack surfaces due to digital transformation. The average rate of attack on banking is increasing day by day. The financial companies and the banks are attacked about a thousand times fortnightly. Therefore, strict measures according to the recommendation of [6] and [7] must essentially be adopted. More recommendations are put forward below.

i. Installation of a "Demilitarized Zone" in Network provides effective security.

ii. The users must seek help from academia and software industry to get resolved their problems.

iii. Installation of a "virtual private network VPN" has been found useful to guard and provide a shield to the online "sending" and "receiving" the Data during the usage of "public Wi-Fi". The SD WAN is very useful for banks connected with their braches. It is software which protects and secures the work of the branches connection with internet and clouds.

iv. The use of Cloud Guard provides full, wide-ranging and comprehensive security to the users of e-banking.

v. Enhance the internet security measures for your installation.

vi. If the attack has occurred, soon after without wasting time, inform to your bank or organization. Let them know the details about the fraud and your "identity-theft".

vii. A complicated pass-word must be used consisting of alpha-characters, numerics and special characters. Its length must be 10 characters.

viii. Continue to change your password over time

ix. Never conduct online banking on a public computer

x. When conducting online banking, only use trusted apps or websites

xi. Ensure that you only use safe internet connections

xii. Avoid being a victim of phishing

xiii. Protect your PC.

xiv. The settings of social media must be kept updated to avoid any harm.

xv. The updated versions of application software, operating systems and Security software must always be used.

xvi. All the identity information must be kept under lock. Protect yourself.

xvii. It is advised by FBI, that people must not use fake and false banking apps, which are prepared to harm the users while the trackers commit cybercrimes

6. Acknowledgements

The authors are grateful to Mr Kaukab Jamal Zuberi, Head of Department of Criminology and Forensic Sciences for his guidance and useful discussion; also to the Chief Editor for encouragements.

7. References

[1]. R. Eric and R. Thompson, "Computer Facilitated White-Collar Crime : Computers & Criminal Justice". https://cod.pressbooks.pub/crimj1165/chapter/-module-7-computer-facilitated-white-collar-crime/

[2]. Cyber Security for Banks, https://www.checkpoint.com/industry/banks/

[3]. L. Vitalise, "Top 10 Best Internet Security Software", https://www.consumersearch.com/technology

[4]. K. Brian and Payne, "White-Collar Cybercrime: White-Collar Crime, Cybercrime, or Both? " ., vol. 19, no. 3, pp. 16–32. Criminology, Criminal Justice, Law & Society E-ISSN 2332-886X https://scholasticahq.com/criminology-criminal-justice-law-society

[5]. A. G. Johansen, "11 ways to help protect yourself against cybercrime", NortonLifeLock. 2020.

[6]. A. A. Malik, "Bank Frauds Using Digital Devices and the Role of Business Ethics", IJECI., vol. 2, no. 4, pp. 21-32. 2018.

[7]. A. A. Malik, M. Asad and W. Azeem,"-Frauds In Banking and Entrepreneurs by Electronic Devices and Combating using Software and Employment of

Demilitarized Zone in the Networks", IJECI. vol. 1, no. 1. 2023.

[8]. Katherine Skiba(2022), " 12 Tools in a Fraudster's Toolbox", EN ESPANOL

Hussain *et al. (IJECI)* 2023

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

International Journal for
Electronic Crime Investigation

DOI: https://doi.org/10.54692/ijeci.2023.0701125

Research Article

Vol. 7 issue 1 Year 2023

Security Issues and challenges in Cloud Computing

Hussain Akbar, Muhammad Zubair and Muhammad Shairoze Malik

Department of Information Technology, Superior University Lahore Pakistan

Corresponding author: msisw-f21-003@superior.edu.pk

Received: November 20, 2022; **Accepted:** January 20, 2023; **Published:** March 03, 2023

Abstract:

A cloud computing model allows customers to use a pool of shared computer resources on-demand or pay-per-use basis. In terms of capital investment and operational cost reductions, cloud-based computing offers users and organizations many benefits. Despite these advantages, several challenges still limit the adoption of cloud computing. A crucial concern that is usually taken into account is security. Without this vital component, the computing model has a negative influence, which causes suffering on the human, ethical, and economic levels. This essay will look at the security issues that cloud entities must deal with. This group includes Cloud Service Provider, the Data Owner, and the Cloud User—concentrating on the communication, computation, and service level agreements that make up the crypto-cloud. It will offer the required updates by evaluating the origins and consequences of different cyberattacks.

Key words: Cloud computing, security, high performance, challenges, quality.

1. Introduction

Users are given a network-based environment perception through cloud computing, which makes it possible to share calculations and resources anywhere in the world. Cloud computing is described by the National Institute of Standards and Technology (NIST) as "a template for delivering the appropriate and when required internet access to a shared pool of quickly manipulable programmable grids, servers, amenities, storage, and software." [1]. On-demand self-service, High-performance network access, Accelerated Elasticity, High Scalability, and Defined Performance are the processing type traits shown in Fig. 1. Four deployment types are also offered, including Community, Private, Hybrid, and Public Clouds. Hybrid, community, private, and public clouds. The three service

models—PAAS (Platform as a Service), IAAS (Infrastructure as a Service), and SAAS (Software as a Service)—are then connected with this model. The NIST definition of cloud computing provides the necessary framework, illustrating commonalities, including Geographic Distribution, Homogeneity, Virtualization, and Service Orientation.

Security concerns must be considered when using the cloud service models with all the levels. When the stories are contrasted, the browser's significant dependence puts it at the top. In contrast, the lower levels are more focused on web services. Overall operational costs and investments are reduced, and improved productivity and scalability throughout the levels.

Depending on the customer's needs, hybrid, community, private, and public cloud service models may be used.

Organization: The security issues are highlighted in the following two sections. The problems with security in Service Level Agreement (SLA), computational, data, and communication levels are addressed in Sections 4–7. Lastly, Section 8 concludes with the author's research with other previous studies for comparison.

2. Challenges With Security

Because cloud service providers (CSPs) have data centers in different geographical locations, which presents several security issues and dangers, consumers in cloud computing are oblivious to the precise location of their sensitive data. Due to the quick propagation of threats in virtualized environments, conventional security measures like host-based antivirus, firewalls, and intrusion detection technologies do not provide sufficient security in server virtualization.

2.1. Cloud computing dangers and threats

Walker [2], on the other hand, highlighted that the Cloud Security Alliance (CSA) had published a list of the top 12 cloud-related risks. Table 1 contains a list of these twelve dangers. Data breaching is the most pressing security concern that requires attention among these threats.

2.2. Security in crypto-cloud

As Kamara [3] explained, there are several upsides to utilizing a public cloud. They also noted several security hazards associated with using public cloud services. Many serious worries center on the possibility of damage to the data's privacy and authenticity. Kamara [3] 2010 presented a crypto-cloud architecture, which is depicted clearly in Fig. 3. There are three primary actors involved: the data's owner (the Data Authority), the data's end user (the consumer), and the storage service provider (the Cloud Storage Service Provider) (CSSP). Customers or users of cloud services are granted authorized access to encrypted files uploaded by the data authority. After those steps, the requested file may be downloaded and decrypted using the proper tokens and credentials. These three groups have unique data protection problems in their communications, computations, and SLAs.

Table 1. CSA'S Top 12 threats

Threat no.	Threat name
1	Violated privacy.
2	Passwords and authentication issues.
3	Broken APIs and hacked user interfaces.
4	Taking advantage of loopholes in the system.
5	Taking someone else's account without permission.
6	Contaminated by malicious insiders.
7	The APT virus, or Advanced Persistent Threat.
8	Inaccessible files are forever gone.
9	Having not done enough research.
10	Misuse of cloud services.
11	Attacks using the denial-of-service (DoS) protocol.
12	Shared technology, shared dangers.

3. Security Issues That Cloud Companies Must Deal

Authentication, integrity, transparency, confidentiality, availability, and audits are a few fundamental security criteria that must be addressed in addition to legal security standards, according to Rebollo [4]. The security tree in Fig. 4 is an example of the value of fundamental security criteria. Just like the root anchors the tree in the ground, the issues identified at the root must be correctly treated. The security tree, figuratively represented as the fruits and leaves on a tree, provides advantages in terms of anything/everything as a Service (XaaS) when these fundamental conditions are duly satisfied. Data is transmitted securely using the protocols (TLS) and (SSL), which stand for Transport Layer Security and Secure Socket Layer, respectively.

4. The Quality Of Communication

Due to attacks on Virtual Machines (VMs), there will surely be communication challenges due to the VMs' shared resources, infrastructure, etc. Bhadauria [5] separates this into three categories: network, host, and application. These three tiers of interaction serve as a basis for detecting attacks.

4.1. Security on the level of the network

Data privacy and security are two of the most important aspects of any network infrastructure. When it comes to safety on a network level, the problems include the following:

- Attacks Made Against Domain Name Servers
- Hijacking of prefixes in the Border Gateway Protocol (BGP).
- Concerns Regarding the Reuse of IP Addresses
- Sniffer Attacks etc.

4.2. The security of the application level

Applications require security to prevent allowing attackers the opportunity to obtain control over them by changing settings that they haven't been permitted to modify.

Their configurations.

- ✓ Cookie Poisoning is one of the problems that must be addressed at this level.
- ✓ DDoS.
- ✓ The manipulation of the hidden field
- ✓ An attack with a dictionary
- ✓ Breaking CAPTCHAs
- ✓ Hacking Google

4.3 Security measures used at the host level

At the level of the operating system, which is the foundation upon which applications run, host risks are handled. Worms, viruses, and Trojan horses are the primary dangers found at the host level.

- Profiling.
- Methods for breaking passwords.
- Footprinting.
- A refusal to provide a service.
- Unauthorized entry or use

5. Computational Level

One of the most challenging problems to solve on a computational level is figuring out how to implement virtualization in the cloud.

5.1. Challenges posed by virtualization

Virtualization may be thought of as the abstraction of physical resources. The terms "desktop virtualization," "application virtualization," "network virtualization," " and "server virtualization "machine virtualization" are examples of some of the most prevalent categories of virtualization.

Multiple instances of Virtual Machines make up the virtual layer, which is made up of these machines. It paints a picture of a virtual and distributed environment that operates on top of the cloud architecture and is managed by a cloud provider. The virtualization layer allows it to simultaneously deploy and operate several virtual machines (VMs) on the same physical host. It is carried out by a particular component or piece of software known as the hypervisor or the Virtual Machine Monitor (VMM), which divides up resources among the several VM instances and ensures that they remain isolated. VMs can communicate with one another over the virtual switch, thanks to the virtual network. Ram, the Central Processing Unit (CPU), and storage are examples of hardware resources included in the physical layer.

5.1.1. Security problems at the virtual machine level (also known as the virtual layer)

The virtual machines go through their unique life cycles, which include a variety of states such as being created, pending, operating, suspended, restarted, powered off, shut down, destroyed, and others.

5.1.1.1. Cloning a virtual machine (VM)

Cloning a virtual machine (VM) means creating a clone of an existing VM with the exact identification (ID), computer name, Internet Protocol (IP), and Media Access Control (MAC) addresses. This process is referred to as VM cloning. The cloned virtual machine (VM) shares its virtual resources with the original virtual machine (VM), referred to as the parent. The cloned virtual machine is unaffected by any modifications made to the original VM after completing the cloning process, and vice versa. Because both virtual machines (VMs) will use the same network, there will be a duplication of IP addresses, which may cause security problems.

5.1.1.2. Isolation of VMs

To guarantee safety and security, the VMs need to be isolated. Virtual machines (VMs) can be kept secure by isolating them from one another, even if another VM running on the same physical host is breached. However, virtual machine isolation is not a foolproof solution when the hypervisor has been breached. The virtual machines' shared usage of IP addresses, which breaks the isolation between them, causes problems that must be fixed as soon as possible. This may bring the whole system's performance down.

5.1.1.3. Migration of Virtual Machines

Virtual Machines may be moved simply from one server to another, which helps improve the efficiency with which resources are used. Automating this procedure to achieve load balancing and energy savings is possible. Because of the dynamic nature of the migration, there is a potential for security issues, not only with the virtual machine being moved but also with the new VM host. Live VM migration and non-live VM migration are the two forms of migration. Compared to non-live migration, the live migration process results in a more difficult task.

5.1.1.4. Virtual Machine Exit

Virtual machines (VMs) often operate in secluded and self-contained settings within the host. Any effort by the virtual machine (VM) to directly interact with the hypervisor by intervening in an isolated environment would result in the VM escaping the environment. Therefore, this problem must be handled carefully to avoid compromising the overall virtual setup.

5.1.1.5. VM rollback

Allows virtual machines to be reset to their previous state at any time. Restoring the afflicted virtual machines to their last state may involve the removal of hazardous viruses and worms. As a result, virtual machines (VMs) might be re-exposed to security flaws when rollbacks are performed. Memory snapshot was protected by Sabahi [7] using per-page encryption in conjunction with hashing. The memory contents were hashed using a Merkle hash tree, with the pages' granularity determining the hash's precision. Maintaining logs for the processes, exceptionally suspend/resume and migration, is the recommended best practice. An in-depth investigation indicates that VM rollback, if not managed safely, might activate even hazardous viruses and worms. This was discovered as a result of an investigation into the matter.

5.1.1.6. VM sprawl

Uncontrolled deployment of virtual machines is known as "VM sprawl," and it's a problem that can be avoided. According to Bose [8], VM sprawling is a scenario in which there is a linear growth in the number of VMs, but most themes are inactive. There is a risk that a significant amount of the host's resources will be wasted. Virtual machine sprawl must be controlled to manage resources with the fewest possible efforts efficiently.

5.1.1.7. Virtual Machine (VM) Hopping and Virtual Machine (VM) Hyper Jumps

Virtual Machine (VM) hopping refers to the process of getting access to another VM by exploiting a flaw in the hypervisor. Because of this vulnerability, remote assaults and malware can infiltrate and eventually take control of the middleware packages running on the underlying host by jumping from virtual machine to virtual machine (VM to VM). The most susceptible virtual machines (VMs) are frequently singled out as the entry point for further assaults on the system.

This problem will need to be addressed at some point in the future. The vulnerability in the hypervisor creates a single point of failure in the system.

5.1.1.8. Virtual machine (VM) poaching

The vulnerabilities in the operating system and applications cause the system to behave unanticipatedly. They use up the system resources, which might fail other virtual machines hosted on the same host. It is recommended that patches be applied to both the guest operating system and the regular application to mitigate VM poaching successfully. The issues posed by virtual machines (VMs) are addressed in the publications listed in Table 2.

The overall study shown in Table 2 displays the many options available to ensure the safety of VMs. A comparison of the many methods that have been suggested eliminates the possibility of an increase in either the amount of time required for the execution or the number of test systems. To keep the integrity of the system intact, it is recommended that virtual machines (VMs) not be subjected to the transmission of packets at a fast pace as well as avoiding the application of false assumptions, which would make the problem more complex, and avoiding the oversight of certain specific assumptions and parameters. The Advanced Cloud Protection System (ACPS) raises the level of security and keeps the integrity intact while degrading performance only a little. Wei [9] came up with the idea for a system that assumes several virtual machines (VMs) belong to the same organization, even if they are hosted on a shared network. The authors have argued that there is a requirement for the provision of a protected system, regardless of the virtual machines (VMs) deployed by various enterprises on the same shared network.

5.1.2. Hypervisor level (Virtualization layer)

Qin [10] mentioned that a hypervisor keeps track of virtual machines as they are created, stopped, restarted, and moved around. The Hypervisor or Virtual Machine Monitor (VMM) is nothing more than a low-level code

that is capable of independent operation regardless of the operating system. The hypervisor facilitates virtualization by pooling available resources and supporting many tenants. The hypervisor-based virtualization technique known as para-virtualization is the one that is used most frequently. Complete virtualization and virtualization aided by hardware According to Sabahi [7], hypervisor-based virtualization is prone to having a single point of failure. The current methods for improving hypervisor security are listed in Table 3. All these methods, in their manner, ensure a safe hypervisor. Based on the comparison results, it is suggested that multi-factor authentication be used to strengthen the hypervisor's security further. Protection against software-related vulnerabilities in virtualization cloud computing infrastructures (VCCI) is achieved by combining physical and virtual measures.

Table 2: Security issues in V.M. compared to similar systems.

S. No	Author	Title of the security scheme	Work proposed	Strengths	Weakness
1	Schwarzkopf, 2012	The protection of cloud-based virtual machines.	Checker for updates: Find software that has become obsolete (inactive)—free online hacking toolkit: Runs tests on virtual machines (VMs) before releasing them.	Prevents execution of flawed VMs. Handles multiple software repositories from different vendors.	The time required to complete a task will linearity Quantity of test systems has grown. Identifying software defects that cause network disruptions.
2	Bindra, 2012	The Analysis and Risk Management of Virtual Machine Images on the Cloud.	Suggest doing a security review of the virtual machine images.	Assures the safety of the virtual machine image	……
3	Shea, 2013	Experiments and Analysis of Virtual Machine Performance During Distributed Denial of Service Attacks	Strengthening the stability and safety of current virtualization technologies. (Denial of Service) Attacks.	SYN- proxies are now in place. DOS attacks are no match for container-based virtualization.	When sending tiny packets rapidly, issues occur.

4	Qin, 2012	State-of-the-art Safeguarding Virtual Machines in the Cloud.	Separated the problems into several virtualization security categories.	Methods are classified as either "within" or "outside" the V.Ms.	Some of the identified performance factors are ignored. Some plans are overly complicated and based on false assumptions.
5	Lombardi, 2010	Safe and sound virtualization on the cloud.	Highly Efficient Anti-Cloud Systems (ACPS).	Better protection for cloud data. Constant vigilance ensures that no one's honesty is compromised.	Minimal hit to performance.
6	Duncan, 2013	Insider Threats to Migrating Virtual Machines in the Cloud.	Using digital forensics and system administration methods, identify malicious insider activity.	Ethernet tap detection of packet sniffing.	There isn't a simple way to tell if a network is being passively tapped or not.
7	Wu, 2010	Safeguarding Virtual Machine Networks in the Cloud.	Recommended an innovative framework for virtual networks to manage VM-to-VM interaction.	Improve safety by adding a firewall and a routing layer to your secure, shared network. Defeats attempts that attempt to sniff or fake your signal.	Virtual machines (VMs) should only be used within a company's shared network.

5.1.2.1. Threats in virtual networking

The potential dangers of virtual networks are that they are challenging to construct securely and that all the cloud components need to be connected. Brohi [11] has argued that hypervisor-resident VFs (Virtual Firewalls) on the VMM is a need for protecting virtual machines. Threats like as traffic eavesdropping (intercepting network communication), address spoofing (faking an IP address), VLAN hopping (breaking network segregation), etc., have been cataloged by Laniepce [6] and will need to be quickly addressed in the future.

5.1.2.2.VM-to-VM attack

Vvirtual machine (VM) can be attacked by another VM on the same physical host, using

hypervisor vulnerabilities and perhaps a side channel attack to compromise the coveted VM, as described by Laniepce [6]. Zhang [12] has suggested a methodology for systematically identifying and investigating several common but elusive inter-VM assaults. Therefore, action is required to resolve the problem.

5.1.2.3. Security issue with VM introspection

Virtual machine (VM) introspection is a security concern since it allows for monitoring VMs on a physical server. Expanded [13] coverage of VMI tools for the hypervisor. Intruding in private virtual machines is a sure way to get unauthorized access to their contents and running processes. That's why cutting-edge safeguards against intrusion are required.

5.1.2.4. Issues due to virtualized trusted computing (VTC)

Problems with virtual trusted computing (VTC) are an emerging concern since this technology represents the next logical step in virtualization but has the potential to compromise security if it fails. As described by Laniepce [6], Trusted Platform Module (TPM), a dedicated TPM is required for each virtual machine (VM) and hypervisor. However, the hypervisor often controls a single hardware TPM, which might introduce vulnerabilities. Dongxi L [14] mentioned vTPM and certificate and critical administration. Trusted Platform Module (TPM) implementation in software exacerbates existing problems in the TCB and introduces new vulnerabilities.

5.1.2.5. Hyperjacking / hypervisor subversion

When an attacker uses a compromised virtual machine (VM) to access the hypervisor and then uses that access to try to take over the virtualization layer. Miller [15] has described the assaults on dropbox, Linkedin, etc., resulting from hyperjacking. According to Microsoft's latest page on Hyperjacking, "viruses planted in the hardware/BIOS can't be identified by the O.S." These problems cause bottlenecks that must be addressed.

5.1.2.6. Issue due to resource sharing

Sharing shared resources is a source of contention since a malevolent VM might cause the intended VMs to go without essential resources. Seventy-five percent of security issues, according to Wueest [16], are the result of sharing resources. The cloud computing paradigm relies heavily on the pooling of available resources. Therefore, it's crucial to work out the kinks in the system that prevent people from pooling their resources.

5.1.2.7. Challenges to the Security and Isolation of Virtual Machines (VMs) Caused by Hypervisors: The hypervisor controls the degree of separation between virtual machines. There is a risk that guests' secrets will be revealed if the hypervisor's security is not guaranteed. Therefore, the hypervisor needs better techniques for controlling access.

Table 3: Here are a few publications that discuss the difficulties with hypervisor security

S. no.	Author	Title of the security scheme	Work proposed	Strengths	Weakness
1	Romney, 2013	Hypervisors' Versatility, Adaptability, and Productivity in the Classroom of Engineers.	co-created a Master of Science in Cyber Security and Information Assurance (MS-CSIA) degree program at NU with Efficiency Student access to cutting-edge technology; agility; flexibility; simplicity of cloning;	The use of more than one authentication method improves safety. The bandwidth has been doubled from 50 Mbps to 100 Mbps.	When virtual memory (VM) size grows from 200 to 770, it becomes a crucial concern.
2	Sabahi, 2012	Safeguarding Virtualization in a Cloud Setting Technology based on a hypervisor is used.	Recommended a different approach to virtualization security that relies on a hypervisor.	A safer environment. Identifies an overflow attack. Better use virtualization.	Both VSEM and VREM are essential to the effectiveness of a security system.
3	Turnbull, 2013	Limitations: Examining Possible Entry Points for Hypervisor Attacks.	Four possible attacks in the ESXi5.0 hypervisor were found and examined.	Cloud computing is now safer to eliminate data rerouting and system call hooking.	
4	Brohi, 2013	Security Risks in Virtualized Cloud Computing Environments: Identification and Analysis (VCCI).	The Virtualization Attack Model (VMM) is a technique for virtualizing CCI-style attacks against VCCI.	Protected VCCI by tracing intrusions both from the inside and the outside.	

5	Laniepce, 2013	Intruder Detection and Prevention in IaaS Clouds using Hypervisor-Based Engineering.	advocated for a hypervisor-based method of keeping tabs on things	Perhaps most encouraging, it strengthens end users' virtual machine (VM) security.	That's up to the reliability of your cloud service.
6	Nimgaonkar, 2012	Ctrust is an infrastructure for running applications in the cloud safely and reliably.	The Ctrust framework, a proposed attack model, and a prototype implementation are presented.	Gives people a sense of safety and confidence. Scalable.	The incorporation of hardware design.

The VMM/Hypervisor from both internal and external threats. When an overflow attack occurs, hypervisor-based monitoring immediately alerts the administrator. By safeguarding the hypervisor as a whole, we can eliminate a potential catastrophic failure point (SPoF). If you want to implement the no hypervisor idea, you'll have to upgrade your operating system to include all the capabilities that hypervisors typically provide. However, doing so increases the already high complexity of the OS beneath it. This means that the hypervisor is essential for implementing virtualization.

For cloud computing to work, virtualization must be at its core. The VMM allows for the construction, suspension, restart, activation, and allocation of resources for Virtual Machines (VMs). The cloud computing paradigm suffers from SPoF's performance degradation and must be protected.

Cloud-based virtual machines (VMs) share the hardware layer's central processing unit (CPU), memory, network interface card (NIC), and storage space (among other resources). If a visitor can circumvent DAC and MAC due to a hypervisor flaw, isolated protections are at risk. Hardware security and vulnerability considerations have been brought to light, as Zissis [17] has noted. In the lack of protection to hardware, a variety of dangers, including Distributed Denial of Service (DDOS), hardware disruption, hardware theft, hardware modification, abuse of infrastructure, and so on, are a possible; server placement, firewall upkeep, and hardware health monitoring are all problems at the physical layer, as categorized by Mathisen [18].

In addition to the problems described above, hardware health monitoring is essential, as Turnbull [19] explains. This is necessary for determining the capabilities of the various hardware components and conveying that information to the kernel and the virtualization manager. To reduce the impact of issues in the physical layer, the system should employ a

robust authentication method in the virtual Border to lessen hyperjacking's associated problems.

6. Problems With The Data Itself

Any crypto-cloud system's entities may be considered extensions of the data that serves as its source and beating organ. Table 1 shows that CSA feels data breaches are the most significant security risk. Understanding how many layers of protection the new computing technology offers to the data the author foresees before adopting is crucial since hacking skills are also well-versed. Data Leakage is a problem that arises when data is stored off-site (outside of our control) to support several tenants. Data at every point of its life cycle—from creation to distribution to use to sharing to archiving to deletion, as outlined by Chen [20]—must be safeguarded. Generally, there are two types of data level security: those that apply while the data is in motion and when the information is at rest. Since data transmission is performed using TLS by default, there are no additional security concerns associated with data-in-transit compared to data-at-rest. It's more appealing to a hacker to access data when it's resting in storage.

6.1. Information in transit

During data transfers, entities in the crypto-cloud interact with one another. Instances of the following problems may arise due to the entities' attempts to communicate with one another via a secure communication channel, such as Transport Layer Security.

6.1.1. Data Lineage

There's the concept of "data lineage," which refers to the history of where and from whom specific data has been collected. Data lineage is a concept suggested by Bhadauria and Sanyal [5]. It's useful for auditing. Due to the non-linear structure of the cloud, it is one of the most challenging and time-consuming aspects of tracing.

6.1.2. Data Leakage

The second problem is data leakage, which occurs whenever more than one tenant accesses data. As Sabahi [7] described, one of the concerns is information loss. Security flaws in Google Docs have been known since at least March 2009, when Chen first brought them to light [20]. With such a high risk of compromised information, handling must be done with extreme caution. Leaks of sensitive information can occur through various channels, including instant messaging, email, webmail, blogs/wikis, malicious web pages, the file transfer protocol (FTP), and USB/mass storage devices.

6.2. DATA- IN-REST

Vyas [21] presented a method for ensuring data integrity and performance during cloud storage and retrieval. Improve cloud data security by storing encrypted files, hash files, and meta-data.

Data security in the cloud, using cryptographic mechanisms to protect individual privacy, is a topic that has been extensively reviewed by Chatterjee [22].

6.2.1. Data Recovery

Data recovery is extracting data from damaged or unreadable storage media and restoring it for use. Figure 11 shows the progression through the four stages of data recovery. When a file is deleted, just its information is erased; the data itself is still stored on the disc. Retrieval using "file carving" is possible. Bifragment gap carving, Smart Carving, and Carving memory dumps are a few examples of popular Carving techniques. Problems with the operating system, the disc, or the deletion of files are common obstacles to data recovery. These obstacles must be conquered.

6.2.2. Data Remanence/Sanitization/Removal

All data must be thoroughly and safely wiped after its useful life. One of the most time-honored methods of cleaning data is overwriting. As stated by Chen [20], physical properties allow for the restoration/recovery of lost data, which might lead to the exposure of private information. It is feasible to retrieve information from damaged storage media with the proper knowledge and tools. There has to be consideration given to the persistence of data after deletion.

6.2.3. Data backup

Data loss occurs when data is updated often. In the event of data loss, it is essential to have a recent backup stored in the cloud or on an external server. The 3-2-1 rule, as outlined by Bhargav Vora [23], requires keeping three copies of all critically significant data: one primary copy and two backups. Two separate storage mediums are used to protect against potential threats. Hold one duplicate in a secure location. Replication maintenance compromises data safety.

6.2.4. Data isolation

Information must be kept completely isolated from unauthorized access. Access control and encryption methods should protect sensitive information from prying eyes. A user's identification can provide several fine-grained access control types, such as attribute-based, time-based, etc. Isolation is a very exclusive setting. Carelessness can result in a virtual machine (VM) to VM assault, compromising user privacy.

6.2.5. Data segregation

The separation of data across users in a virtualized cloud environment is known as "data segregation." Data segregation is a concern brought up by multi-tenancy, according to Negi [24]. Data segregation in the cloud should be accomplished with the help of highly protected protocols and encryption methods. SQL injection, unsecured storage, and improper data validation contribute to data segregation issues. In a multi-tenant setting, the difficulty of data segregation can be reduced by catering to tenants' specific needs in the ways outlined.

6.2.6. Data Lock-in

Data lock-in is the most significant barrier to achieving data portability and interoperability, bringing us to point six. Sax [25] warns that, according to a well-documented industry perspective, the possibility of cloud provider lock-in impedes the free flow of data into, throughout, and beyond the cloud. Due to the

lock-in nature, it is challenging to integrate data from many sources. Cloud users should be unaffected by the current situation with one provider.

6.2.7. Data Location

Where the data is physically stored is crucial to the success of any storage as a service model. Users are hesitant to keep sensitive data in the cloud due to the lack of transparency surrounding the data's physical location. It's a typical challenge for businesses. Concerns about data safety, legality, and meeting regulatory standards arise when their whereabouts are unknown. This is a complicated matter because certain cloud storage services can't be relied on.

Problems that arise when data is both in motion and at rest constitute Section 6.3.

1. The first tenet of sound data management ensures that only authorized parties may read and change stored information. Independent verification of data integrity is possible. However, Kaur [26] offered a data correctness system that assured data security through a third-party audit. Static and dynamic data require security measures to prevent accidental or malicious use or disclosure.

2. Integrity and computational correctness are data provenance aspects, referred to as "provenance." Provenance may be defined as (integrity + computational correctness =). However, Muhammad Rizwan Asghar[27] emphasized the significance of provenance in post-incident investigations by explaining how data is created. Martin[28] proposed a risk-based strategy for determining origin. Data provenance presented several difficulties, including computational cost, storage overhead, platform independence, and application independence.

Table 4: The current methods for fixing Data Level Challenges

S. no	Author	Title of the security scheme	Work proposed	Strengths	Weakness
1	Chen, 2012	The challenges of protecting sensitive data and personal privacy in the cloud.	Survey: Data security and privacy at different stages of the data's life cycle were analyzed.	Discussed the data security and privacy studies that will be conducted in the future	
2	Wang, 2012	The move toward safe and reliable cloud storage services.	Saving money on bandwidth and processing by auditing cloud storage.	Accurately pinpointing the source of data problems in a hurry. Dynamic efficiency.	Stores supplemental data structures locally for ease of usage.

3	Liu, 2013	Safe Multi-Owner Cloud Data Sharing for Evolving Communities, or Mona.	With MONA, cloud-based groups may be dynamic and responsive.	100% Safe and Effective. Revoked users incur no additional costs for storage or processing.	
4	Wei, 2014	Protection of personal data during cloud computing storage and processing.	Prevention of privacy breaches and promotion of a trustworthy auditing methodology for computing.	This first protocol audits safe storage and computation—the bare minimum.	Using SecCloud takes a little longer than the original protocol.
5	Dong, 2014	Developing a cloud-based file-sharing service that meets these criteria—efficient, scalable, and protective of user privacy—is a primary goal of modern cloud computing.	A strategy utilizes both CP-ABE and IBE methods.	Data privacy is efficient, scalable, and adaptable. Safe and allowing for granular permissions	
6	Dong, 2015	Cloud-based data collaboration services that prioritize security and scalability, aka SECO.	An identity-based, multi-level encryption system for use in an insecure cloud environment.	Safe online data sharing with granular permissions Efficient Minimal computational, networking, and storing overhead.	Data synchronization and security concerns have not been resolved.
7	Khalid, 2013	Protocol for improved authentication and authorization based on security and privacy, implemented in the cloud.	A method for establishing trust and exchanging information in an untraceable fashion.	Simplicity to implementing Compatible	

8	Sun, 2013	A system for assessing encryption software based on its properties.	The use of properties is recommended to verify the security of encryption software.	Effective. Effectiveness at finding problems is rather good.	The differences between defects that have been mimicked and those that occur in real-time are striking. The Number of Metamorphic Relationships is bounded (Mrs)
9	Liu, 2014	Cloud-based data sharing security protocol that uses time-based proxy re-encryption.	A TimePRE that causes a user's privileges to lapse on their own time.	Accomplishes efficient and granular access control. A safe and helpful option There is no granularity in the time measurements.	The user's total number of keys will increase proportionally. The price of decryption is little.
10	Koo, 2013	Safe and quick decryption of encrypted data. Data on the cloud utilizing attribute-based encryption.	A fast information retrieval system based on ABE.	Optimal for Large Data Archives Controlled entry and rapid searching	
11	Puthal, 2017	The efficient security of large-scale sensing data streams based on a dynamic prime number.	Security verification for massive data streams using dynamic prime numbers (DPBSV).	It cuts down on time spent communicating. Increases verification efficiency. Saves time. Make use of minimum size.	
12	Shaikh, 2015	Cloud computing security is only achievable with properly organized data.	A system for collecting and analyzing data tested with representative data sets.	Strength and safety are greatly enhanced.	

The most fundamental component of a cloud that needs protection is its data. Threats to data security can occur both while information is in transit and while it is stored. Without adding to the cost of storage, transmission, or computing, Table 4 outlines the several security concerns that must be overcome. For instance, the SecCloud method adds negligible time over the currently used, more insecure protocol. Reducing exposure even if doing so causes unexpected financial strain. Combinations of encryption methods that are efficient, scalable, adaptable, secure, and allow for granular control over who has access to data. Research in the future can focus on methods that improve security while requiring less work from administrators.

A system that provides maximum security at a minimum cost in terms of memory, bandwidth and processing power is urgently required. The system must be reliable, extensible, and safe. Security, however, should not be an afterthought; instead, it should permeate the entire system and be built at each step (Computational, Communicational, and Service Level Agreement).

7. Service Level Agreements (Slas)

Providers are responsible for delivering services to customers by agreed-upon SLAs. The obligation of upholding SLAs falls on crypto-fundamental cloud entities' shoulders. Bandwidth, central processing unit, memory, and critical management are just a few factors that might affect resource allocation at any given time. SLAs may be broken down into three distinct tiers: customer-centric, service-centric, and multi-tiered. The amount of money and workforce allocated is crucial and shouldn’t be underestimated.

While privacy concerns motivate the development of service-level agreements, principles of honesty motivate their introduction. Hoehl [29]. Risk reduction and efficient assignment of responsibilities between parties is facilitated by incorporating security metrics within the SLA. Regarding security management, no one SLA standard fits all scenarios. However, measures such as the European Commission's SPECS (Secure Provisioning of Cloud Services) and ENISA's (European Network and Information Security Agency) guarantee security by requiring the upkeep of SLAs. Quality of Service (quality of service) may be improved using SLA. Define, negotiate, monitor, and enforce the terms of a contract using Service Level Agreements. While defining and negotiating a contract, both parties can determine their respective roles and the duration of their separation agreements. The relationship between the supplier and the customer is strengthened using monitoring and enforcement.

Guaranteed service availability was also brought forward by Dash [30]. Depending on the SLA, the provider's capabilities, the efficiency of the users, and the accessibility of the services will vary. To mitigate any adverse outcomes, consider the following information. Loss of bandwidth and operations, business continuity, data location, data appropriation,

data integrity, and data dependability are just a few of the many concerns that must be addressed. The pay-as-you-go business cannot persist without adequate SLAs.

8. Wrapping Up

Questions of data, system and Service Level Agreement security are examined. Security problems with virtualization and data are seen as the most dangerous to a computer system. The benefit of cloud computing is enhanced through virtualization, a core component of the cloud. The problems that can arise at the virtual, virtualization and physical levels are discussed. There are two main types of data security problems: those that occur when the data is at rest and those that occur while it is in transit. Both are investigated, and there's a pressing need to resolve any problems. Numerous chances for hackers to crack the crypto-system exist nowadays due to the proliferation of security threats. However, many studies and polls agree with the author's vote. Cloud computing still appears to be in its infancy regarding protecting user data.

Table 5 shows how our survey stacks up against previous survey papers when comparing the three foundational dimensions. The table reveals that very few reports have comprehensively examined the causes and consequences of problems at the Virtual Machine, Hypervisor, and Hardware levels of computing. Future research on Service Level Agreements has to be deeper and broader. This article paves the way for future research in cloud computing to explore previously uncharted territory.

Table 5: A look at our study in comparison to others from three different vantage points

S. no	Author	Communication level		Computational/Functional level			SLA level	
		Network level	Application level	Virtualization		Data security		
				V.M. level	Hypervisor level	Hardware level		
1	Ali, 2015	X		X	X		X	X
2	Rong, 2013						X	X
3	Zissis, 2012		X	X		X	X	
4	Sun, 2011	X	X				X	
5	Shahzad, 2014	X					X	X
6	Rao, 2015	X					X	
7	Soofi, 2014	X	X				X	
8	Warhade, 2014	X	X				X	
9	Padhy, 2011	X	X	X			X	X
10	Denz, 2013			X	X	X		
11	Ouedraogo, 2015			X	X		X	X
12	Rawat, 2014					X	X	
13	Our survey	X	X	X	X	X	X	X

Table 5: A look at our study in comparison to others from three different vantage points

Security should not be an afterthought for cloud service providers; it should be a primary concern.

9. References

[1] P. Mell and T. Grance. "The NIST definition of cloud computing". National Institute of Standards and Technology; 2009http://csrc.nist.gov/groups/SNS/cloud-computing.

[2] K. Walker. "Cloud security alliance(CSA)". The treacherous 12: cloud computing top threats in 2016. https://cloudsecurityalliance.org/media/news/cloud-security-alliance-releases-the-treacherous-twelve-cloud-computing-top-threats-in-2016/.

[3] S. Kamara and K. Lauter. "Cryptographic cloud storage". Microsoft Research Cryptography Group; January 2010 http://research.microsoft.com/pubs/112576/cryptocloud.pdf.

[4] O. Rebollo, D. Mellado, E. Fernandez-Medina and H. Mouratidis. "Empirical evaluation of a cloud computing information security governance framework". Inf SoftwareTechnol 2015. vol. 58: pp. 44–57www.elsevier.com/locate/infsof.

[5] R. Bhadauria and S. Sanyal. "Survey on security issues in Cloud Computing and Associated Mitigation Techniques". Int J Comput Appl (0975-888). vol. 47, no. 18. June 2012.

[6] S. Laniepce, M. Lacoste, M. Kassi-Lahlou, F. Bignon, K. Lazri and A. Wailly. "Engineering intrusion prevention services for iaas clouds: the way of the hypervisor", 2013.IEEE seventh international symposium on service-oriented system engineering.

[7] F. Sabahi. "Secure virtualization for cloud environment using hypervisor-based technology". Int J Mach Learn Comput. vol. 2, no. 1. February 2012.

[8] R. Bose and D. Sardar. "A Secure Hypervisor-based technology creates a secure cloud environment". Int J Emerg Res Manage Technol. Vol. 4, no. 2. February 2015.

[9] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen and AV Vasilakos. "Security and privacy for storage and computation in cloud computing". Inf Sci;258: pp. 371–386. 2014. www.elsevier.com/locate/ins.

[10] Z. Qin, Q. Zhang, C. Wan and Y. Di. "State-of-the-art virtualization security in cloud computing". J Inf Comput Sci. vol.9, no. 6. 2012.

Khurram *et al. (IJECI)* 2023

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

International Journal for
Electronic Crime Investigation

DOI: https://doi.org/10.54692/ijeci.2023.0701126

Research Article

Vol. 7 issue 1 Year 2023

Nanoforensic: An Advanced Perspective in Crime Investigation

Syed Khurram Hassan[1] and Hafiza Hadia Shehzad[2]

[1] Institute of Quality and Technology Management, University of the Punjab, Lahore, Pakistan.

[2] Department of Chemistry, University of Education, Lahore.

Corresponding author: khuramshah6515@gmail.com

Received: November 28, 2022; **Accepted:** January 24, 2023; **Published:** March 03, 2023

Abstract:

Nano-forensics is the advanced application of nanotechnology-based techniques to resolve cases in forensic science. Forensic science offers scientific methods in criminal investigation. Nano-forensics deals with the development of new appoaches for fingerprint visualization, DNA isolation, forensic toxicology, explosive detection, identification of body fluids, gunshot residue analysis, detection of illicit drugs, etc. The nanomaterials used in forensic science are nanocrystals, nanoparticles, quantum dots, nanobelts, nanocomposites, nanoclusters, nanotubes, nanorods, etc. The scope of nanotechnology is very wide.

Key words: nanoforensic, nanotoxicology, forensic science, nanoparticles, nanomaterials

1. Introduction

Nanotechnology is an advanced approach to design, production, manipulation, and application of useful materials, systems, and apparatuses by regulating matter at the nanoscale. It has been used in numerous fields of inquiry, including biomedical sciences, physical sciences, electronic engineering, and many more. First, because nanotechnology can detect and analyses samples at the nanoscale, it allows for the collection and analysis of crucial evidence that was previously impossible. Second, because it can now analyze samples on a lower scale. Furthermore, nanomaterials have novel features that make it possible to gather and find evidence that was previously impossible to do so. Examples include trace amounts of explosives, DNA on fingerprints, and trace amounts of hazardous metals on palm prints.

Basic researcher and demonstration of chip-based or micro device technology for DNA analysis in forensic application are both included in the DNA Research and Develop-

ment programme. The chemical and biological defense initiative's objective is to develop a wearable, affordable technology that can warn its user of potential chemical and biological threats in time for them to take the necessary safeguards [1].

2. Characterization Of Nanomaterials

Nanomaterials can be characterized by using atomic force microscopy, dynamic light scattering, and Raman micro spectroscopy (Micro-Raman). Since electron beams serve as the light source, electron microscopy can magnify incredibly minute details of nanomaterials with resolution down to the sub-nanometer range. The light source is a cathode that produces a lens-focused high voltage electron beam. When the beam contacts a photographic plate, phosphor screen, or another light-sensitive sensor, a picture is produced. Through TEM, the internal structure of the materials under study is made visible. Scanning electron microscopy (SEM), which searches for secondary or backscattered electrons, creates images. In comparison to TEM, the process used to create the final images in SEM is very different. SEM scans can show surface shape and produces three-dimensional images [2].

2.1. Atomic Force Microscopy

AFM is very effective tool for assessing nanoparticles. It can determine magnetic forces, chemical bonding, capillary force, electrostatic force, and others. Although SEM and AFM are both capable of producing 3-D images [3].

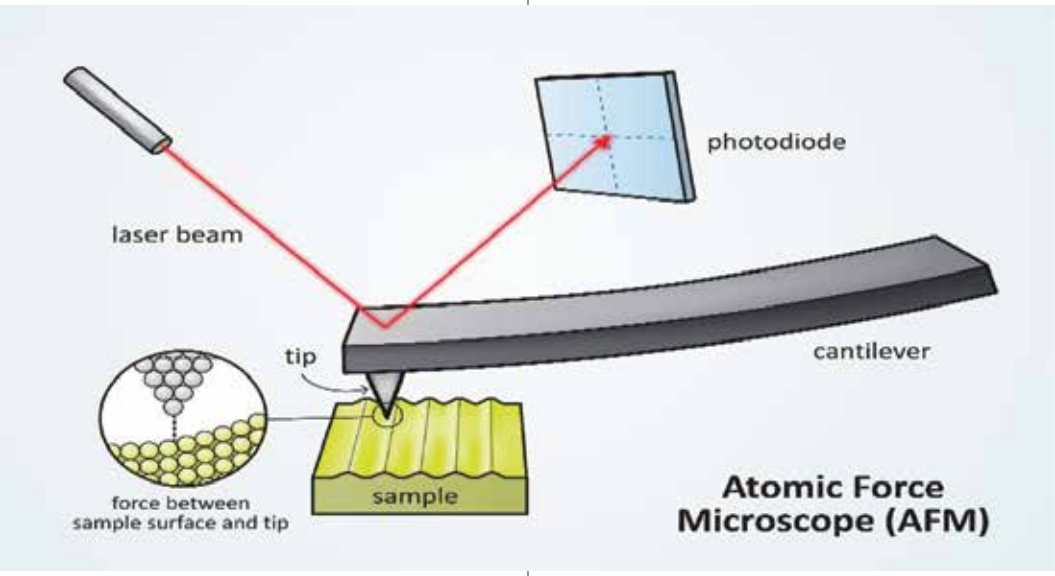

Fig 1: Atomic Force Microscope

2.2. Dynamic Light Scattering

Dynamic light scattering is a well-known technique for estimating particle size in the range from a few nanometers to a few microns (DLS). DLS is excellent at identifying even trace amounts of aggregated protein. The typical detection window is 0.8 to 6500 nm [4].

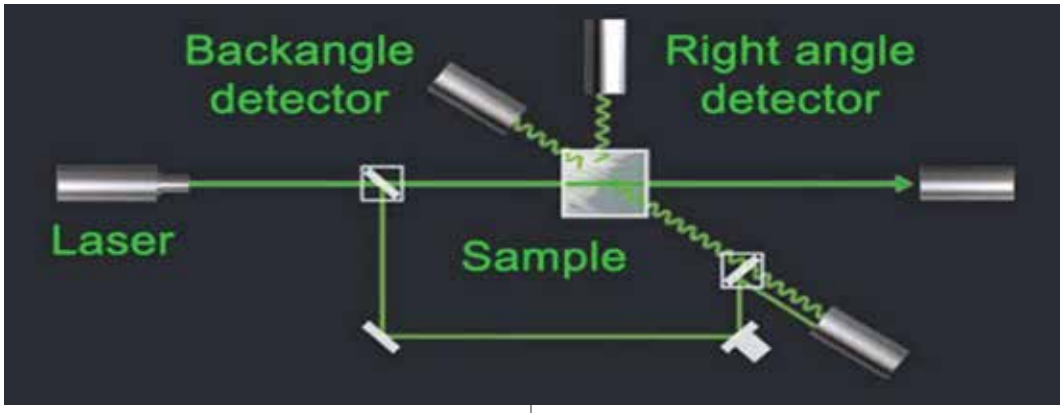

Fig 2: Dynamic Light Scattering

2.3. Raman Micro spectroscopy

Raman spectroscopy, as opposed to focusing on absorption, examines how the sample scatters light. It accomplishes this by counting photons using a charged-coupled device (CCD), a multiple dispersion prism, or a diffraction grating. Filtering removes the wavelength that is near the laser line (Raleigh scattering). The interference from water to the Raman spectrum is far less than it is for infrared spectroscopy. The study of biological objects like as cells, tissues, peptides, and proteins is thus excellently suitable to it. Extremely specific energy ranges can be connected to the rotational and vibrational motions of particular types of chemical bonds in organic molecules. The fingerprint that can be used to identify the molecule is provided [5].

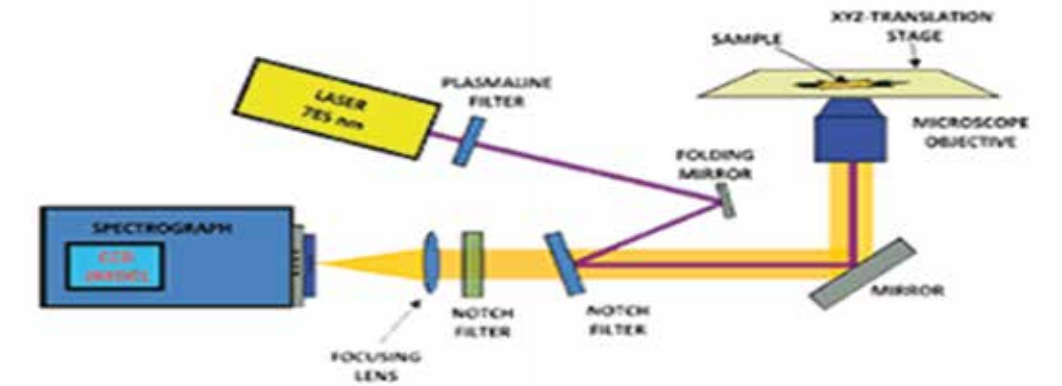

Fig 3: Raman Micro spectroscopy

3. Forensic Applications

The forensic applications of nanotechnology are as follows.

3.1. Latent Fingerprint Enhancement of CdS

Dr. Menzel invented the technique for improving latent fingerprint detection using photoluminescent CdS semiconductor nanocrystals topped with dioctyl sulfosuccinate. His idea was to use fluorescent dye to pre-fume items with cyanoacrylate ester and to paint electrical tape's sticky side with fluorescent dye [6].

3.2. Nano-Fingerprint Residue Visualization

By detecting inorganic elements in the impressions, MXRF produces images of latent fingerprints. The non-destructive analysis and stable inorganic residues make it more advantageous. Fingerprints are saved during processing and might be utilised for further inquiries, such as elemental analysis for gunshot residue. Chloride ions and potassium are the inorganic residues that can be present in fingerprints. MXRF offers an elemental assessment of the inorganic elements present in fingerprints. Additionally, MXRF has the ability to identify chemicals that are not often seen on the hands, such as sweat, saliva, lotion and sunscreen. For instance, MXRF can be used to connect salivary components with food remains in fingerprints to look into situations of missing children [7].

3.3. Gold Nanoparticles to Enhance PCR Efficiency

The effectiveness of the polymerase chain reaction can be considerably enhanced by the use of Au nanoparticles (PCR). The reaction time was found to be reduced while the heating/cooling thermal cycle rates were raised when 0.7nM of 13 nm Au nanoparticles were added to the PCR reagent. The huge increases in PCR efficiency are the result of Au nanoparticles' extraordinary capacity to transmit heat [8].

3.4. AFM and Questioned Documents

For the first time, pen and ink's 3-D surface morphology (AFM) may be studied thanks to a method created by Swiss researchers. They claim that AFM can offer crucial details for comprehending the arrangement of lines produced by ballpoint ink and ribbon dye. They claim that AFM images include the same level of qualitative data as those obtained using scanning near-infrared microscopy [9].

3.5. AFM and the Time of Death

The morphological changes in blood cells can be utilized to calculate the time of death. The cell and membrane surfaces of unfixed erythrocytes are observed to deform with time. Within a half-day, fissures and cell shrinkage occurred. An early indicator of death is protuberance on erythrocytes, which can be utilized to determine the precise time of death. A study that was published in the journal Cell Mechanisms of Cells suggests that there are two potential causes for the development of holes in cells. One is when dehydration causes holes to emerge and hemoglobin in the cytoplasm flows outward; the other is when membrane proteins thin out as a result of dehydration. A group of researchers from the University of Bristol looked into the red blood cells' (RBC) time-dependent surface adhesive force and shape. Their findings imply that AFM is a new potential forensic medicine tool (the estimation of the time of death). RBC cells on mica were noticeably larger in both form and volume than cells on glass, but, surprisingly, their adhesive properties were substrate-independent. On a mica substrate, RBC has the normal biconcave shape, while on a glass substrate, it has a flattened or bicavity shape. In controlled room temperature conditions, changes in the RBC's cell volume and adhesive force were comparable to those in uncontrolled outdoor environmental conditions. To effectively assess blood age, more research is required on a variety of environmental parameters, including humidity, pH value, temperature, and light [10].

3.6. AFM Force Spectroscopy and Bloodstain

In two steps, the nanometer-scale elasticity of

erythrocytes was examined. Red blood cells typically have a "doughnut-like" look, which indicates that they are dry. The modification of the drying and coagulation processes most likely contributed to the changing elasticity pattern over time. It is possible to estimate the age of bloodstains and utilize this information to support criminal investigations once the elasticity of time's calibration curve has been produced [11].

3.7. AFM and Trace Evidence

The surface texture parameters of environmentally problematic materials were quantitatively evaluated using AFM images as a function of exposure time. Three different types of fibres were applied to two distinct soils (town and riverbank) and two distinct types of water during 0, 2, 4, and 6 weeks (ponds and water). The average maximum peak heights (Hpm), average maximum heights (Hz), and average maximum valley depths of each sample's surface morphology were assessed (Hvm). AFM can differentiate between various environmental exposures or violent damages to fibres, making it an efficient approach for forensic evaluation of fibre evidence.

Criminals frequently use pressure sensitive adhesive (PSA), which can be found in adhesive tapes and packaging. Images illustrating the mechanical characteristics of several PSA tape types, which are frequently used to secure parcels and confine suspects in kidnapping investigations, are displayed. The AFM phase pictures of the three tapes under research show dark and bright regions that, respectively, represent the soft polymer molecules and the rough surfactants. This work is the first to use force mapping and AFM imaging to comprehensively investigate several tapes. According to a number of studies, AFM has also been applied in criminal investigations in various ways. AFM microcantilever provides the ability to do selective detection as well as surface and image analysis. The study of DNA hybridization, the discovery of two prostate-specific antigen isoforms, C-reactive proteins, Salmonella enterica, Vaccinia virus, and explosives like trinitrotoluene (TNT) and PETN are a few examples of applications. It uses the proper coatings on the cantilever surface to identify molecules [12].

4. FUTURE PROSPECTS

Taiwan has the potential and capacity to lead the world in the integration of forensic sciences and nanotechnology. More knowledge in disciplines relating to nanotechnology will be required of forensic scientists. Taiwan's forensic scientists are more qualified and knowledgeable in general than those in most other nations. It is not "mission impossible" to merge forensic science and nanotechnology and create a world-leading environment. It can be accomplished by emphasizing the development of educational research, a competent workforce, and the enabling infrastructure and resources. Additionally, greater forensic lab instrumentation use along with equipment capable of doing nanoscale analysis would be necessary for this [13].

5. CONCLUSION

Real-world criminal cases now have better forensic evidence thanks to analytical chemistry. Many forensic laboratories continue to be understaffed and underfunded, especially at the state and local levels, despite the fact that television programmed have glamorized the field and drawn attention from the general

public and potential students. To address these personnel requirements, formal programmed in forensic chemistry and forensic science education are growing, and there is already a system in place to recognized those that adhere to basic curriculum criteria. The self-evaluation process will surely help the training programmed that opt to pursue accreditation, and in the end, they will generate graduates who are more equipped and future leaders in the forensic science field.

6. Refrences

[1]. B. Srividya. "Nanotechnology in forensics and its application in forensic investigation". Res. Rev. J. Pharm. Nanotechnolvol. 4, no. 2, pp. 1-7. 2016.

[2]. Y. F. Chen. "Forensic applications of nanotechnology". Journal of the Chinese Chemical Society. Vol. 58 no. 6, pp. 828-835. 2011.

[3]. A. K. Mittal, Y. Chisti and U.C. Banerjee. "Synthesis of metallic nanoparticles using plant extracts". Vol. 31, no.2, pp. 346-356. 2013.

[4]. S. Shah, S. Dasgupta, M. Chakraborty, R. Vadakkekara and M. Hajoori. "Green synthesis of iron nanoparticles using plant extracts". Vol. 5, no.7, pp 549-552. 2014.

[5]. V. A. Boumba and T. Vougiouklakis. "Impact of blood collection tubes on erroneous 1-propanol detection and on forensic ethanol analysis". J Forensic Toxicol Pharmacol, vol. 4, no. 1: pp. 551-562. 2015.

[6]. A. Pandya and R. K. Shukla. "New perspective of nanotechnology: role in preventive forensic". Egyptian Journal of Forensic Sciences, vol. 8, no.1, pp. 1-11. 2018.

[7]. S. S. Bharati, M., Byram and V. R. Soma. "Femtosecond laser fabricated Ag Au and Cu Au alloy nanoparticles for surface enhanced Raman spectroscopy based trace explosives detection. Frontiers in Physics, vol. 6, pp. 28-35. 2018.

[8]. R. Lohiya and P. Shah. Video Based Face Detection and Tracking for Forensic Applications.

[9]. S. Singh and N. Samal. Nanotechnology: A Powerful Tool in Forensic Science for Solving Criminal Cases. Arab Journal of Forensic Sciences & Forensic Medicine, vol. 3, no. 2, pp. 273-296. 2021.

[10]. R. Peters, Z. Herrera-Rivera, A. Undas, M. V. der Lee, and H. Marvin, "Single particle ICP-MS combined with a data evaluation tool as a routine technique for the analysis of nanoparticles in complex matrices". 30(6), 1274-1285. 2015.

[11]. I. M. Sadiq, B. Chowdhury, N. Chandrasekaran, A. J. Mukherjee, "Antimicrobial sensitivity of Escherichia coli to alumina nanoparticles". Vol. 5, no.3, pp. 282-286. 2009.

[12]. K. Muthukumar. "Detection of Improvised Explosive Devices Using Nanotechnology". AJES, vol 1, no.1, pp. 11-17. 2012.

Areej *et al. (IJECI)* 2023

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

International Journal for
Electronic Crime Investigation

DOI: https://doi.org/10.54692/ijeci.2023.0701127

Research Article

Vol. 7 issue 1 Year 2023

Skin Lesion Detection and Classification Using Deep Learning

Areej Fatima
Department of Computer Science, NCBA&E, Lahore, Pakistan.
Corresponding address: areejfatima@ncbae.edu.pk

Received: December 22, 2022; Accepted: January 30, 2023; Published: March 03, 2023

Abstract:

exposure to ionizing radiation (IR) can cause basal cell carcinoma (BCC) development. A skin lesion is a region that is differentiable from another skin surface which can occur because of skin damage, allergy, etc. Even though the majority of skin lesions are mild and are not that dangerous yet few of them are infectious and their severity can turn into skin cancer. In USA, 5.4 million people are analyzed with skin cancer. The diverse types of skin lesions result in an incorrect diagnosis because of their high similarity. Skin lesions can be treated by dermatologists. The current work proposes a model for the classification of skin lesions. The proposed methodology aims to detect and classify skin lesions using potential and different deep-learning algorithms. The research focuses to achieve state-of-the-art accuracy and compare the performance of algorithms.

Keywords: deep learning (DL), skin lesion, detection, classification, ionizing radiation

1. Introduction

Skin cancer is common types of cancer which has a life-threatening effect. The atomic bombs exploded over Nagasaki and Hiroshima exposed the population to both neutrons and gamma rays. Epidemiological studies revealed that atomic bomb survivors living in Nagasaki and Hiroshima showed relationship between ionizing radiation and risk of skin cancer development (1). In united states, it has affected more than 9500 individuals on regular basis and around 3.6 million individuals suffered from basal cell skin cancer on annual basis. Most occurring form of skin cancer is Melanoma which grow in melanocytes cell and its severity can affect stomach, lungs and other body parts. According to report, the early detection of malignant melanoma can be treated 99% whereas; patients with progressive melanoma has 25% survival probability [2].

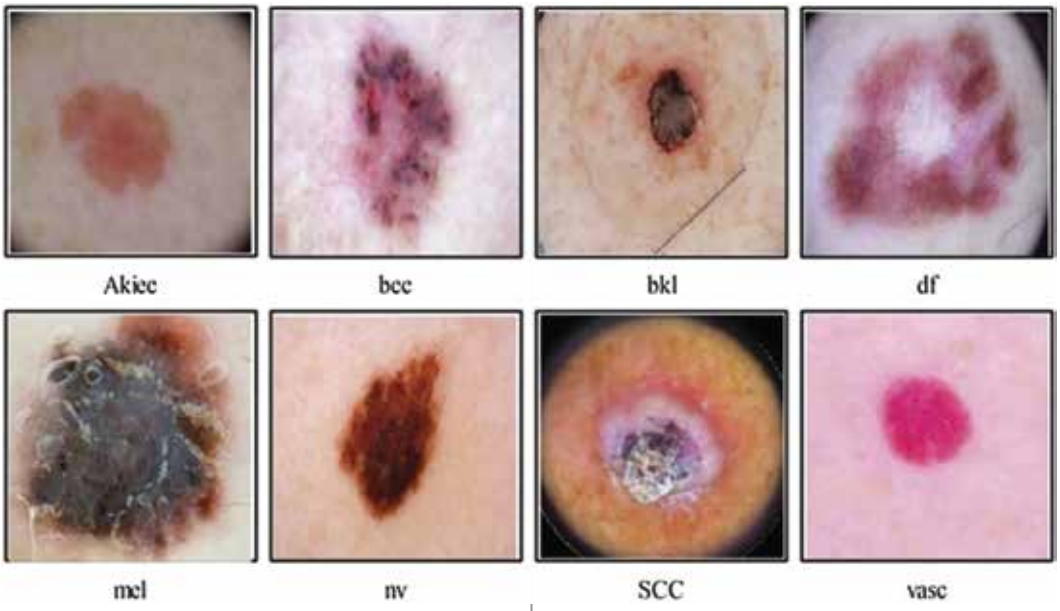

Figure 1: Sample images of Skin lesion from Ham1000 dataset

Early detection of skin lesion increases probability of patient's survival. So, the significance of detection and classification of different skin lesion has raised. The similar appearance of mild and severe skin lesion makes the detection and classification, a challenging task. The diagnostic task of skin lesion is based on ABCDE formula:

- A representing asymmetric skin surface
- B representing abnormal border
- C representing lesion color
- D representing lesion diameter
- E representing lesion enlargement

Different skin cancers seem alike with respect to above properties. There is a chance of error if detection is made via naked eye [3]. Dermoscopy is the significant method for detecting skin lesion as compared to clinical approach like biopsy etc. which is time taking procedure. But dermoscopy has some demerits as it is error prone. So, there is high need of effective technique for accurate detection with less error rate [4,5].

Deep learning (DL) is edge cutting technology which trains model for specified task more accurate as compared to machine learning. This research aims to utilize deep learning algorithm for skin lesion detection and classification through dermoscopic images as DL fast learning models are less error prone. Data augmentation is required as dataset is disproportional, it is done through affine transformation. Moreover, the model is cross-validated for effective performance [6].

2. Methodology

Figure 2 shows the proposed methodology of system.

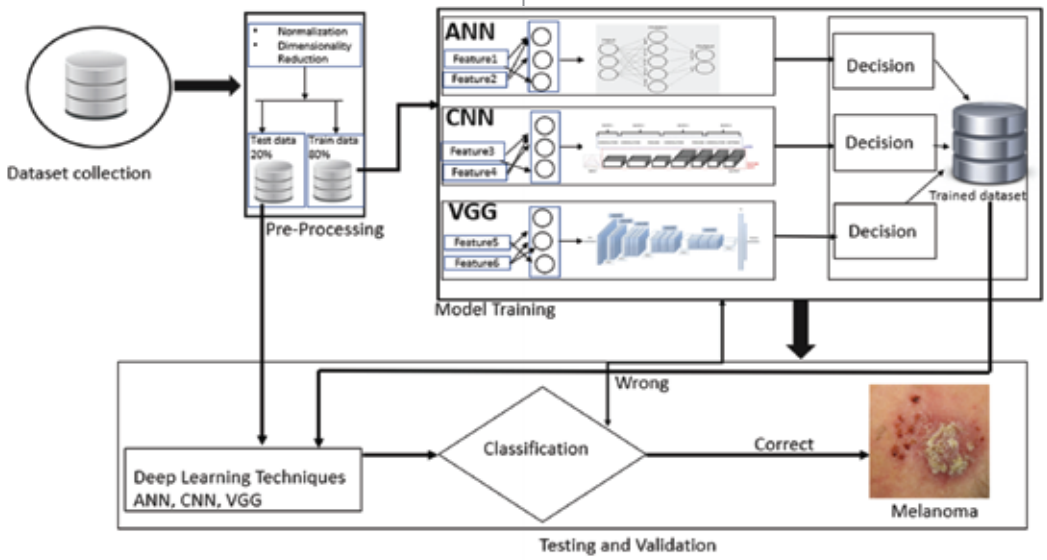

Figure 2: Proposed methodology

The methodology of the proposed research comprised of following phases:

2.1 Dataset collection

The targeted dataset is HAM1000 dataset. The HAM10000 ("Human Against Machine with 10,000 training images") dataset is a collection of multi-source dermatoscopic images of pigmented lesions,which is sourced from various populations and stored by using different techniques. It comprises of 10,015 images and 7 distinct categories of skin cancer. The seven categories of skin cancer are Melanocytic nevi, Melanoma, Dermatofibroma, Benign keratosis-like lesions, Actinic keratosis, Basal cell carcinoma, Vascular lesions.

2.2 Preprocessing

After collecting the target dataset, it is passed to a preprocessing phase where data cleansing is performed. The data underwent normalization through various methods, such as reducing missing values, resizing images, and properly labeling them. This normalization process is crucial for the success of the research as it minimizes the loss of information. This helps to concentrate on the region of interest. Figure 3 shows the dataset image size reduction to minimize the computational cost of the model.

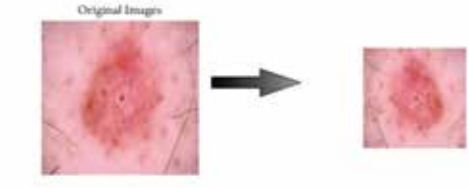

Figure 3: Image resizing

2.3 Training

After undergoing processing, the dataset was used to train three different neural network models. The training models include Artificial Neural Network (ANN), Convolutional Neural Network (CNN) and Visual Geometry Group (VGG-16).

2.3.1. ANN

Artificial Neural Networks (ANNs) are mathematical models made up of interconnected processing units, also known as neurons. These neurons receive signals from other neurons, process the information by combining and transforming it, and produce a numerical output. The processing units in an ANN mimic the structure of biological neurons and are interconnected to form a network, creating the artificial neural network.

2.3.2. CNN

A Convolutional Neural Network (CNN) is a technique in computer vision that is designed to identify and distinguish the features of images. This architecture takes skin lesion images as input and passes them through a convolutional layer, where the weights are transformed into features. These features are further refined in the pooling layer before being transformed into a 1D representation in the fully connected layer. Finally, the features are classified using a Softmax layer.

2.3.3. VGG-16

The VGG16 architecture, a Convolutional Neural Network (CNN), won the 2014 ILSVRC (Imagenet) competition. It is considered to be one of the most advanced vision models developed to date. The VGG16 model consists of 16 layers and is known for its consistent placement of convolutional and max-pool layers throughout its architecture [7].

2.4. Model Validation

After training, the performance of the model is evaluated based on some parameters. It evaluates if the model is classifying the classes accurately or not. Figure 4 shows the block diagram of the proposed research.

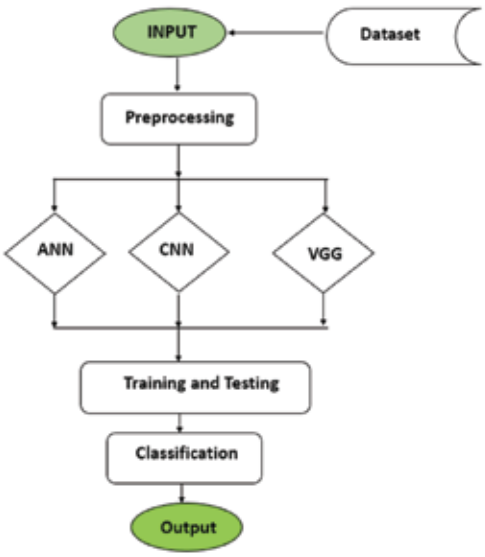

Figure 4: Block diagram of a system

3. RESULTS

In present section, the results of the proposed study are presented in numerical values and confusion matrices. Three classifiers were used for the experimental process, including Artificial Neural Network, Convolutional Neural Network, and Visual Geometry Group. First, the ANN model is considered which is comprised of three different layers (input,

hidden, and output). Figure 5 shows the architecture of ANN.

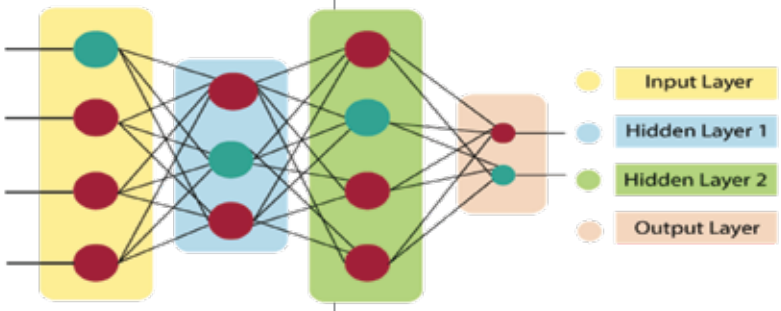

Figure 5: ANN architecture

ANN took input image from HAM1000 dataset and performance classification according to 7 different skin cancer classes. Figure 6 shows the accuracy of ANN model after 10 epochs. The average accuracy gained after ANN training is 70.5%

```
Epoch 1/10
419/419 [==============================] - 5s 10ms/step - loss: 1.0243 - accuracy: 0.6640
Epoch 2/10
419/419 [==============================] - 3s 7ms/step - loss: 0.9112 - accuracy: 0.6803
Epoch 3/10
419/419 [==============================] - 3s 7ms/step - loss: 0.8650 - accuracy: 0.6934
Epoch 4/10
419/419 [==============================] - 3s 7ms/step - loss: 0.8305 - accuracy: 0.7091
Epoch 5/10
419/419 [==============================] - 3s 8ms/step - loss: 0.7965 - accuracy: 0.7176
Epoch 6/10
419/419 [==============================] - 4s 9ms/step - loss: 0.7714 - accuracy: 0.7243
Epoch 7/10
419/419 [==============================] - 3s 7ms/step - loss: 0.7509 - accuracy: 0.7336
Epoch 8/10
419/419 [==============================] - 3s 7ms/step - loss: 0.7189 - accuracy: 0.7367
Epoch 9/10
419/419 [==============================] - 3s 7ms/step - loss: 0.6889 - accuracy: 0.7476
Epoch 10/10
419/419 [==============================] - 4s 9ms/step - loss: 0.6622 - accuracy: 0.7584
78/78 [==============================] - 0s 4ms/step - loss: 0.8591 - accuracy: 0.7054
Test: accuracy =  70.53607702255249 %
```

Figure 6: Accuracy of ANN

Figure 7 shows the confusion matrix of the ANN model.

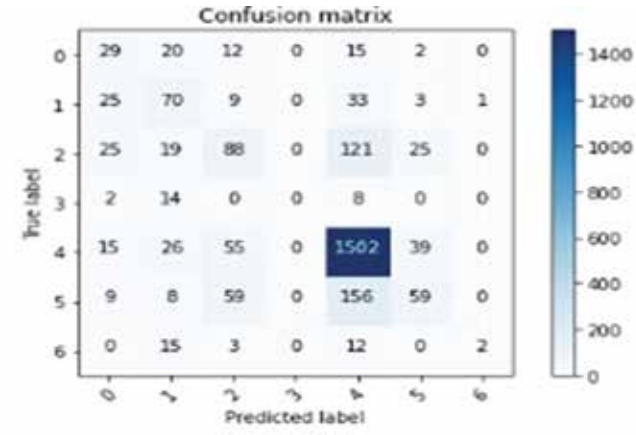

Figure 7: Confusion Matrix of ANN

Secondly, the CNN model is considered which is comprised of different layers. Figure 8 shows the general structure of CNN for skin lesion classification.

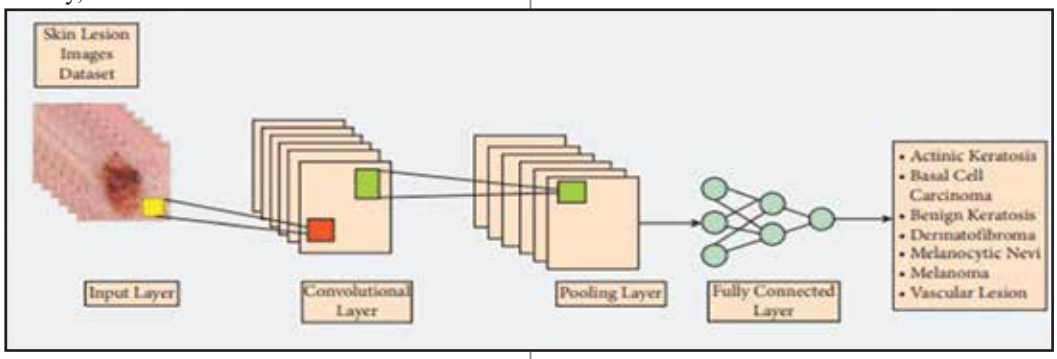

Figure 8: general structure of CNN model

CNN took input images from the HAM1000 dataset and pass them to convolutional, pooling, fully connected layers. After that, it performances classification according to 7 different skin cancer classes. Figure 9 shows the accuracy of CNN model after 10 epochs. The average accuracy gained after CNN training is 71.5%

```
376/376 [==============================] - 137s 359ms/step - loss: 1.0778 - accuracy: 0.6687 - val_loss: 0.9627 - val_accuracy: 0.6716 - lr: 1.0000e-04
Epoch 2/10
376/376 [==============================] - 132s 351ms/step - loss: 0.9692 - accuracy: 0.6892 - val_loss: 0.9323 - val_accuracy: 0.6687 - lr: 1.0000e-04
Epoch 3/10
376/376 [==============================] - 130s 346ms/step - loss: 0.9197 - accuracy: 0.6926 - val_loss: 0.9557 - val_accuracy: 0.6791 - lr: 1.0000e-04
Epoch 4/10
376/376 [==============================] - 130s 347ms/step - loss: 0.8859 - accuracy: 0.6722 - val_loss: 0.8810 - val_accuracy: 0.6836 - lr: 1.0000e-04
Epoch 5/10
376/376 [==============================] - 133s 354ms/step - loss: 0.8632 - accuracy: 0.6882 - val_loss: 0.8267 - val_accuracy: 0.6925 - lr: 1.0000e-04
Epoch 6/10
376/376 [==============================] - 133s 353ms/step - loss: 0.8425 - accuracy: 0.6955 - val_loss: 0.8548 - val_accuracy: 0.6910 - lr: 1.0000e-04
Epoch 7/10
376/376 [==============================] - 132s 350ms/step - loss: 0.8300 - accuracy: 0.6960 - val_loss: 0.8158 - val_accuracy: 0.6881 - lr: 1.0000e-04
Epoch 8/10
376/376 [==============================] - 133s 355ms/step - loss: 0.8235 - accuracy: 0.6990 - val_loss: 0.8046 - val_accuracy: 0.6910 - lr: 1.0000e-04
Epoch 9/10
376/376 [==============================] - 137s 363ms/step - loss: 0.8076 - accuracy: 0.7062 - val_loss: 0.7942 - val_accuracy: 0.7060 - lr: 1.0000e-04
Epoch 10/10
376/376 [==============================] - 134s 355ms/step - loss: 0.7885 - accuracy: 0.7150 - val_loss: 0.8177 - val_accuracy: 0.6985 - lr: 1.0000e-04
```

Figure 9: Accuracy of CNN

Figure 10 shows the confusion matrix of the CNN model.

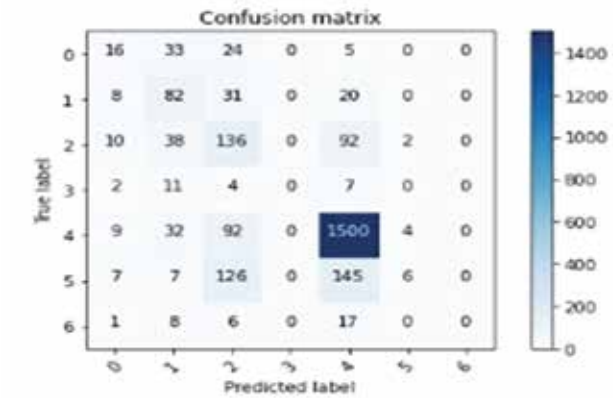

Figure 10: Confusion Matric of CNN

Thirdly, the VGG-16 model is considered which is comprised of 16 different layers. Figure 11 shows the basic structure of VGG-16.

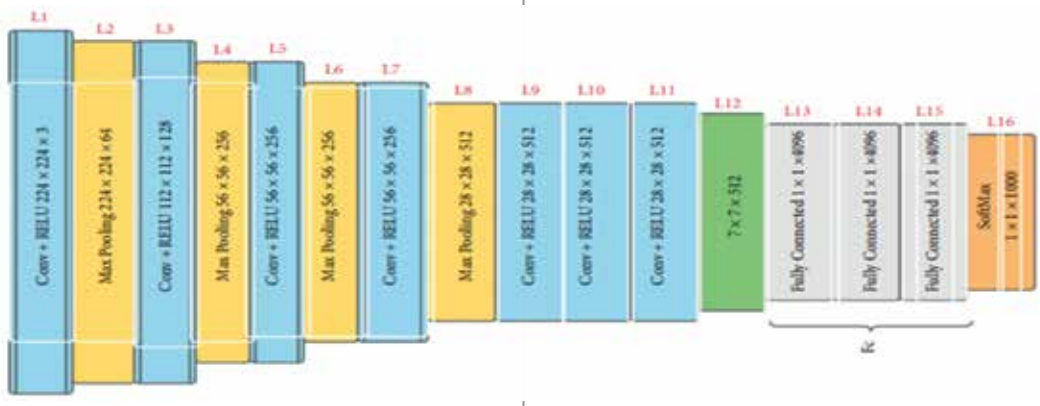

Figure 11: Basic structure of VGG-16

VGG-16 took input images from the HAM1000 dataset and pass them to its 16 different layers. After that, it performs classification according to 7 different skin cancer classes. Figure 12 shows the accuracy of VGG-16 model after 10 epochs. The average accuracy gained after VGG training is 75.6%

```
376/376 [==============================] - 319s 838ms/step - loss: 0.8644 - accuracy: 0.7013 - val_loss: 0.8025 - val_accuracy: 0.7090 - lr: 0.0010
Epoch 2/10
376/376 [==============================] - 294s 781ms/step - loss: 0.7760 - accuracy: 0.7233 - val_loss: 0.8490 - val_accuracy: 0.7119 - lr: 0.0010
Epoch 3/10
376/376 [==============================] - 293s 779ms/step - loss: 0.7379 - accuracy: 0.7406 - val_loss: 0.8001 - val_accuracy: 0.6821 - lr: 0.0010
Epoch 4/10
376/376 [==============================] - 294s 782ms/step - loss: 0.7249 - accuracy: 0.7446 - val_loss: 0.7733 - val_accuracy: 0.7313 - lr: 0.0010
Epoch 5/10
376/376 [==============================] - 291s 775ms/step - loss: 0.7194 - accuracy: 0.7411 - val_loss: 0.7503 - val_accuracy: 0.7308 - lr: 0.0010
Epoch 6/10
376/376 [==============================] - 292s 777ms/step - loss: 0.7022 - accuracy: 0.7496 - val_loss: 0.7873 - val_accuracy: 0.7433 - lr: 0.0010
Epoch 7/10
376/376 [==============================] - 292s 777ms/step - loss: 0.6977 - accuracy: 0.7562 - val_loss: 0.7814 - val_accuracy: 0.7358 - lr: 0.0010
Epoch 8/10
376/376 [==============================] - 294s 781ms/step - loss: 0.7010 - accuracy: 0.7483 - val_loss: 0.7476 - val_accuracy: 0.7313 - lr: 0.0010
Epoch 9/10
376/376 [==============================] - 295s 786ms/step - loss: 0.6979 - accuracy: 0.7506 - val_loss: 0.7308 - val_accuracy: 0.7448 - lr: 0.0010
Epoch 10/10
376/376 [==============================] - 295s 785ms/step - loss: 0.6836 - accuracy: 0.7566 - val_loss: 0.7583 - val_accuracy: 0.7373 - lr: 0.0010
```

Figure 12: accuracy of VGG-16 model

Figure 13 shows the confusion matrix of the VGG-16 model.

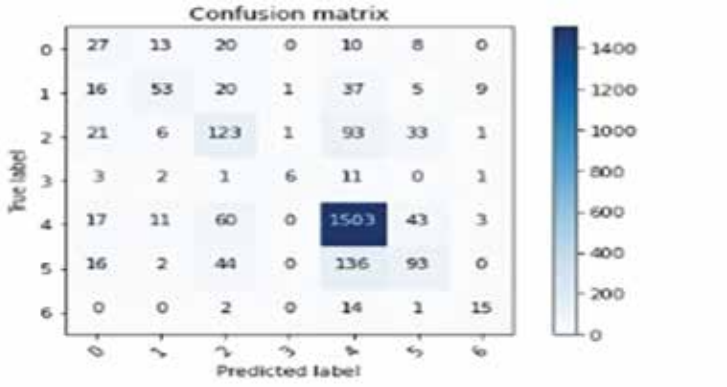

Figure 13: Confusion Matric of VGG-16

Figure 14 shows the comparison in performance of VGG, CNN and ANN.

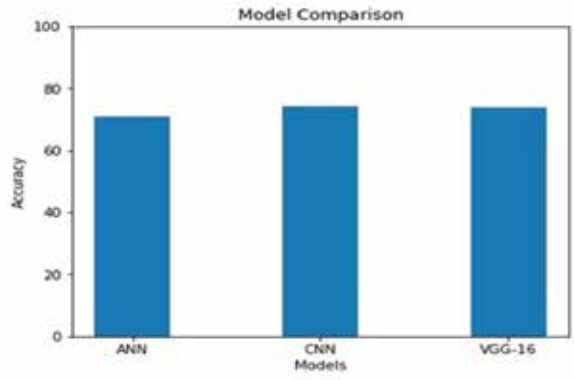

Figure 14: Performance comparison of 3 models

Figure 15 shows a comparison of the model performance of ANN with respect to Precision, Recall and F1-score.

```
Precision
['0.26%', '0.48%', '0.43%', '0.12%', '0.81%', '0.41%', '0.44%']
Recall
['0.29%', '0.51%', '0.22%', '0.08%', '0.92%', '0.25%', '0.34%']
F1 Score
['0.28%', '0.49%', '0.29%', '0.10%', '0.86%', '0.31%', '0.39%']
Specificty
0.46
```

Figure 15: Precision, Recall, F1-Score of 7 classes with respect to ANN

Figure 16 shows a comparison of the model performance of CNN with respect to Precision, Recall and F1-score.

```
Precision
['0.33%', '0.50%', '0.42%', '0.00%', '0.85%', '0.66%', '0.66%']
Recall
['0.38%', '0.65%', '0.51%', '0.00%', '0.91%', '0.21%', '0.59%']
F1 Score
['0.35%', '0.56%', '0.46%', '0.00%', '0.88%', '0.31%', '0.62%']
Specificty
0.5882352941176471
```

Figure 16: Precision, Recall, F1-Score of 7 classes with respect to CNN

Figure 17 shows a comparison of the model performance of VGG with respect to Precision, Recall and F1-score.

```
Precision
['0.32%', '0.53%', '0.46%', '0.62%', '0.83%', '0.54%', '0.76%']
Recall
['0.31%', '0.59%', '0.40%', '0.42%', '0.92%', '0.28%', '0.41%']
F1 Score
['0.31%', '0.56%', '0.43%', '0.50%', '0.87%', '0.37%', '0.53%']
Specificity
0.5714285714285714
```

Figure 17: Precision, Recall, F1-Score of 7 classes with respect to VGG

4. CONCLUSION

A method was developed in the proposed study for classifying seven types of lesions. The proposed method achieved high performance measures, including accuracy, sensitivity, specificity, and precision respectively. The performance of methods increased when the number of images in all classes decreased to address the imbalance issue. Fine-tuning all architecture layers resulted in higher performance measures compared to fine-tuning only the replaced layers. Additionally, the comparison has also performed to evaluate the performance of all three models (VGG, CNN, ANN). After experimental analysis, VGG outperform in classification as compared to other two models with 75.6% accuracy.

5. REFERENCES

[1]. H. Sugiyama, M. Misumi, M. Kishikawa, M. Iseki, S. Yonehara and T. Hayashi. “Skin cancer incidence among atomic bomb survivors from 1958 to 1996”. Radiat Res. vol. 181: pp. 531-539. 2014.

[2]. H. K. Koh, ‘‘Melanoma screening,’’ Arch. Dermatol., vol. 143, no. 1, pp. 101–103, Jan. 2007, doi: 10.1001/archderm.143.1.101.

[3]. Y. Zong, Y, Yang, and T. Hospedales. “MEDFAIR: Benchmarking Fairness for Medical Imaging”. arXiv preprint arXiv:2210.01725. 2022.

[4]. H. Basak, R. Kundu, and R. Sarkar. “MFSNet: A multi focus segmentation network for skin lesion segmentation”. Pattern Recognition, 128, 108673. 2022.

[5]. S. Singla. “Deep Learning for Medical Imaging From Diagnosis Prediction to its Counterfactual Explanation”. arXiv preprint arXiv:2209.02929. 2022.

[6]. A. Singh, S. Bera, P. Chaturvedi, P. Gadhave and C. S. Lifna,. “DermoCare. AI: A Skin Lesion Detection System Using Deep Learning Concepts”. In Data Intelligence and Cognitive Informatics”: Proceedings of ICDICI 2022

(pp. 39-51). Singapore: Springer Nature Singapore.

[7]. M. S. Khan, K. N. Alam, A. R. Dhruba, H. Zunair and N. Mohammed. "Knowledge distillation approach towards melanoma detection". Computers in Biology and Medicine, 105581. 2022.

Nadia *et al. (IJECI) 2022*

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

International Journal for
Electronic Crime Investigation

DOI: https://doi.org/10.54692/ijeci.2023.0701128

Research Article

Vol. 7 issue 1 Year 2023

Data Security and multi-cloud Privacy concerns

Nadia Tabassum, Humaria Naeem and Asma Batool

1Department of computer science, Virtual university of Pakistan

Corresponding author:nadiatabassum@vu.edu.pk

Received: December 25,2022; **Accepted:** February 2,2023; **Published:** March 03,2023

Abstract

The security, privacy, and challenges of establishing trust in cloud computing are examined in this paper. It discusses the issues that must be resolved to guarantee the security, privacy, and reliability of data processed, stored, and shared in cloud architecture. Cloud computing is a rapidly growing field, with more and more individuals and organizations adopting it as their preferred data storage and processing method. However, with this growth comes the need for increased attention to privacy, security, and trust in cloud computing. In this paper, we review the current state of privacy, security, and trust in cloud computing and examine the various strategies and technologies being used to address these concerns. We discuss the importance of end-to-end encryption, strong access controls, and data anonymization techniques in protecting user data in the cloud. Additionally, we analyze the role of trusted third parties, such as auditors and certifications, in ensuring the integrity of cloud services. Finally, we consider the impact of emerging technologies, such as block chain and homomorphic encryption, on the future of privacy, security, and trust in cloud computing. Overall, our analysis highlights the need for ongoing research and development in this area to ensure that cloud computing remains a secure and trustworthy platform for users.

Keywords: Privacy Security, Trust Build, Cloud computing, data security

1. Introduction

Cloud computing has revolutionized how we store, process, and access data. With the growth of this technology, there is a need for increased attention to privacy, security, and trust in cloud computing. In this paper, we review the current state of privacy, security, and trust in cloud computing and examine the various strategies and technologies being used to address these concerns[1].

Cloud computing allows users to store their data in a remote server that can be accessed from anywhere with an internet connection. This has allowed individuals and organizations to reduce their reliance on physical hardware and access their data anywhere. However, this

convenience comes with its own set of challenges. Cloud computing services are vulnerable to a variety of security threats, including data breaches, data loss, and unauthorized access [2].

Privacy is another major concern in cloud computing. Users must often provide sensitive personal information to cloud service providers, such as their name, email address, and payment details. This information can be used for malicious purposes like identity theft or fraud. Additionally, cloud service providers may collect user data for advertising or other purposes, which can raise concerns about user privacy[3].

Trust is also a critical issue in cloud computing. Users need to trust that their data is being stored and processed securely, and that their service provider is acting in their best interests. Cloud service providers may also need to trust their users, to ensure that they are not engaging in malicious activities that could compromise the security of the service[4].

To address these concerns, various strategies and technologies have been developed to improve cloud computing services' privacy, security, and trust. These include end-to-end encryption, strong access controls, data anonymization techniques, trusted third parties such as auditors and certifications, and emerging technologies such as blockchain and homomorphic encryption[5].

Researchers and business experts have identified several security problems in the cloud. solitude as well as computing data exposure, and data management security of the virtual operating system, secrecy mission, trust, and compliance specific security assurance. During dynamic situations, problems arise cooperation and sharing across a number of clouds Concerns of trust, in particular. Multicloud computing raises issues of policy and privacy as shown in Figure 1

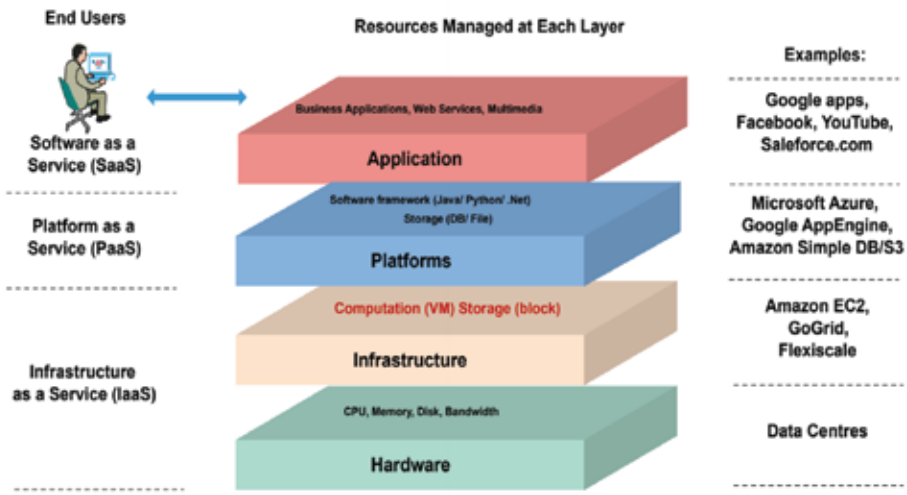

Figure 1: Cloud Resource Management

This paper will provide an in-depth analysis of the current state of privacy, security, and trust in cloud computing. We will examine the various strategies and technologies being used to address these concerns and discuss the implications of emerging technologies on the future of cloud computing. We aim to provide a comprehensive understanding of the challenges and solutions related to privacy, security, and trust in cloud computing, and highlight the need for ongoing research and development in this area[6].

Network security in cloud technology is very important as it affects the complete cloud system deployment from its base, while taking an example of mobile platforms in cloud technology there are a diverse range of users that access cloud services using their smart machines by connecting with a cloud network, so while implementing cloud system if the cloud service provider will not look for security challenges it may allow any external user to access the information and services[7]. besides network firewall is deployed and if the virtual machine is not working properly it may cause a change in the routing path of firewall security, where data can easily be shared and access over multiple clouds and by any unauthorized person as shown in Fig.2

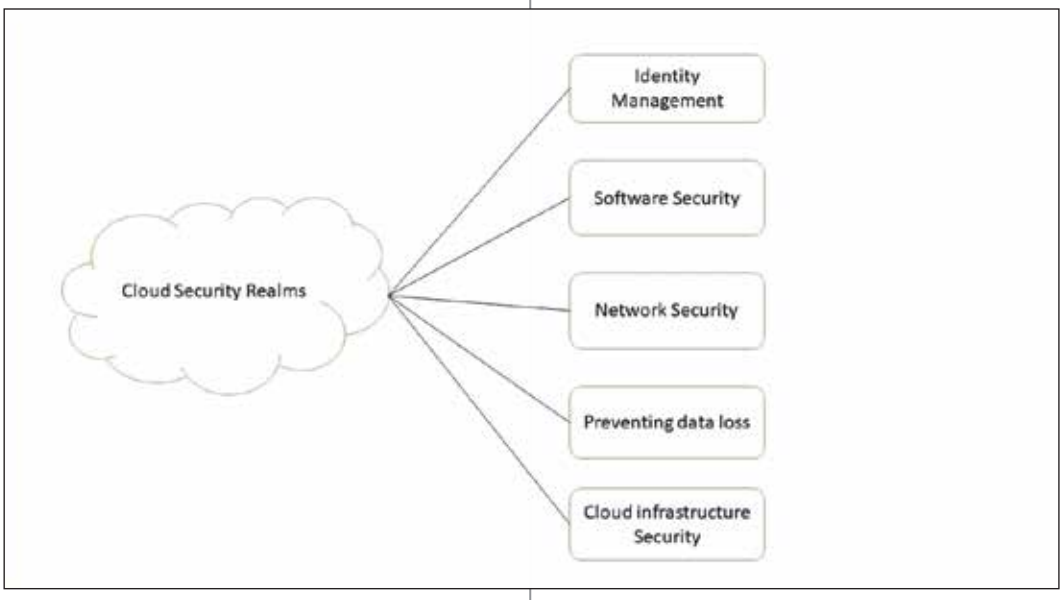

Figure 2. Cloud Security Realms

2. Literature Review

In order to better understand the security, privacy, and trust-building challenges in cloud computing, this paper reviewed the body of previous research in the field. The review included research papers, norms, policies, and recommended practices. and other sources on topics such as encryption, access control, authentication, data leakage prevention, and incident response. Additionally, the literature review highlighted the various challenges

organisations face to ensure the security and trustworthiness of data stored and transmitted in a cloud environment. Consequently, this review provides an in-depth overview of the current state of research on this subject[8].

To comprehensively assess the security, privacy and trust-building issues in cloud computing, this literature review surveyed recent research papers, standards, guidelines and best practices. This review began with examining encryption and access control protocols such as AES and PKI, which, when properly implemented, can protect data from unauthorized disclosure and access. Additionally, authentication protocols such as SAML and OAuth were assessed for their ability to verify the identity of users and prevent unauthorized access. Data leakage prevention measures such as DLP and tokenization, as well as threat detection and incident response methods, were also discussed. The literature review also looked at the various challenge's organizations may be facing when trying to ensure the security and trustworthiness of data stored and transmitted in a cloud[9].

Cloud computing has rapidly gained popularity as a data storage and processing method for individuals and organizations. However, the potential vulnerabilities of cloud computing systems have raised concerns about privacy, security, and trust. This section provides a detailed review of the current state of these issues and the strategies and technologies being used to address them[10].

Privacy is a major concern in cloud computing. Users are often required to provide personal information to cloud service providers, which can be used for malicious purposes. Additionally, cloud service providers may collect user data for advertising or other purposes, which can raise concerns about user privacy. One strategy for addressing privacy concerns is end-to-end encryption. This technique encrypts user data before it is transmitted to the cloud, ensuring that only the user can access it. Another strategy is data anonymization, which removes personally identifiable information from data sets to protect user privacy[11].

Cloud computing systems are vulnerable to a variety of security threats, including data breaches, data loss, and unauthorized access. To address these threats, cloud service providers have implemented a variety of security measures, such as strong access controls and intrusion detection systems. Additionally, cloud service providers may use trusted third parties, such as auditors and certifications, to ensure the security of their services. Another emerging technology that can improve cloud security is homomorphic encryption, which allows for data processing without decrypting the data[12].

Trust is a critical issue in cloud computing. Users need to trust that their data is being stored and processed securely, and that their service provider is acting in their best interests. Cloud service providers may also need to trust their users, to ensure that they are not engaging in malicious activities that could compromise

the security of the service. To address trust issues, cloud service providers may use trusted third parties, such as auditors and certifications, to ensure the integrity of their services[13].

Emerging technologies such as blockchain and homomorphic encryption have the potential to transform the future of cloud computing. Blockchain can provide an immutable ledger for data storage and processing, improving the security and transparency of cloud services. Homomorphic encryption allows for data processing without decrypting the data, improving the privacy and security of cloud services[14].

Insufficient battery life as a consequence of energy-intensive apps like video games, streaming audio and video, running sensors, etc. 2. Users are hesitant to switch their current data centres to this new paradigm due to a lack of established standards, lack of portability, lack of interoperability, restricted scalability, uncertain availability, and inability to install services over numerous Cloud computing service providers. Access management is the CC's obnoxious feature. This really is due to the fact that mobile nodes connect to the cloud via a variety of radio access technologies, including GPRS, WLAN, LTE, WiMAX, etc. Therefore, the most important necessity of CC is always-on and on-demand connectivity. 3. CC (Cloud Computing) cannot allow compute demanding programmes to function efficiently as compared to PC and server platforms due to the limited processor speed and memory limits. The literature review conducted and best practice documents related to the security, privacy, and trust building issues. They assessed topics such as encryption, access control, authentication, data leakage prevention and incident response protocols. Additionally, the authors identified the various challenge's organizations face when trying to ensure the security and trustworthiness of data stored and transmitted through cloud systems. This review provided a comprehensive overview of the current state of research in this area[15].

The literature review assessed the various access control mechanisms that can be used to protect data stored and transmitted in a cloud environment. The review looked at protocols such as AES, PKI and SAML, as well as data leakage prevention methods, authentication protocols, and threat detection solutions. The authors concluded that these mechanisms can be effective in protecting data from unauthorized access and disclosure, while also providing assurance of trustworthiness[16].

Table1. Research Questions and objectives

Q1, What data privacy initiatives are currently being implemented in cloud computing?	To research the ongoing data privacy initiatives in CC (Cloud Computing).
Q2, What are the current CC (Cloud Computing) data privacy threats and attacks?	To recognize the current challenges and risks to privacy in CC (Cloud Computing).
Q3, Which are the privacy measures suggested to support the security of personal data in cloud computing?	To determine the current methods employed in CC for protecting privacy and personal data (Cloud Computing).

3. Propose Methodology

The methodology for a research study on Privacy, Security, and Trust in Cloud Computing may include the following steps:
Identify research questions: Develop a set of research questions to guide the study. For example, "What are the main privacy concerns for cloud computing users?" "How can cloud computing providers ensure data security?" "What factors influence trust in cloud computing?"

Define research approach: Determine the research approach, such as a literature review, case study, survey, or experimental study. Choose the approach based on the research questions and available resources.

Conduct a literature review: Review relevant literature, including academic articles, reports, and industry publications, to understand the current state of research on privacy, security, and trust in cloud computing.

Select data collection methods: Determine the appropriate data collection methods for the study, such as surveys, interviews, or experiments. Choose methods that are appropriate for the research questions and research approach.

Collect data: Conduct data collection according to the selected methods. For example, if using surveys, develop a survey instrument and distribute it to a sample of cloud computing users or providers.

Analyze data: Analyze the collected data using appropriate statistical or qualitative analysis techniques. For example, use regression analysis to examine the relationship between trust and data security in cloud computing.

Draw conclusions: Draw conclusions based on the data analysis and literature review, and answer the research questions. For example, provide recommendations for how cloud computing providers can improve data security and user trust.

Write up results: Write up the results of the study in a report or paper, including an introduction, methodology, results, and conclusions. The report should also discuss any limitations of the study and potential areas for future research.

Researchers are very involved in exposing this emerging technology in a full-fledged mode since it is already in its infancy. Any of those problems, or research questions, have been discussed here, and maybe called potential research scopes for improving this grooming technology to live in a healthy and secure cloud world. The following table assists researchers in determining which level of cloud services these models have been suggested, in addition to discussing the problems and proposed solutions.

Any crypto-cloud system's entities are built on and derive from data. The most significant danger listed by CSA in Table 1 was data breach. It is crucial to understand the various degrees of security that the modern computer technology offers to the data that the author has in mind before continuing on to it, especially in

light of the sophistication of hacking techniques. Data leakage is a problem that arises when data is stored in a distant location (out of our control) and multi-tenancy is achieved. Data recovery is the process of retrieving damaged or corrupted data from storage media. When a file is deleted, just the metadata is lost; the actual data is still on the disk. By employing file carving, it may be restored. Bifragment gap carving, Smart Carving, and Carving memory dumps are some examples of frequently used carving systems. Data recovery is often hampered by OS failure, drive-level failure, and file deletion from a storage media. We must overcome these obstacles. Data loss occurs when data are updated frequently. It's necessary for data backup on an external server or in cloud storage. dealing with data loss Three copies of crucial files—one main and two backup copies. To protect against various threats, they retain the copies on 2 separate storage medium. Keep one duplicate off-site. Sensitive and non-sensitive information must be completely kept apart. Information must be separated from hrough the use of access control and encryption techniques, unauthorized users A user's identity may be used to provide fine-grained access control; some of these include attribute-based, time-based, etc. A unique kind of privacy is isolation. Carelessness in handling results in a VM to VM attack, compromising the users' privacy. The term "segregation of data" describes the complete separation of the Security problems result from replication maintenance. Here we divided the Multi-cloud Integration Framework and Inter-cloud Security Challenges into four major streams VM level, hypervisor level integration level and data level. The major area for paper collection is divided into four security challenges.

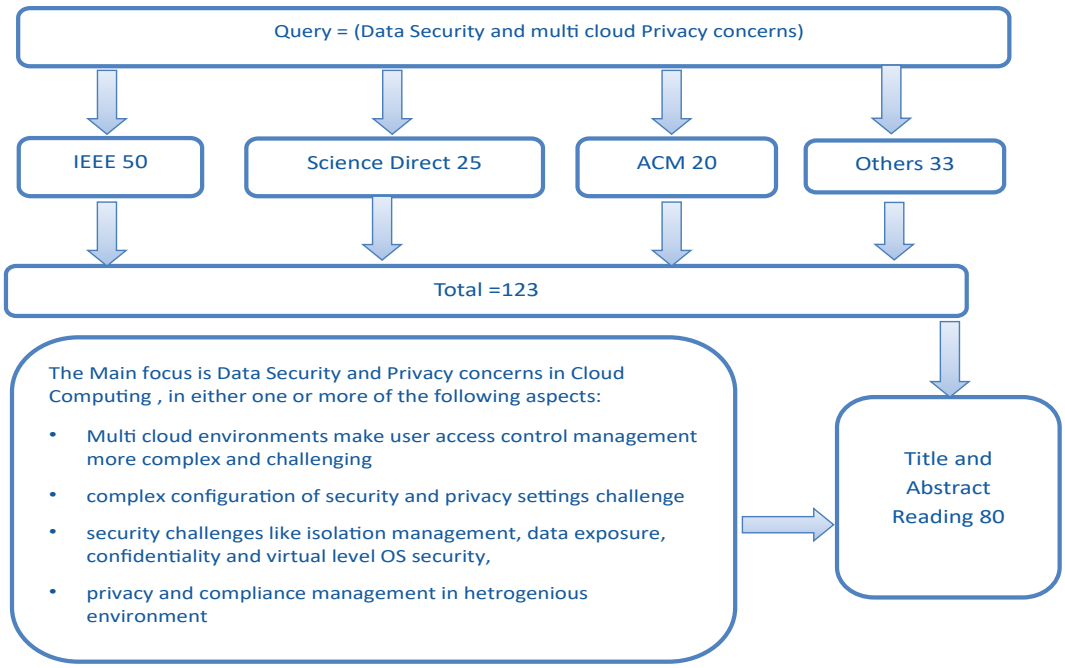

Figure 3: Proposed methodology of Data Security and multi cloud Privacy concerns

For the survey of the Multi-cloud Integration Framework and Inter-cloud Security total 123 paper is selected by dividing the into three major articles databases. The details of papers is reflected in Fig. 3.

Figure 4: Multi-Cloud Security Challenges

This paper examines current research on single and multi-cloud security as well as potential fixes. It is discovered that the usage of single clouds has garnered more attention from the research community than the use of multi-cloud providers for maintaining security. This research intends to encourage the usage of several clouds since it may lower security concerns that impact cloud computing users.
Developing more comprehensive and unified security and privacy frameworks: With the increasing complexity and heterogeneity of cloud computing systems, it is important to develop more comprehensive and unified security and privacy frameworks that can effectively address the various security and privacy challenges.

Advancing data protection technologies: With the growing amount of sensitive data stored and processed in the cloud, more advanced data protection technologies, such as encryption, access control, and data anonymization, need to be developed and optimized to enhance the data security and privacy.

Enhancing trust models: Trust is a critical factor in the adoption and success of cloud computing. Future research should focus on enhancing trust models by incorporating more sophisticated trust metrics, such as reputation, history, and social networks, to provide more accurate and dynamic trust evaluation.

Addressing emerging security and privacy threats: As cloud computing evolves, new security and privacy threats emerge, such as cloud-specific attacks, side-channel attacks, and privacy breaches through social media. Future work should focus on identifying and addressing these emerging threats to enhance the overall security and privacy of cloud computing.

Incorporating privacy by design: Privacy by design is a concept that emphasizes embedding privacy and data protection into the design and development of cloud systems, rather than addressing them as an afterthought. Future research should focus on incorporating privacy by design principles into the development of cloud computing systems to improve privacy and security by default.

4. Conclusion

This paper has presented an in-depth review of Privacy security and trust building issues in cloud computing. It discussed the challenges posed by cloud computing, including the need to protect data from unauthorized access and disclosure, as well as verifying the identity of users. The paper also presented a proposed methodology for these security and privacy concerns and an algorithm for implementing this methodology. Finally, the literature review and simulation results highlighted the importance of taking measures to ensure security, privacy and trustworthiness of data stored and transmitted through cloud systems. This is essential for protecting organizations against the threat of malicious actors and ensuring compliance with relevant privacy laws and regulations.

5. References:

[1] M. I. Sarwar, Q. Abbas, T. Alyas, A. Alzahrani, T. Alghamdi, and Y. Alsaawy, "Digital Transformation of Public Sector Governance With IT Service Management–A Pilot Study," IEEE Access, vol. 11, no. January, pp. 6490–6512, 2023.

[2] T. Alyas, "Performance Framework for Virtual Machine Migration in Cloud Computing," Comput. Mater. Contin., vol. 74, no. 3, pp. 6289–6305, 2023.

[3] M. Niazi, S. Abbas, A. Soliman, T. Alyas, S. Asif, and T. Faiz, "Vertical Pod Autoscaling in Kubernetes for Elastic Container Collaborative Framework," 2023.

[4] T. Alyas, A. Alzahrani, Y. Alsaawy, K. Alissa, Q. Abbas, and N. Tabassum, "Query Optimization Framework for Graph Database in Cloud Dew Environment," 2023.

[5] W. U. H. Abidi, "Real-Time Shill Bidding Fraud Detection Empowered with Fussed Machine Learning," IEEE Access, vol. 9, pp. 113612–113621, 2021.

[6] D. Baig, "Bit Rate Reduction in Cloud Gaming Using Object Detection Technique," 2021.

[7] G. Ahmad, "Intelligent ammunition detection and classification system using convolutional neural network," Comput. Mater. Contin., vol. 67, no. 2, pp. 2585–2600, 2021.

[8] S. Malik, N. Tabassum, M. Saleem, T. Alyas, M. Hamid, and U. Farooq, "Cloud-IoT Integration: Cloud Service Framework for M2M Communication," Intell. Autom. Soft Comput., vol. 31, no. 1, pp. 471–480, 2022.

[9] A. Alzahrani, T. Alyas, K. Alissa, Q. Abbas, Y. Alsaawy, and N. Tabassum, "Hybrid Approach for Improving the Performance of Data Reliability in Cloud Storage Management," Sensors (Basel)., vol. 22, no. 16, 2022.

[10] N. Tabassum, "Semantic Analysis of Urdu English Tweets Empowered by Machine Learning," 2021.

[11] A. Amin, "TOP-Rank: A Novel Unsupervised Approach for Topic Prediction Using Keyphrase Extraction for Urdu Documents," IEEE Access, vol. 8, pp. 212675–212686, 2020.

[12] S. Abbas, M. A. Khan, A. Athar, S. A. Shan, A. Saeed, and T. Alyas, "Enabling Smart City With Intelligent Congestion Control Using Hops With a Hybrid Computational Approach," Comput. J., vol. 00, no. 00, 2020.

[13] M. Asadullah, M. A. Khan, S. Abbas, T. Alyas, M. A. Saleem, and A. Fatima, "Blind channel and data estimation using fuzzy logic empowered cognitive and social information-based particle swarm optimization (PSO)," Int. J. Comput. Intell. Syst., vol. 13, no. 1, pp. 400–408, 2020.

[14] A. Nasir, T. Alyas, M. Asif, and M. N. Akhtar, "Reliability Management Framework and Recommender System for Hyper-converged Infrastructured Data Centers," 2020 3rd Int. Conf. Comput. Math. Eng. Technol. Idea to Innov. Build. Knowl. Econ. iCoMET 2020, no. Dc, 2020.

[15] U. Tariq, Haroon-Ur-Rashid, A. Nadeem, M. Khan, S. Saqib, and T. Alyas, "Urdu Handwritten Signature Recognition Empowered with PNN," vol. 19, no. 12, p. 132, 2019.

[16] T. Alyas, K. Ateeq, M. Alqahtani, S. Kukunuru, N. Tabassum, and R. Kamran, "Security Analysis for Virtual Machine Allocation in Cloud Computing," Int. Conf. Cyber Resilience, ICCR 2022, no. Vm, 2022.

Editorial Policy and Guidelines for Authors

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

The following note set out some general editorial principles. 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 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