Grenze International Journal of Engineering and Technology, January Issue

Security Analysis of Cloud Attacks using Conventional Cryptographic Techniques, A Case Study based on CloudSim Tool

Siya Garg[1], Vinita Jindal[2] and Rahul Johari[3]
[1]Department of Computer Science, University of Delhi, North Campus, New Delhi, 110007, Delhi, India.
E-mail: gargsiya90@gmail.com
[2]Department of Computer Science, Keshav Mahavidyalaya, University of Delhi, New Delhi, 110034, Delhi, India.
E-mail: vjindal@keshav.du.ac.in
[3]University School of Automation and Robotics (USAR), Guru Gobind Singh Indraprastha University, East Delhi Campus, New Delhi, 110032, Delhi, India
E-mail: rahul@ipu.ac.in

***Abstract*— In the age of cloud computing, where every second application is storing its data online, cloud security becomes critical. After examining previous security breaches and various cloud-based attacks, the authors conclude that in order to provide 360-degree protection, cloud security must be viewed from different angles, including data, end users, and infrastructure. In an attempt to safeguard users' needs for virtual machine resources, the authors of this study built on a customer resource allocation framework [CRACLE [1]], which allowed users to select cloud resources according to their different needs. This extension gives users an opportunity to choose resources while also securing their data using three different encryption techniques, protecting them from snooping attacks and safeguarding their requirements.**

***Index terms*—Cloud Computing, Attacks, Cryptography, Encryption, CloudSim.**

I. INTRODUCTION

In 1961, John MacCharty delivered his speech at MIT that "Computing Can be sold as a Utility, like Water and Electricity [2], which was later implemented by Salesforce.com in 1999. The term "cloud computing" refers to accessing, storing, and provisioning of computing-related services over the Internet. This technology can be used on a pay-per-use basis and operates just like any other utility. Despite being a game-changer, this technology has seen several setbacks because of built-in security flaws and several previous cloud-based attacks. The frequency with which these attacks can render an application entirely ineffective is growing daily, as is their cardinality. Any application, whether on a physical device or in a cloud ecosystem, becomes vulnerable as soon as it is made available to the public. It becomes essential that we consider cloud security from both the infrastructure and user perspectives when discussing cloud computing. The infrastructure can be kept safe and orderly by the cloud providers. Still, misconfiguration and ignorance on the part of the cloud user could result in malware insertion and other such attacks. Thus, cloud security ought to be viewed as an expanded approach that concentrates on edge devices that consumers directly access in addition to infrastructure. To devise any strategy to mitigate these vulnerabilities, one needs to first understand what constitutes a cloud attack.

Grenze ID: 01.GIJET.11.1.506_1

A cloud attack is a type of cyberattack that target cloud services like storage, computing, networking, etc. that are hosted in one of the following modes: Platform as a service (PaaS), Software as a service (SaaS), or Infrastructure as a service (IaaS). To understand the impact of these cloud attacks, a few of them have been discussed at length in the following section

A. A Popular Cloud Attacks

Denial-of-Service Attacks - A denial-of-service (DoS) attack includes flooding a cloud service with a lot of traffic, which can overwhelm the system and prevent it from handling valid requests. DoS attacks can have negative effects that are detrimental to an organization's reputation, the availability of essential services, and financial loss. The scale and complexity of cloud infrastructures can make it difficult to detect and neutralize cloud-based DoS attacks, making them particularly difficult to defend against.

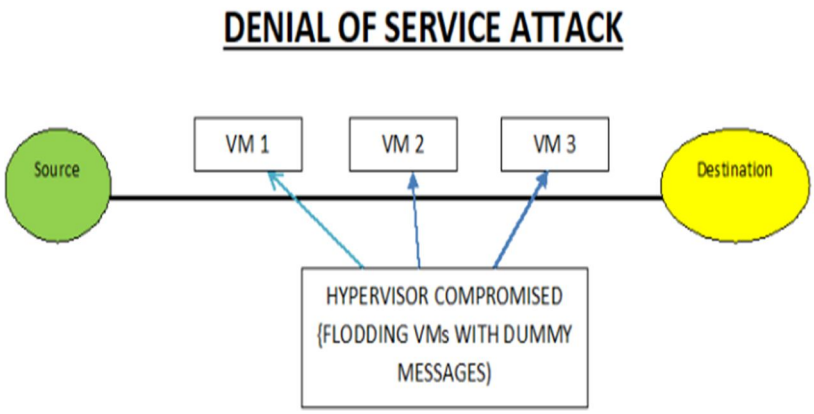

Figure1. Denial of service

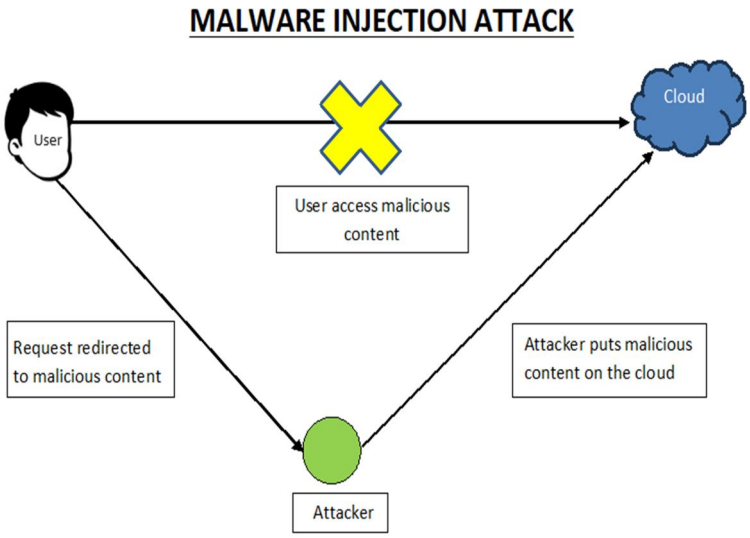

Figure. 2 Malware Injection Attack

B. Types of DoS –

Distributed Denial of Service (DDoS) - These assaults typically affect the entire neighborhood in a public cloud. It can result in attackers accessing cloud computing resources for illegal operations by changing cloud computing behaviors if it is left uncontrolled or neglected for a while.

Hypervisor DoS - attacks using hypervisor vulnerabilities are becoming relatively common these days. A hypervisor cyberattacker targets the hypervisor space, which it uses to manage several virtual machines on a single virtual host. After the hypervisor becomes infected, the Dos malware can harm any VM running on the host.A rootkit that has been installed on a virtual machine (VM) is used by the attacker to attack and take over the hypervisor. This is often called Hyperjacking.

Permanent denial-of-service (PDoS) - Plashing, also known as permanent denial-of-service (PDoS), is a rapid assault intended to take down the target and prevent it from offering services
Economic denial of sustainability (EDoS) - Attacks that exploit cloud computing's resource utilization, aiming to impact the CSP(Cloud Service Provider) financial bottom line (e.g., to increase the bill), but not its physical network or server resources[3]. It forces CSP to keep increasing its resource utilization to fulfill the Service-Level Agreement (SLA) of its clients to the point it is economically non-viable or unable to sustain further demand for services.
Cloud Malware Injection Attacks - These attacks include inserting malicious software, such as viruses or ransomware, into a cloud infrastructure. As a result, the attacker may be able to compromise the resources in question, steal data, or utilise the resources for their benefit. Attackers can introduce malware into cloud resources in several ways, such as by taking advantage of weaknesses in the cloud infrastructure, adding a malicious service module to a SaaS or PaaS system, or adding an infected VM to an IaaS system and redirecting user traffic there or by taking advantage of a flaw in a system.
Security Misconfiguration - When resources and infrastructure are not correctly configured to guard against online threats, it is referred to as security misconfiguration. This can involve improperly configuring access controls, improperly securing systems and applications, and improperly maintaining and patching systems and applications.
Exploiting Live Migration - A virtual machine or application can move between various physical devices through a process known as live migration without losing connectivity with the application or the client. While live migration is practical, it is a risky process because cloud malware can target it. Attackers can enter an automatic live migration and infiltrate its cloud management system.

II. Literature Survey

Authors in [1] presented a review of known data security issues, covering everything from DNS and sniffer attacks to unauthorized access, data lock-in, and SQL injection. They also went into detail about four different Man in the Middle (MiMA) attacks, starting with Wrapping Attack (1), in which an attacker attempts to copy the user's credentials by using SOAP messages, Flooding Attack (2), in which a constant stream of requests is passed through the servers, making it difficult for the employee to concentrate resulting in system failure. Internet attack (3) - This addresses data theft that occurs when SOAP messages are encrypted and SSL(4)(Secure Socket Layer) Attack- This defense mechanism is positioned between the user and the server where an attacker can simply steal information. The authors of [5] conducted a review of the methods that are frequently used to create cybersecurity systems with the goal of reducing potential security attacks. The comparison helped to establish that there is always a need for new artificial intelligence and machine learning systems that can profile many known and undiscovered assaults, detect them, and stop them with high performance. Payment for cloud services is based on usage charges. This functionality led to the development of a new sort of DDoS attack known as EDoS, in which the victim of the attack is required to pay an additional price to the cloud provider. The authors of [6] evaluated a better EDoS attack detection and mitigation system based on SVM, KNN, RF trees, and DL, among other machine learning methods. They provided two EDoS detection scenarios: multi-classification, which includes nine attack classes, and binary classification, which includes normal and attack classes. On binary classification, RF trees showed the best performance at detecting DDoS attacks, whilst SVM methods were the best on multi-classification datasets. The authors of [7] went into great length about the factors influencing cloud security. Among these are: 1. Virtualization, which carries security flaws originating from the underlying technology 2. Multi-tenancy and isolation, which necessitates a strategy from the SaaS layer through infrastructure facilities; 3. Security management is essential in overseeing and controlling a multitude of requirements and limitations. A system consisting of data fragmentation and dual encryption approaches was presented by the authors of [8] to visualize secure information dissemination in a multi-cloud context. There has been discussion of the several issues surrounding this field, including challenges with integrity, security, confidentiality, and authentication. To mitigate the difficulties of imposing information security protection in the cloud, a secure computing protocol and an HBDaSeC prototype were employed. Additionally, they demonstrated a two-tier architecture—one on the client side and another on the server side—for security in a multi- cloud platform. The vital problem of vendor lock-in connected to a single cloud platform is eliminated when data is stored on a multi-cloud platform. In [9], the authors presented a novel SDMTA (Scattered Denial-of-service Mitigation Tree Architecture) that can solve the data shift issue and provide reliable DDoS attack detection and mitigation in a hybrid cloud. The architecture uses the IP address as the base in the attacker database to generate

a log as soon as it detects one. All potential correlations between access trace log patterns and the corresponding system activity are found using the special SDMT technique. A survey of the several homomorphic cryptography algorithms utilized in cloud computing was offered by the authors of [10]. Transforming highly sensitive data from its original format into one that cannot be read is the best method to safeguard it, and homomorphic encryption (HE) makes this feasible. It exists in three distinct forms: fully HE (FHE), somewhat HE (SWHE), and partial HE (PHE). Following a thorough analysis, the authors concluded that FHE can give the cloud complete security.

III. METHODOLOGY ADOPTED

- The user is first asked to specify what cloud resources they require.
- Accepted user requirements are concatenated into a String.
- String input is used as plain text for the encryption.
- The user can encrypt their text using one of three available techniques-Caesar, Affine, and Rail Fence.
- After the user selects the technique, encryption begins to safeguard user credentials and mitigate eavesdropping attacks.
- User requirements are archived in the database and the process stops.

A. Algorithm

- U inputs VMR
- Vi (VMM, VMID, MIPS, SIZE, RAM, BW, PES) is created
- PT=VMM+VMID+MIPS+SIZE+RAM+BW+PES
- U selects ET from CC, AC, and RFC
- N=0
  LOOP : do { (N)
  {
  case 1: CAESAR(PT,3) //User opts for Caesar cipher for encryption break LOOP
  case 2: AFFINE(PT.toCharArray()) //User opts for Affine cipher for encryption break LOOP
  case 3: KEY-Accept key for encryption
  RAILFENCE(PT,KEY) //User opts for Rail fence for encryption break LOOP
  default: if N!=1 || N!=2 ||N!=3 CHOOSE AGAIN
  } while N!=1 || N!=2 ||N!=3
- CAESAR(text, s)
  {
  for i=0 to text.length
  if Character.isUpperCase() OR Character.isLowerCase()
  UPDATE: ch%26
  if Character.isDigit()
  UPDATE: ch % 10
  res=res+ch return res }
- AFFINE (char[] msg)
  {
  for i=0 to i<msg.length
  if Character.isUpperCase() OR Character.isLowerCase()
  UPDATE: cipher%26
  else if (Character.isDigit()
  UPDATE: cipher % 10 else
  cipher += msg[i] return cipher }
- RAILFENCE(text, key)
  {
  char[][] rail = new char[key][text.length()] for i=0 to i<key
  Arrays.fill(rail[i], '\n') for i=0 to text.length
  if row == 0 || row == key - 1
  dirDown = !dirDown rail[row][col++] = text.charAt(i) for i=0 to i<key
  for j=0 to j<text.length if rail[i][j] != '\n'
  result.append(rail[i][j]); return result }

- Vi added to <VL>
- Submit <VL> to B
- U inputs CR
- CL (ID, LEN, FSIZE, OSIZE) is created
- CL added to <CL>
- CL submitted to B
- Simulation begins
- UC secured
- UC archived into DB

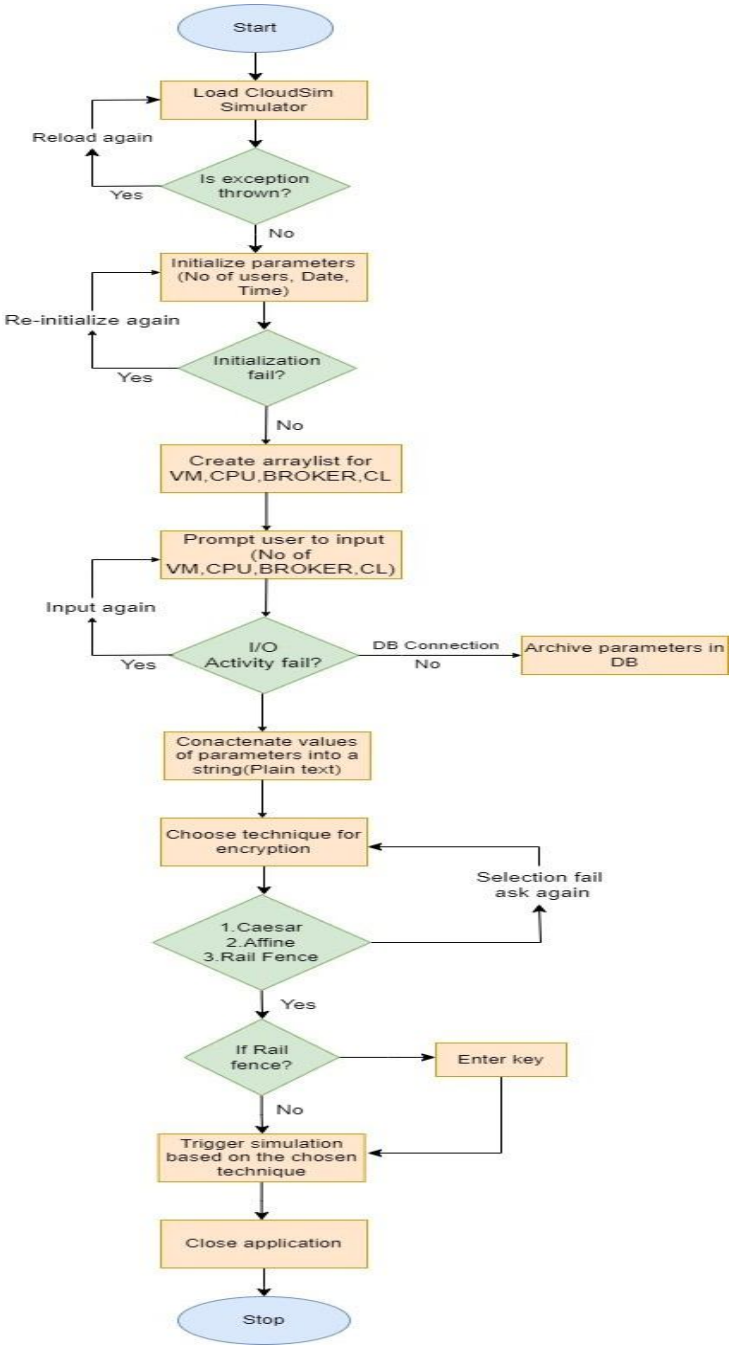

Figure.3 Flowchart of the proposed work

IV. RESULTS

The user was requested to input his resource demand. After accepting the user requirements, To serve as plain text for the selected encryption method, values of the input parameters were concatenated into a string. The broker received the encrypted values in order to create the virtual machine. After the data center established the virtual machine (VM), CL was transferred to it. In the CRACLE framework, every CL was completed successfully. The Java code for user input-driven CloudSim tool-based simulation has been showcased in Figures 4-7. A comparative analysis of different encryption techniques based on three different parameters has been showcased in Fig. 8.

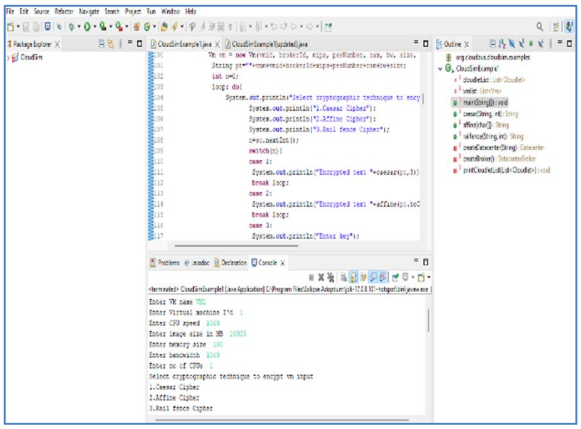

Figure. 4 Simulation Snapshot of CloudSim Tool

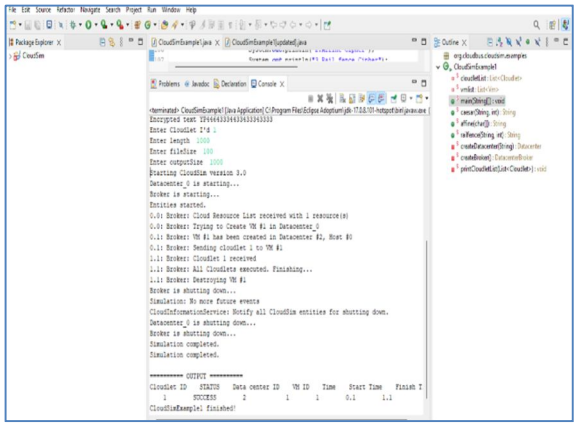

Figure 5 Caesar Cipher

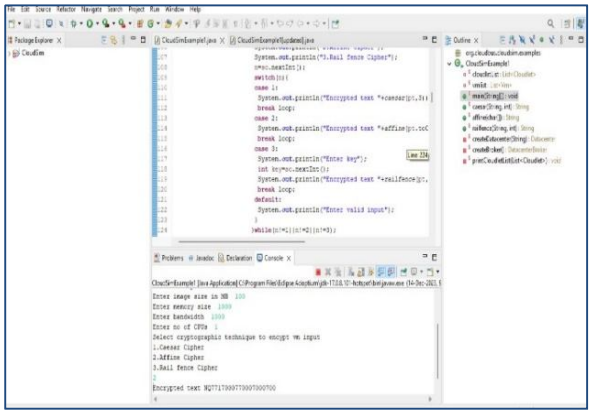

Figure. 6 Affine Cipher

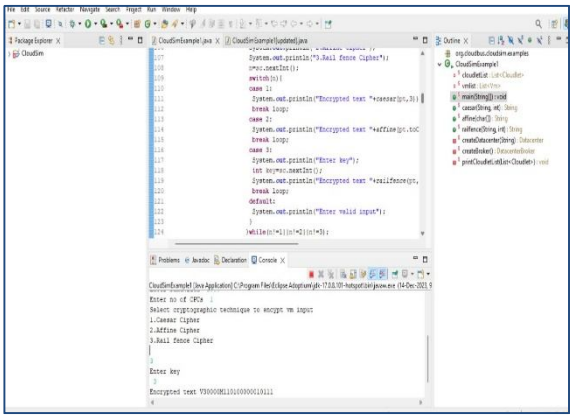

Figure. 7 Rail Fence Cipher

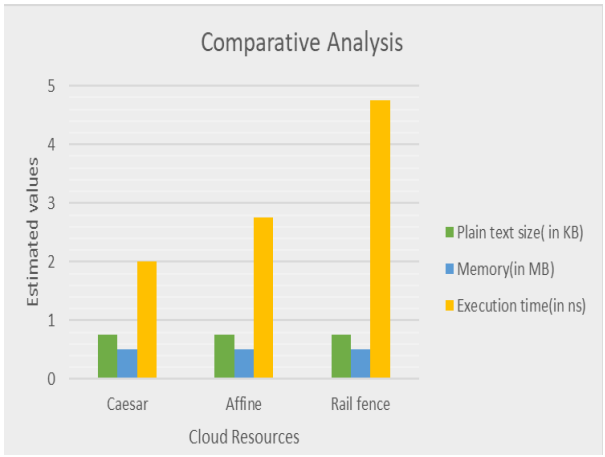

Figure. 8 Comparative Analysis

V. Conclusions

The sharing model that underpins cloud computing allows resources to be quickly made available to customers based on their needs. The accepted user requirements were translated into plain text and used as input for the user-selected encryption technique in an effort to secure the user credentials and protect them from snooping attacks. The experiment outlined in the paper demonstrates how the user credentials have been protected from malicious users and effectively archived in the database.

Declarations

Availability of data and materials- No explicit data sets or material were used in this paper.
Competing Interest- The Author(s) have no competing interest and no disclosures to make.
Funding- There is no funding agency involved.

Acknowledgment

The author(s) would like to thank the administration of the University of Delhi for providing a research-oriented academic environment.

Appendix A-Abbreviations

Table I

S.No.	Abbreviations	Full Form
1	U	User
2	VMR	Virtual Machine Requirement: VMM-Virtual machine name VMID-Virtual Machine I'd MIPS-CPU Speed SIZE-Image Size RAM-Memory Size BW-Bandwidth PES-No. of CPUs
3	CR	Cloudlet Requirements: ID-Cloudlet I'd LEN-Length FSIZE-File Size OSIZE-Output Size
4	Vi	VM Instance
5	VL	VM array list
6	CL	Cloudlet Instance
7	CL	Cloudlet array list
8	B	Broker
9	PT	String with concatenated VMR
10	ET	Encryption Technique
11	ET	Encrypted Text
12	CC	Caesar Cipher
13	AC	Affine Cipher
14	RFC	Rail Fence Cipher
15	UC	User credentials
16	DB	Database

References

[1] Garg, Siya, Rahul Johari, Vinita Jindal, and Deo Prakash Vidyarthi. "CRACLE: Customer Resource Allocation in CLoud Environment." Proceedings of Data Analytics and Management (2022): 621.
[2] https://www.geeksforgeeks.org/history-of-cloud-computing/;.
[3] Alashhab, Ziyad R., Mohammed Anbar, Manmeet Mahinderjit Singh, Iznan H. Hasbullah, Prateek Jain, and Taief Alaa Al-Amiedy. "Distributed denial of service attacks against cloud computing environment: survey, issues, challenges and coherent taxonomy." Applied Sciences 12, no. 23 (2022): 12441.
[4] Kaja, Durga Venkata Sowmya, Yasmin Fatima, and Akalanka B. Mailewa. "Data integrity attacks in cloud computing: A review of identifying and protecting techniques." J. homepage www. ijrpr. com ISSN 2582 (2022): 7421.
[5] Eddermoug, N., Mansour, A., Azmi, M., Sadik, M., Sabir, E., & Bahassi, H. (2023). A literature review on attacks prevention and profiling in cloud computing. Procedia Computer Science, 220, 970-977.

[6] Aldhyani, Theyazn HH, and Hasan Alkahtani. "Artificial intelligence algorithm-based economic denial of sustainability attack detection systems: Cloud computing environments." Sensors 22, no. 13 (2022): 4685.
[7] Maheshwari, Vanshika, Subrata Sahana, Sanjoy Das, Indrani Das, and Ankush Ghosh. "Factors influencing security issues in cloud computing." In International conference on advanced communication and intelligent systems, pp. 348-358. Cham: Springer Nature Switzerland, 2022.
[8] Seth, Bijeta, Surjeet Dalal, Vivek Jaglan, Dac-Nhuong Le, Senthilkumar Mohan, and Gautam Srivastava. "Integrating encryption techniques for secure data storage in the cloud." Transactions on Emerging Telecommunications Technologies 33, no. 4 (2022): e4108.
[9] Kautish, Sandeep, A. Reyana, and Ankit Vidyarthi. "SDMTA: Attack detection and mitigation mechanism for DDoS vulnerabilities in hybrid cloud environment." IEEE Transactions on Industrial Informatics 18, no. 9 (2022): 6455-6463.
[10] Mahato, Ganesh Kumar, and Swarnendu Kumar Chakraborty. "A comparative review on homomorphic encryption for cloud security." IETE Journal of Research 69, no. 8 (2023): 5124-5133.