Modeling Cloud-Oriented Cryptographic Techniques inCloudSim for Comparative Analysis

Amit Kumar Singh Sanger Sanger

amitsanger.cse@gmail.com

Guru Gobind Singh Indraprastha University

Rahul Johari Johari

Guru Gobind Singh Indraprastha University

Research Article

Keywords: Cloud Computing, CloudSim, Symmetric key, Encryption, Decryption

Posted Date: February 21st, 2024

DOI: https://doi.org/10.21203/rs.3.rs-3958900/v1

Additional Declarations: No competing interests reported.

Modeling Cloud-Oriented Cryptographic Techniques in CloudSim for Comparative Analysis

Amit Kumar Singh Sanger[1,2*] and Rahul Johari[1]

[1*]SWINGER : Security, Wireless, IoT Network Group of Engineering and Research, USICT, GGSIP University, Sector-16C, Dwarka , Delhi, 110078, India.
[2]KIET Group of Institutions , Delhi-NCR, Ghaziabad-Meerut Road, Ghaziabad, 201206, Uttar Pradesh, India.

*Corresponding author(s). E-mail(s): amitsanger.cse@gmail.com, amit.18416490020@ipu.ac.in;
Contributing authors: rahul@ipu.ac.in;

Abstract

Cloud technology is essential for modern businesses, revolutionizing IT by overcoming traditional data processing limitations. However, security concerns, especially with increasing cloud attacks, pose a significant challenge to the potential benefits of cloud computing. This article explores the fundamentals and models of Cloud Computing, shedding light on the critical issue of security in this evolving landscape. This study examines the usage of CloudSim, a cost-free and open-source programme, for the purpose of simulating and comparing secure cryptographic encryption methods. We propose two novel methodologies: Geometrical Cryptography Technique (GCT) and Circular Cryptographic Technique (CCT). Both methodologies are simulated and executed using CloudSim, enabling a regulated and repeatable comparison across different performance measures. We assess both strategies by considering criteria such as code length, space complexity, and time complexity. The findings indicate positive results for both GCT and CCT, presenting encouraging possibilities for further investigation and advancement in secure communication systems based on cloud computing. This study complements to the current discussion about strengthening security measures in cloud computing settings, providing significant insights on the viability and efficacy of various cryptographic methods for protecting the transmission of resource allocation requests.

Keywords: Cloud Computing, CloudSim, Symmetric key, Encryption, Decryption

1 Introduction

According to the "National Institute of Standards and Technology (NIST)" definition of Cloud Computing, *"Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"*[1].
The term "cloud computing" makes reference to a field of information technology that focuses on providing customers with online access to a variety of IT services, including servers, virtual machines (VMs), databases, memory, and software, as needed. In addition to enabling customers to store, evaluate, and publish massive databases and repositories over the data center, cloud technology has revolutionized the way that processing is done by lowering the computational burden of establishing information systems

and by enabling the architecture, advancement, and implementation of stable apps over the network. Pay-as-you-go policies allow anyone, regardless of the size or nature of the company, to easily obtain cloud resources. Corporate computers necessitated the building of their individual server rooms with substantial storage devices, electrical wiring, backup machines, and knowledgeable personnel before the emergence of this approach. Owing to the increased initial cost for information technology systems, poor CPU usage during periods of low demand and high recovery costs indicate inefficient management. Client requests for resources might be inconsistent, spiky, and uncertain, depending on the circumstances. The requirement to transition to cloud computing is driven by a combination of factors, including network costs, compatibility constraints, and reliability difficulties. As a result, businesses are utilizing cloud capabilities to reduce expenses and effort.

There are several security issues with cloud technology that must be considered. The security issue emerges as a result of the customer's loss of control of the data, which is now within the region of the cloud provider. The cloud customers, who may be the legitimate owner of the underlying data or service, are entirely reliant on their CSPs to protect the confidentiality of their data. The principle of mutual consent is established to a certain degree by agreeing on the SLA, however, a lot of cloud-related security problems arise that must be addressed by the CSP or customer. Regardless of the architecture employed, data security is a very crucial aspect of IT cybersecurity. Cloud technology is everywhere; in fact, due to its decentralized structure and multi-tenant design, it emphasizes additional security considerations. The data life cycle encompasses the creation, archiving, utilization, dissemination, and disposal. Every CSP should provide suitable security features for all stages of the life cycle of data [2]. For instance, if the software service is not developed appropriately, a customer may be able to employ a SQL injection [3] to achieve unauthorized exposure to the data of some other client, erase it, or otherwise alter it. To avoid this, adequate security mechanisms must be put in place. The phenomena of data eradication are again fairly critical in the cloud and must be managed properly by the CSP to guarantee the irreversible and total collapse of data at the demand of a customer. Furthermore, the storage devices utilized to prevent information leakage should be visible and traceable for consumers. All of those difficulties, as well as many others, must be addressed when employing a cloud service.

Virtualization is also significant in cloud technology because it provides the necessary level of personalization, security, separation, and availability for offering IT resources on-demand. The notion of virtual machines underpins IaaS, whilst software-level virtualization adds to PaaS solutions. Through virtualization introduces the notion of Cloud Computing, which allows a variety of software or offerings to share the infrastructure of a specific hardware server at the same without disrupting or even disclosing it to the customer programs. Thus, it is evident that VMs build the complete back-end for Cloud-based resources. In addition, it poses specific risks to the Cloud. It allows for a novel and unpredictable type of spoofing. The potential to entirely transparently emulate a host may allow malware to collect confidential data from the customer. Furthermore, the notions of Virtualization Image [4] and Online Deployment are both beneficial to customers while also introducing security weaknesses that must be addressed by CSP. As a result, when reliability in the cloud is taken into account, it shouldn't be limited to just protecting sensitive data and should also take into account the protection of the related virtual machines (VMs).

For simplicity and ease, the article continues as follows: Section 1.1 outlines the features of cloud technology, Subsection 1.2 exemplifies Cloud Computing Architecture, Subsection 1.3 presents Cloud Services and Applications offered by the cloud, and forthcoming issues are described in Section 1.4, Section 2 introduces the statement of the research problem, Section 3 introduces the literature survey, Section 4 describes security concerns and attacks, Section 5 describes basics of cryptography, Section 6 describes the methodology adopted, Section 7 describes algorithm formulation, Section 8 describes results, Section 9 describes the summary of the study, Section 10 describes acknowledgment accompanied by the conflict of interest and references section.

1.1 Features of Cloud Technology

Cloud Technology offers following features:

- **Multitenancy**: Many single instances of the computing resources provided by a cloud vendor can be shared by different users at the same time as per their usage assuring the security. It can be understood as resource pooling and is very common in public cloud.

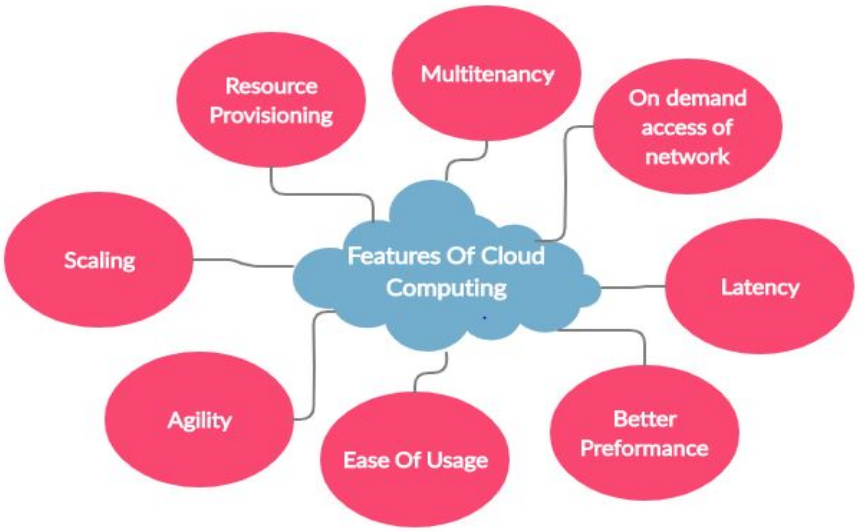


Fig. 1: Features of Cloud Computing

- **Resource Provisioning**: The resources/ services, including data centers, VMs, servers, and apps under different levels of services, are provided to the user for which they would be charged as per their usage.
- **Scalability**: The cloud vendors assure the scalability of the cloud services with varying demands of the requests by the end users by load balancing. The client can easily access the resources without having knowledge of the server location being used to serve the particular request.
- **Latency**: The time period between requesting for the service and the retrieval of response from the datacenters is called the latency and is reduced.
- **Agility**: To drive the business growth, the cloud vendors offer platforms to easily develop, deploy and test the application.
- **Ease of Usage**: The Graphical User Interface (GUI) Offered by cloud service providers makes the service easy to be accessed by anyone.
- **On demand access of Network**: The services can be accessed anytime by the clients and the enterprise as the datacenters are maintained 24*7 by the cloud providers.
- **Better performance**: Performance is improvised by the load balancing, and resource partitioning.

1.2 Cloud Computing Infrastructure

The service model and deployment model are the two different sorts of paradigms used in the cloud. Three types of services are included in the service delivery model:

- **Software as a Service (SaaS)**: The end customers are the major target audience for this offering. Customers do not have to install the additional application on their local computers in order to use the cloud provider's service. As a result, SaaS is accessible from any sort of device and offers clients limited usage. Enterprise applications, content management, messaging services, and social networking applications are among the four categories of services that make up SaaS.
- **Platform as a Service (PaaS)**: Platform as a Service is primarily developer-focused and can be thought of as an alliance between SaaS and IaaS. For users to create, implement, and evaluate enterprise applications, cloud providers sell run-time environments and database resources. The two main providers of PaaS platforms are Google App Engine and salesforce.org. The two services that can be used and altered according to demand by software developers employing the service are apps and information. Vendor Lock is a potential problem because it forces programmers to use just their proprietary platforms and preferred coding languages when creating applications.

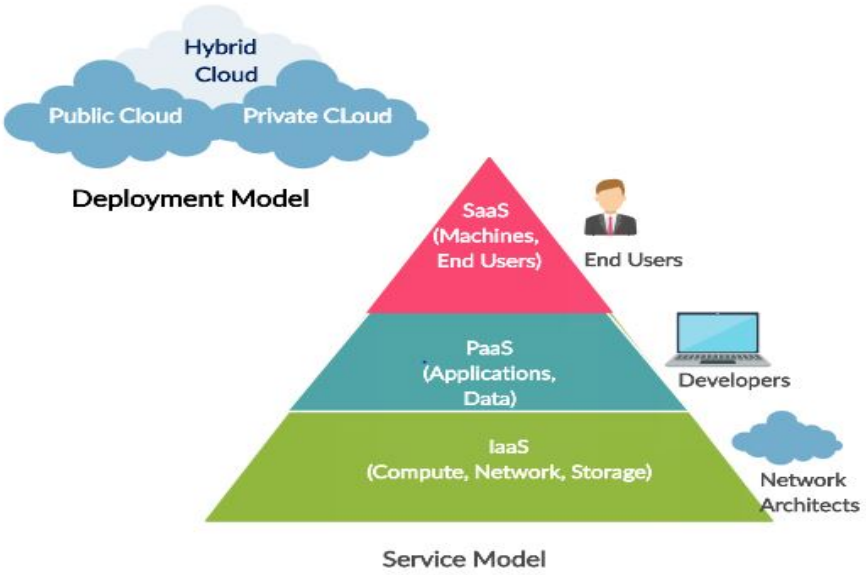


Fig. 2: The two models of Cloud Computing

- **Infrastructure as a Service (IaaS)**: With the help of this offering, customers can use networking, server, database servers, VMs, and load optimizers for computing, memory, and computing. The client is billed in accordance with consumption. Large companies like Amazon Web Services (AWS), Google Cloud, and Windows Azure are the primary providers of these technologies.

1.3 Deployment models

When classifying models, deployment models generally take into account usage accessibility and proprietary rights. Three deployment models are typically employed. Only allowed personnel of a specific organization can access a private cloud. Consumers are contained and restrained inside specific organizational boundaries.
All users have accessibility to public clouds, which are not just available to businesses. Although such clouds are quite expensive, they offer less protection and upkeep. The advantages of the private and public cloud offerings are combined in hybrid clouds. The key to properly understanding cloud technology is virtualization. The technology of virtualization enables the supply of various cloud services over a given piece of hardware, acting as the host VM and sponsoring numerous guest systems. Virtualization can take the form of application, OS, host, or hypervisors, as well as infrastructure virtualization. Cloud technology is a consequence of fusing the ideas of virtualization and multitenancy.

1.4 Cloud Services and Applications

There are various big firms investing at the Cloud development in public, private as well as hybrid domain. With a wide range of services offered, these organizations have been the leading masters in the revolution of Cloud Computing. The enterprises are now shifting their focus from traditional ways of hosting softwares to avail the on demand cloud services. The ventures not only include the software development including machine learning (ML), big data analytics, the Internet of Things (IoT), Artificial Intelligence, Quantum technologies and blockchain.
Some of these services which have added to the major impact are:

Google App Engine (GAE) by Google was launched in 2008 as a PaaS service with the motive to support the development and deployment of business applications using Java, Python or Go as the programming languages. Google provides the compatibility to use the same single Google account to access the services. Sandbox isolates the applications from the operating system to provide security. It is supported by other Google services such as Google Cloud, Google Cloud Storage, and GAE Datastore.

Fig. 3: Pizza as Service Analogy example to understand Cloud Service Model

It is used by the developers to build games and mobile applications too. Various enterprises are using this service for their products such as 'BugSense' which maintains the logs of the bugs encountered in software and analyze them; and 'Claritics' for the game analysis [5].

Amazon Web Services (AWS) which was established by Amazon in 2006 offers more than 150 cloud services support to both product and service based enterprises at all the levels. It has AWS Instance store which is block storage, AWS S3 bucket storage which is an object store. For deployment of applications, it uses AWS Elastic BeanStalk supported by AWS CloudWatch, Amazon S3 bucket, Instance Security Group, EC2 instances (for compute). Further, many services and products are provided and the cloud providers use multitenancy and automate scaling process through their tools. Load balancers are used for multiple instances support and primitive settings can be controlled by developers [6].

International Business Machines Corporation (IBM) has its own **IBM Cloud** around 170 cloud services with footprint in all private, public and hybrid domains. IBM has been working on virtualization projects since 1990 and came up with its own cloud for business enterprises in 2007. Initially, IBM was specifically for big enterprises and offered private and hybrid cloud but in 2020, it has announced to supply public cloud services too [7].

1.5 Challenges

Cloud Computing offers several advantages to change the era of computing but at the same time, has some challenging aspects too. The challenges offered are:

- **Security**: Cloud vendors ensure the data security through their own software and algorithms but the enterprises are not given any details about the location of their data in the datacenters which can be a risk to the security of data.
- **Continuous Connectivity**: Internet connection is required every time one needs to access or compute anything using cloud service.

- **Authority Restrictions**: Servers and datacenters are located at various locations of the world and authority of every country offers certain restrictions on the resources, services and data which must be followed by the companies to smoothly function there which may limit the resources to the users.

2 Problem Statement

The importance of cloud-based services in current Information Technology (IT) is undeniable, especially for developing concepts like Internet of Things (IoT), big data, and quantum technologies. With the growing dependence of organisations on cloud computing to transform their data processing and storage approaches, ensuring security becomes of utmost importance. Ensuring the integrity and confidentiality of data inside cloud-oriented systems is crucial, necessitating the protection of sensitive data during communication and the prevention of active attacks. Emphasising strong cryptographic encryption approaches is crucial for strengthening the fundamentals of Cloud Based Security. The presence of current and developing cloud computing environments requires strong encryption methods which guarantee secure transfer of requests and offer protection against advanced active assaults. The task at hand involves creating and executing encryption protocols that can smoothly incorporate into various cloud infrastructures while effectively dealing with the distinct security demands presented by IoT, big data, and quantum technologies. The current issue is around the need to create, refine, and implement cryptographic solutions specifically designed for the complexities of cloud systems. This encompasses the process of reducing potential risks, guaranteeing adherence to regulatory standards, and achieving a careful equilibrium among performance and security. It is crucial to prioritise these issues in order to build confidence in cloud technology, facilitate its extensive use, and fully achieve the goals of IT business transformation.

3 Literature Survey

In[8], author(s) provides a detail description of CloudSim as an open source software for simulations of cloud computing systems and resource provisioning environment.Developed by University of Melbourne, Australia, it is not a framework with ready to use environment but a Java based modelling tool for simulating the environment to map the virtual resources with cloud servers and datacenters.
In[9], the author(s) mentions that there are many variants of CloudSim available for the developers with various domain specific features such as platform, simulator type, networking, availability, and programming language. CloudAnalyst is useful for examining the behavior of cloud applications. It adds a Graphical User Interface(GUI) with the CloudSim simulation environment. GreenCloud is another variant of CloudSim focusing on the energy consumption during the cloud communication. It is a packet level network simulator that consolidates the workload by datacenter virtualization and improves sustainability by reduction in the host count. Network CloudSim is structured to support the simulation of latency in network traffic, mapping of nodes and designing of cloud datacenters. Out of all the simulators, CloudSim is the most sophisticated one and hence, preferred for the implementation.
In[10] authors discussed many security issues, vulnerabilities, threats, and risks that slow down cloud computing adoption. The authors also focused on cloud security problems and challenges that emerged from the distinctive characteristics of the cloud. They presented a thorough explanation of these underlying problems in an effort to emphasize the necessity of investigating security issues in the context of cloud technology and providing suitable solutions. The authors also provided written rules, procedures, and processes that specify the risk-reduction security management strategy in the cloud system by increasing assurance in a continually interconnected world. Furthermore, they classified security issues, conducted a comparative study of security concerns, and proposed countermeasures to address these issues.
In[11] the author(s) surveyed different cloud-based attacks at various levels. Author(s) found there was a change in attack surface with the emergence of multi-cloud computing. Further, the integrated cloud with machine learning and artificial intelligence posed more significant security concerns.
In[12] the author presented different communication, computational, and SLA concerns through a comparative study. Computational and virtualization levels considered data-related security issues as the most crucial entities. The virtualization layer covered Hardware and virtual-level issues. Also, the Data gaps grouped into several categories. Additionally, the authors discussed further extensive cloud computing analysis for comparative purposes.

In[13] author(s) presented a qualitative analysis of all security flaws and associated risks with each service model. In addition, they proposed countermeasures to strengthen the security in cloud computing. The author(s) also depicted security concerns based on Cloud computing service paradigms including SaaS, IaaS, and PaaS. Moreover, a classification in terms of vulnerabilities, related threats, and viable countermeasures was being given based on broad and diverse literature published to address the security issues and their potential solutions in cloud computing. However, many of them were offered but not implemented, new approaches such as virtualization in cloud infrastructure and the use of cryptofunctions can be developed for more resilient cloud systems.
In[14] the authors emphasized the problems that occurred due to cloud characteristics and suggested the utilization of adaptive allocation of resources and task scheduling approaches in a multitenant system for equitable resource allocation. Further, the authors also proposed multifactor optimization approaches for better solutions to existing issues.
In[15] authors described cloud computing and its benefits. They emphasized on many security problems that must be handled appropriately, as well as the needs of cloud security. Further, authors focused on the reformulation and development of new standards and security approaches in order to give the best one for cloud computing.
In[16] author(s) focused on data integrity and privacy protection safeguards. They proposed a novel genetic algorithm (GA)-based model CryptoGA which is offered as a solution to data integrity and privacy concerns. The author(s) used GA for keys generation and integrate those keys using a cryptographic technique to protect the confidentiality and integrity of data stored in the cloud. Further, the author(s) also made a comparative study of widely used parameters and concluded that the CryptoGA model was more reliable and had improved performance as compared to cryptographic algorithms. The use of cryptographic methods to ensure high degree security for user data was proposed by the author(s) in [17] author(s) used split algorithm with cryptography and steganography to improve cloud storage and sharing security.
In[18] the author(s) discussed various kinds of cloud security, including what cloud technology is and how data is managed inside. Network encoding and cryptographic algorithms secure the cloud. Then the author(s) discussed ways to enhance cloud resource consumption and standards. The author(s) also discussed future development including redesigning the cloud infrastructure to be an effective files system. Innovations will bring new flaws and malfunctions, thus security will be studied, specifically with the cloud's expansion.
In[19] the author(s) addressed how cryptography approaches might help secure cloud technology. Also, the author(s) discussed that combining distinct cryptographic methods could result in the creation of hybrid solutions, which would be superior in terms of cloud computing security.
In[20] the author(s) investigated, analyzed, and classified cloud computing security difficulties, risks, and concerns utilizing five levels of computer networks, cloud technology implementation patterns, and client-side and server-side services. Also, they categorized alternatives and prevention techniques for persistent cloud computing security by security concerns. This categorization included cloud computing's architecture, services, implementation methods, and benefits. The suggested taxonomy also categorized security issues. The author(s) also proposed security standards and preventive actions to protect users' information and mitigate cloud vulnerability.
In [21] the authors explored the field of cryptographic methods and algorithms, offered a detailed overview of the current scene. The authors methodically examined a diverse range of cryptographic approaches, elucidating their uses, advantages, and constraints. This study provided a comprehensive perspective, making it a great resource for academics and professionals who want to traverse the complex field of cryptographic solutions. In [21] the authors not only facilitated comprehension of the mathematical foundations of cryptography approaches but also functions as a pragmatic manual for applying these algorithms in various scenarios. This paper added to the continuing discussion on the importance and effectiveness of cryptographic methods in the light of changing technological frameworks like cloud computing.
In [22] the authors focussed on Hybrid cryptographic methods on cloud security and cryptography. To secure cloud systems, the authors explored the complexities of developing and deploying hybrid cryptographic approaches.IN [22] the authors discussed the benefits of hybrid cryptography in handling the specific difficulties of the cloud by investigating several approaches. This paper provided a road map for improving the security status of cloud-based applications by introducing approaches and models that add

to the practical use of hybrid cryptographic techniques. In [23] the authors critically evaluated the efficacy of several homomorphic encryption algorithms on cloud security. Investigating the complex world of cloud security, the paper highlighted the advantages and disadvantages of various cryptographic methods. By conducting a thorough review of the available research, the authors enhanced our comprehension of how homomorphic encryption might strengthen cloud systems. The study highlighted the necessity for adaptive encryption methods and the dynamic character of cloud security. In its last section, the research suggested directions for further research on homomorphic encryption and its effects on cloud security as a whole. In [24] the authors explored modern cryptographic techniques in the framework of smart data analytics, Internet of Things (IoT), and blockchain. The authors provided a thorough examination of contemporary symmetric and asymmetric cryptography techniques, with a critical evaluation. The authors also provided significant insights for improving the security architecture in the changing landscape of information technology and future technologies by analysing the strengths and limitations of these strategies.

4 Security Concerns and Attacks

As in[25], to understand the security issues,the author(s) firstly addresses to the architecture of the CloudSim. It consists of three layers-Source Code, CloudSim Services, and CloudSim Core Simulation Engine. Source Code layer is responsible for all the simulation related specifications and requirements needed which are supplied to the Cloud Broker who further transfers the information as input to the CloudSim Services layer which is the middle layer in the architecture.It supplies virtual machines, datacenters, servers, storage resources and cloudlets. The underlying system allocation is managed by CloudSim Simulation Engine.
There are various security concerns linked with cloud computing such as:

- **Malicious Insiders**: An attacker can be anyone from the cloud service providing company or the business firm who has the access to the resources.To avoid it, Identity and Access Management(IAM) technology is used by various leading service providers.
- **Data Threats**: Cloud providers ensure that secure cloud environment is provided to the users but there can be damages or unforeseen emergencies uncontrollable for cloud service providers. Hence, developers should be using encryption algorithms at their end.
- **Provider lock-in**: Providers supply with fixed number of services and the users may not be able to get the functionality out of the services available and hence, need to look at other companies.
- **Cloud API vulnerabilities**: Strong control on Application Program Interface(API) is needed to avoid API vulnerabilities.
- **Vulnerable cloud services**: It can be the case that the cloud service provided is vulnerable to attacks by hackers.
- **Hypervisor vulnerabilities**: Weakness or vulnerabilities in a hypervisor can lead to gaining control over VMs or hosts by the hackers.

In [26], author(s) explains the security concerns associated with Cloud Computing. There are various attacks which show the lack of security in the cloud systems used.There are two types of attacks as explained in information security.These two are Active Attacks and Passive Attacks.
Active attacks entail manipulating or changing data as it is being transmitted. It is a danger to the integrity and availability as it can affect all the system resources. **Passive attacks** are those which don't involve system resources usage. The data streams are monitored to retrieve the desired information and attack the sender/receiver.Victim doesn't get to know about this kind of attack as the system resources are not harmed. Few of these attacks are specified.

- **Masquerade attack**: It is an active attack in which the sender of the information tries to be someone else.
- **Man in the middle attack**: In this passive attack, the man in the middle impersonates the communication between two end users without letting them know and monitor the information shared between them.
- **Injection attacks**: Through vulnerable web pages, hackers inject malicious codes and hence, redirect the user's request to their own modules and steal their data.German researchers tested AWS by performing XSS attack.

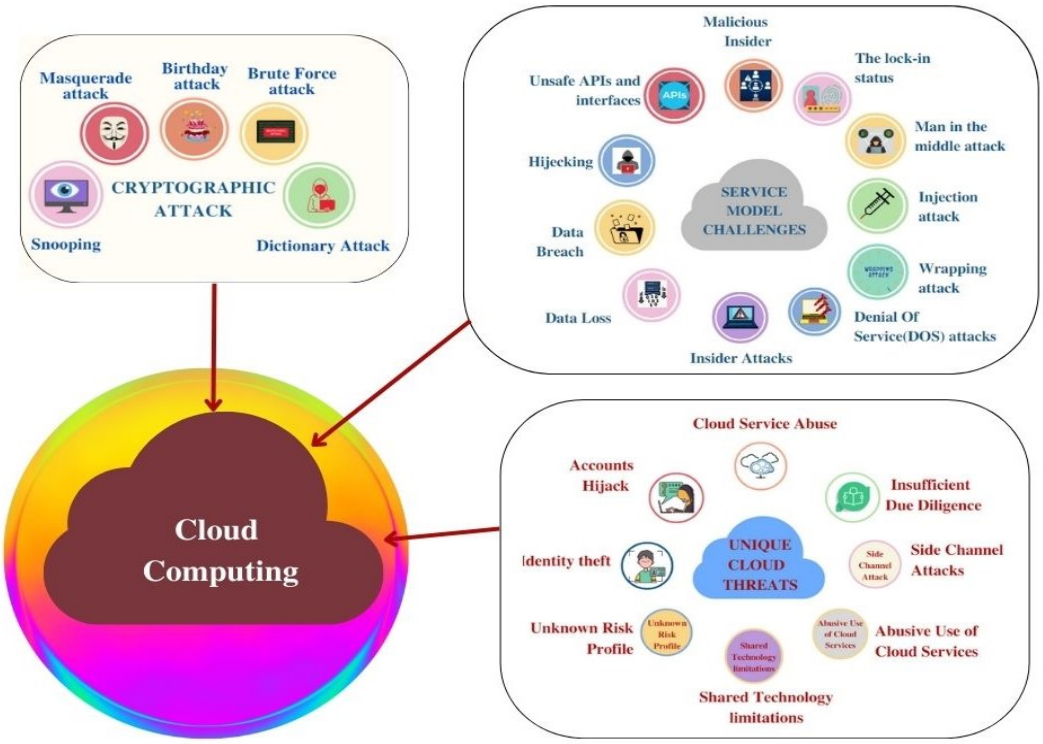


Fig. 4: Different Attacks in Cloud Computing

- **Wrapping attacks**: The data transferred in format of XML or JSON is manipulated by the hacker and wrong information is supplied. Such an attack was done on EC2 instance in 2009 using the SOAP interface.
- **Accounts Hijack**: The user account is hijacked by applying hacking techniques and then, used to steal the user account's information. This was done in salesforce.org where a user account was used leading to risk in stake of business's reputation.
- **Birthday Attack**: Such attacks are based on birthday paradox and applied on hash functions.The paradox says that atleast two students will have birthday on same day if there are 366 students in a class.
- **Brute Force attack**: The computer uses all the possible combinations to crack the password or credentials of the system or account.The attacker relies on the system for the task. It is seen that a fast computer can crack the security in about two hours using such an attack.
- **Dictionary attack**: The attackers use dictionary based passwords to crack the system login details and steal information. Users mostly use same password for all of their social media accounts and hence compromise with the security. Dropbox was attacked and resulted in loss of 60 million user credentials in 2012.
- **Cloud Service Abuse**: Cloud services are rented by hackers to perform brute force attacks on target users. The best example is the demonstration of brute force attack on Amazon EC2 instance by Thomas Roth at Black-Hat conference[27].
- **Side Channel Attacks**: The attackers create malicious virtual machines which resemble the VMs provided on the clouds.These are used to obtain crucial data of the users.
- **Denial Of Service(DOS) attacks**: The nodes send so many requests and hence, overload the server resulting into slowing down of server.
- **Insider Attacks**: An attacker can be a cloud broker, cloud service administrator who has access to the crucial content. hence, design system should restrict the leverage of details to anyone.
- **Snooping**: When a person unethically access or reads the information of the other system then that is known as Snooping. This not only includes data stream but the information on anyone's computer or hackable device.

The following major security risks have been identified by security experts [28], [29], [30], [31], [32]:

- **Data loss** may occur in a variety of ways. Data can be corrupted for the following reasons: deletion, modification, theft of the encryption key, and additional causes including disasters, floods, and wildfires, among others. To avoid such risks, a whole backup of the Organization's data should be kept.
- **Data breaches** are described as sensitive data to unauthorized individuals. Inappropriate identity verification and authentication systems, monitoring systems, unethical usage of cryptographic keys, disposal problems, and operating system malfunction all contribute to data breaches. This is a problem that many businesses have encountered.
- **Hijacking** a Service or Account The opponent obtains credentials, and the compromised account becomes a launchpad from which the adversary may snoop on the customer companies, return fake data, modify data, respond to sessions, divert the customer to illegal websites and issue numerous threats.
- **Unsafe APIs** and interfaces, since the security risks of cloud applications depend upon such APIs. To eliminate risks such as unauthenticated access, clear-text authentication, reused credentials, and improper authorization, APIs should be verified as secure and have specific access restrictions and session monitoring tools.
- **Malicious Insiders** are trustworthy individuals inside a company who have access to sensitive organisational resources. These hostile insiders can execute unprivileged operations to infiltrate organisational resources and cause damage by impersonating approved activities such as the Intrusion Detection System (IDS).
- **Insufficient Due Diligence** occurs when companies begin utilizing cloud service providers' services without knowing the level of computing models and operations.
- **Abusive** Use of Cloud Services is a consumer's irresponsible and unlawful act to take advantage of the services. Attackers can attack the system by taking advantage of the moderate architecture, resource-intensive provisioning, and poor authentication of users.
- **Shared Technology** limitations come up in a multi-tenant environment. Due to flaws in virtualized hypervisors, fraudulent customers can get improper access and control genuine customers' VMs.
- **Unknown Risk Profile** will come with major advantages such as saving time by maintaining infrastructure and granting possession. Customers, on the other hand, do not appear to be bound to internal security characteristics, upgrading, strengthening, monitoring, and logging processes, etc., eventually resulting in an unidentified risk profile that might create significant risks.
- **Identity theft** arises when a perpetrator makes a false identity claim in order to obtain authorization to access a company's resources. Changes to the business model pose a major risk because consumer data may be located in many countries regulated by various federal laws. The cloud service provider offers numerous resources to clients apart from informing them of the location of such services, and the client keeps losing control across the infrastructure, It poses a substantial risk and can have an impact on cloud users' lives.
- **The lock-in status** implies the inability of switching between clouds. This danger develops when companies enter the cloud service provider without an adequate understanding of the cloud model they are using, i.e., if the cloud model is acceptable for them based on their needs in order to avoid Lock-IN. Other security threats are less significant yet nevertheless exist in cloud settings. These security concerns include loss of governance, cloud service provider acquisitions, implications affecting credibility, a breakdown in data separation, compromised servers, and adherence to regulations, among others.

5 Cryptography

The major challenge faced by cloud companies is the security issues associated with cloud communication and storage. To ensure secure and safe cloud computing, there are three goals to be accomplished-reliability, secrecy, and integrity. The privacy protection of data is achieved by crypto techniques and integrity is taken care of by hashing algorithms.
In [33], the author(s) defines Cryptography as the art of converting plain text into an encoded message using some encryption function so that it is non-understandable by anyone and can only be decrypted using a secret key. It is an efficient tool used by developers to prevent the data and code from various attackers and hackers. It can be implemented using three techniques: Symmetric algorithms which comprise a single key to both message encryption/decryption. It has two types: Stream and block cipher

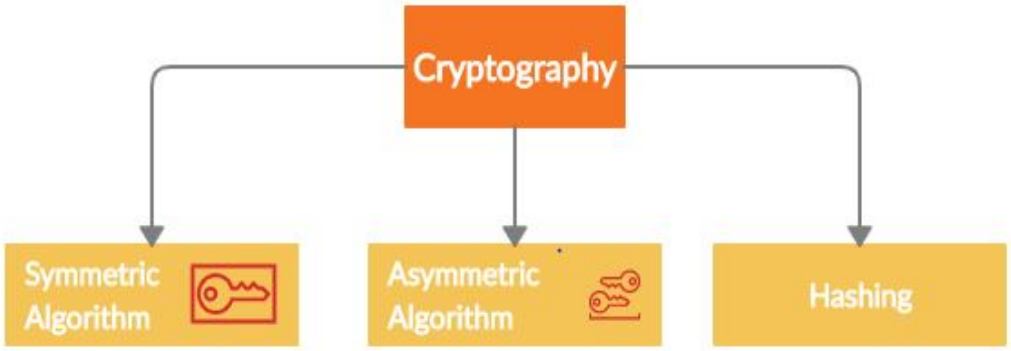


Fig. 5: Different types of Cryptography algorithms

algorithm. A few of its algorithms are Data Encryption Standard (DES), Triple DES, and Advanced Encryption Standard (AES). Asymmetric algorithms require two different keys for encryption and decryption: Public key encryption and decryption using separate keys. Rivest, Shamir, and Adleman's (RSA) algorithm is the popular technique used for encoding the message. In [34], the author(s) used a cryptographic algorithm called Cross Language Cryptography technique(CLCT) in which the simple text that is written in the English language, is first converted into Hindi and then encoded using a traditional Encryption Algorithm. Similarly, the message at the receiver end is decoded by applying a decryption algorithm and then converting the obtained code into plain text again. This cryptographic algorithm is more secure compared to other algorithms and has good performance. As any language chosen can be chosen by the sender to convert the message into, this technique can be used to improvise the efficiency of existing algorithms.
In [35], the author(s) compared two cryptography techniques in the user's data verification in a credit card-based mobile bill payment application. This paper is an extension of the work done in [34]. CLCT was applied using English and Hindi as the cross languages on the message and further, at the core, two encryption algorithms were implemented and compared which are the Rail fence cipher algorithm and the modified Affine algorithm. The two algorithms were compared according to runtime and the number of lines. The key used for encryption was the geographic location which is dynamic in nature and the application was deployed on Google App Engine.

6 Methodology Adopted

6.1 Work Flow in CloudSim

The CloudSim toolkit works as the intermediate layer between IaaS and PaaS and plays a key role in the development of simulations and modelling environment for cloud.The work flow of toolkit is as follows:

1. A Cloud Information Service(CIS) instance is instantiated by the user.
2. Data center is registered to CIS.
3. CIS is enquired by the data center broker for the data center allocation.
4. Details of data center registered is provided.
5. Cloudlets are delivered to the data center and registered.
6. Cloudlets are submitted to Virtual Machines by brokers.

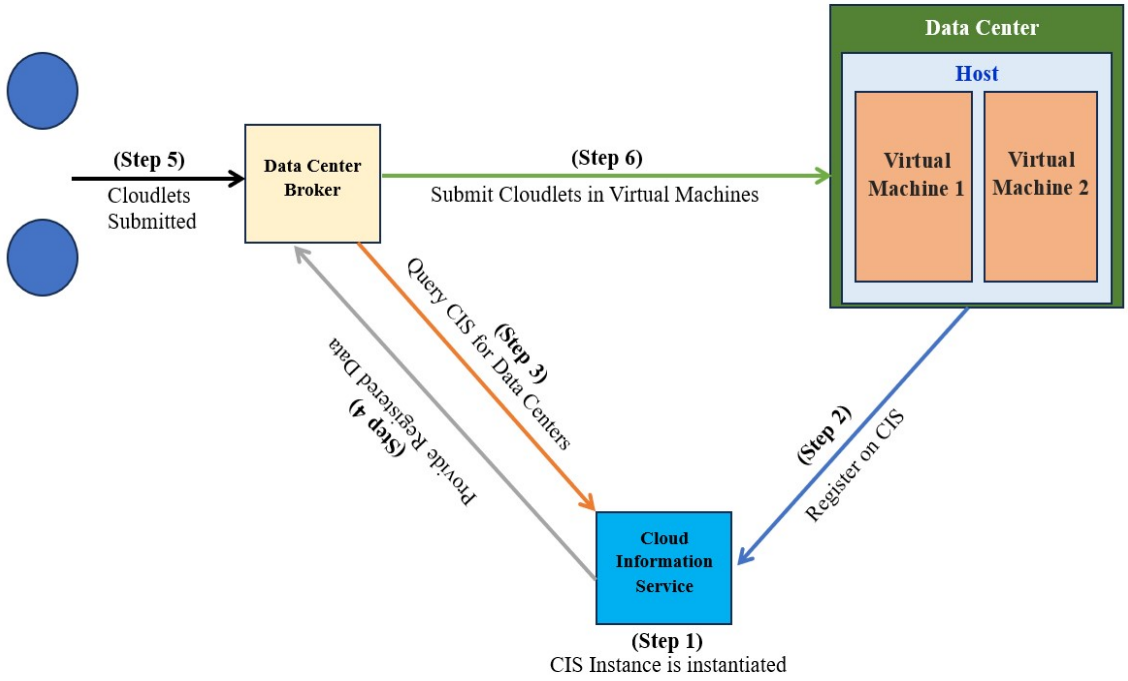


Fig. 6: Work flow in CLoudSim

7 Algorithms Formulation

7.1 Algorithm 1: Verify the User Information

7.1.1 Symbol

U_ID : User Id Entered
U_PWD : Password Entered
SUPWD : Password Stored in database for corresponding U_ID.

Algorithm 1 Trigger: As the user attempts to access CloudSim

Retrieve the password associated with U_ID from the database

if *U_PWD equals SUPWD* **then**
  Initialize the Resource Allocation Process
  return true
else
  return false
end

7.2 Algorithm 2: User-Specific Allocation of Resources

7.2.1 Symbol

MIPS : User-specified MIPS demand
RAM: User-imposed RAM requirements
CPU: Processing needs of the user (Number of Processors)
BW: Required bandwidth by the user
VM: Represents Virtual Machine
ID: Auto-generated VM's ID

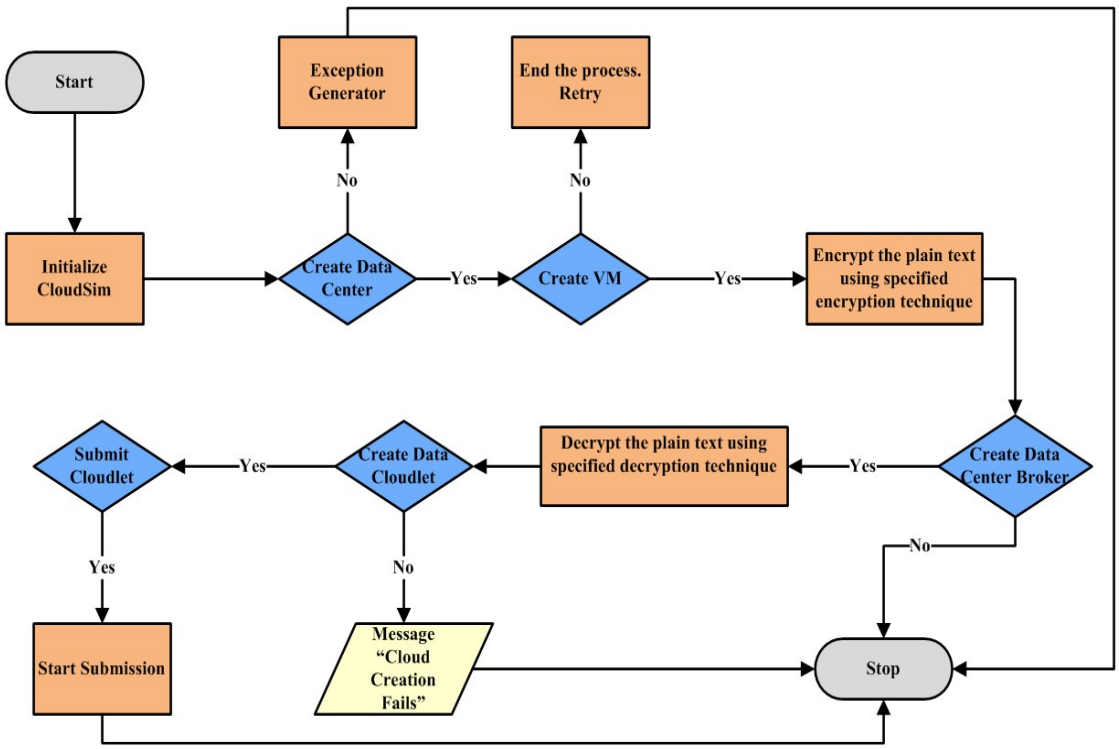


Fig. 7: Flowchart showing process of implementation

Algorithm 2 Trigger: Once resources are ready to be allocated

Begin the process of initializing the CloudSim Library
Build a datacenter
Setup a Broker for the DataCenter
Build a virtual machine with the following properties: VM (ID, MIPS, CPU, RAM, BW)
Add a VM to the VM List
Make a Cloudlet
Include Cloudlet on the Cloudlet List
Launch the Simulation

7.3 Algorithm 3: Allocating VM Resources.

Symbol
U_ID : User Id Entered
MIPS : User-specified MIPS demand
RAM: User-imposed RAM requirements
CPU: Processing needs of the user (Number of Processors)
BW: Required bandwidth by the user
VM: Represents Virtual Machine
ID: Auto-generated VM's ID

Algorithm 3 Trigger: As CloudSim user requests resource

```
for 1 to n do
    if (validateUser(U_ID,U_PWD)) then
        if (MIPS and RAM and CPU and BW == available) then
            ResourceAllocation (MIPS,RAM,CPU,BW)
        else
            Print "Requested resources are not available"
        end
    else
        Print "Please Enter correct User Id AND Password"
    end
end
```

7.4 Algorithm 2: User-Specific Allocation of Resources

7.4.1 Symbol

MIPS : User-specified MIPS demand
RAM: User-imposed RAM requirements
CPU: Processing needs of the user (Number of Processors)
BW: Required bandwidth by the user
VM: Represents Virtual Machine
ID: Auto-generated VM's ID

Algorithm 4 Trigger: Once resources are ready to be allocated

Begin the process of initializing the CloudSim Library
Build a datacenter
Setup a Broker for the DataCenter
Build a virtual machine with the following properties: VM (ID, MIPS, CPU, RAM, BW)
Add a VM to the VM List
Make a Cloudlet
Include Cloudlet on the Cloudlet List
Launch the Simulation

7.5 Algorithm 3: Allocating VM Resources.

Symbol
U_ID : User Id Entered
MIPS : User-specified MIPS demand
RAM: User-imposed RAM requirements
CPU: Processing needs of the user (Number of Processors)
BW: Required bandwidth by the user
VM: Represents Virtual Machine
ID: Auto-generated VM's ID

Algorithm 5 Trigger: As CloudSim user requests resource

```
for 1 to n do
    if (validateUser(U_ID,U_PWD)) then
        if (MIPS and RAM and CPU and BW == available) then
            ResourceAllocation (MIPS,RAM,CPU,BW)
        else
            Print "Requested resources are not available"
        end
    else
        Print "Please Enter correct User Id AND Password"
    end
end
```

7.5.1 Caesar Cipher Algorithm

Simplest of all the Encryption techniques,Caesar Cipher works on shifting of the letters of the plain text to be encrypted by some constant factor called as shift.This algorithm is simple to decode and was first used by Julius Caesar and hence named after him.

Notation

x: Plain Data (digit).
n : Shift value (In our case n = 3).
E(x) : Encryption Function that returns Encrypted Data.
D(x) : Decryption Function that returns Decrypted Data.

$$\textbf{Encryption Function} \ : \ E(x) = (x + n) mod \ 26 \tag{1}$$

$$\textbf{Decryption Function} \ : \ D(x) = (x - n) mod \ 26 \tag{2}$$

Algorithm 6 Caesar Cipher Algorithm
Trigger-When user submits their requirements

Encryption/Decryption()

1. Scan each character in the specified Plain Text one by one.
2. For each digit, modify the specified character according to the encryption or decryption function, based on if the text is being encrypted or decrypted.
3. Return the newly created digit.

7.5.2 Vigenere Cipher Algorithm

Vigenere Cipher Algorithm is a poly-alphabetic substitution that uses Vigenere table to encode the message.A keyword is used in cyclic manner through the plain text such that each letter of keyword is used for substitution of corresponding letter in plain text as per the Vigenere table.

Notation

P : Plain text(digit).
K : Repeating Keyword used for encryption of plain data.
Ex : Encryption Function that returns Encrypted Data.
Dx : Decryption Function that returns Decrypted Data.

The Plain Text(P) and Key(k) are added with modulo 26

$$\textbf{Encryption Function} \ : \ Ex \ = \ (Px \ + \ Kx) mod \ 26 \tag{3}$$

$$\textbf{Decryption Function} \ : \ Dx \ = \ (Ex - Kx + 26) mod \ 26 \tag{4}$$

Algorithm 7 Vigenere Cipher Technique
Trigger- When user submits their requirements

Encryption()

1. Encryption of the original text is done with the help of Vigenere table
2. Vigenere table contains alphabets written 26 times in multiple rows
3. During encryption, cipher text employs a distinct alphabet from one of the Vigenere table's rows.
4. Plain data 's alphabet is mixed with keyword . The alphabet at every point uses a repeating keyword

7.5.3 Affine Cipher Technique

Affine Cipher Algorithm is mono-alphabetic substitution cipher technique prone to many types of attacks and hence is not considered secure. It needs two coprime numbers within a given range of 26 such that all the alphabets of the plain text are encrypted using the encryption function.
Notation:
x : Plain text(character)
a, b: The Cipher Keys (a and m need to be co-prime).
E(x) : Encryption Function that returns Encrypted Data.
D(x) : Decryption Function that returns decrypted (Plain) Data.
a $^{-1}$: modular multiplicative inverse of (a modulo m).

$$\textbf{Encryption Function} \ : \ E(x) \ = \ (ax + b) mod \ m \tag{5}$$

$$\textbf{Decryption Function} \ : \ D(x) = a^{-1}(x - b) mod \ m \tag{6}$$

Algorithm 8 Affine Cipher Technique
Trigger-When user submits their requirements

Encryption()

1. In affine Cipher , each alphabet is mapped to an integer
2. Key in affine cipher contains two numbers , we call a and b. a should be co-prime to m
3. The encryption function converts the integer (to which each simple text alphabet belongs) to some other integer using modular arithmetic (that is equivalent to the encryption alphabet)

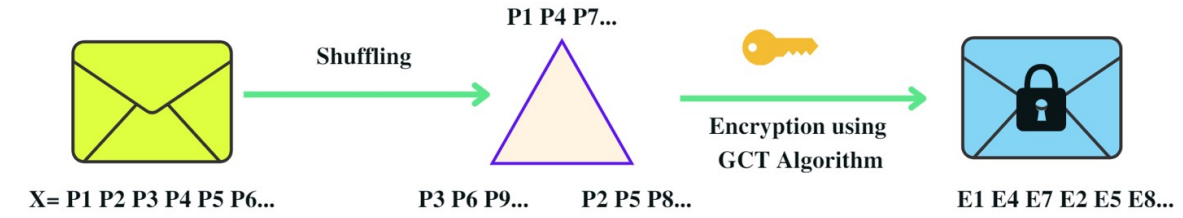
Decryption()

1. In decryption also , each alphabet is mapped to an integer
2. Then, compute multiplicative inverse
3. Decryption function also employs modular arithmetic to convert the integer (to which each simple text alphabet relates) further into an integer (corresponding to the cipher alphabet) after multiplying with the multiplicative inverse

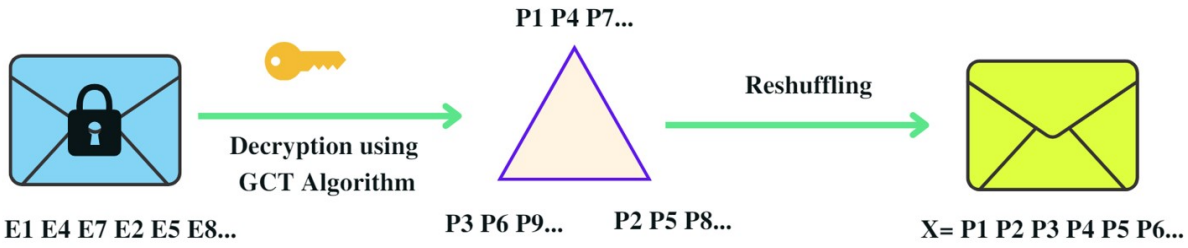
7.5.4 Geometrical Cryptography Technique (GCT)

In this Encryption technique, GCT works on shuffling the Alphanumeric letters of the plain text to be encrypted by using a triangular shape, and then the encryption/decryption is performed. Finally, a reshuffling is done to get the original message. The Fig.8 depicts how the GCT works:
Notation
x: Plain Data (Alphanumeric with whitespace).
K_{GCT}: Key value.
E(x): Encryption Function that returns Encrypted Data.
D(x): Decryption Function that returns Decrypted Data.
Encryption / Decryption Function:

$$Encryption Function: \ E(x) \ = \ (x + K_{GCT}) \, mod \, 26 \tag{7}$$



(a) Encryption using GCT



(b) Decryption using GCT

Fig. 8: Encryption and Decryption using GCT

$$DecryptionFunction: \ D(x) \ = \ (x - K_{GCT}) \, mod \, 26 \tag{8}$$

Algorithm 9 Geometrical Cryptography Technique (GCT)
Trigger:When user specifies their requirements

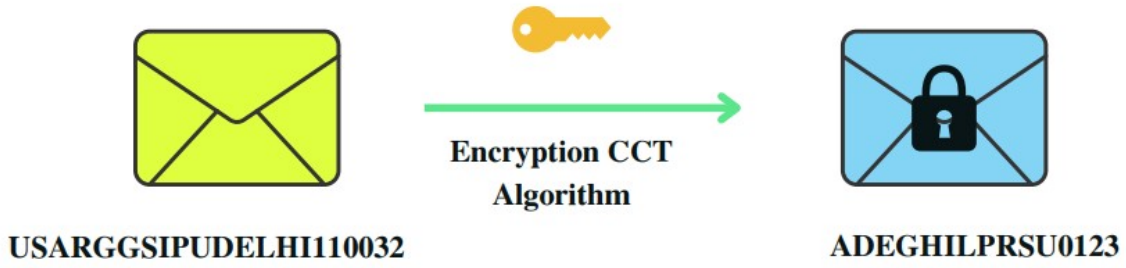
1. Shuffling and division of Plaintext using Triangular shape. (Padding is done if required.)
2. Encyption/Decryption
   (a) Scan each character in the specified Plain Text one by one.
   (b) For each digit, modify the specified character according to the encryption function `encryptedData(`*StringinputStr,intsKey*`)` or decryption function `decryptedData(`*StringenText, intsKey*`)`, based on if the text is being encrypted or decrypted.
   (c) Return the newly created Alphanumeric.
3. Reshuffling the decrypted text.

7.5.5 Circular Cryptographic Technique (GCT)

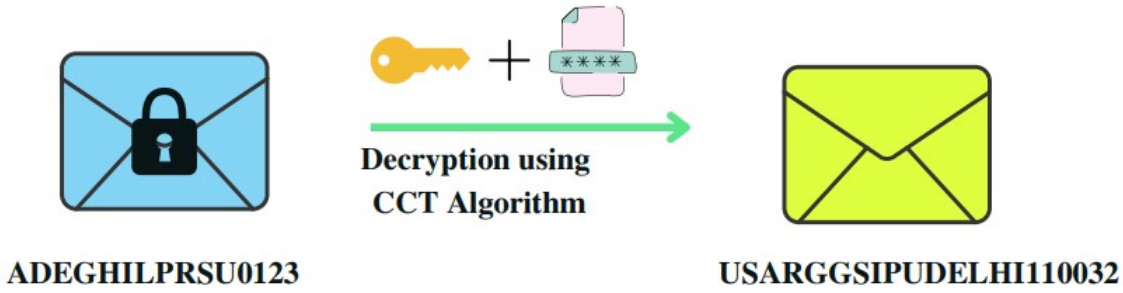
In CCT Encryption technique the alphanumeric letters of the plain text are encrypted by using the key generated. Encryption function make use of finite number of circular tracks of fixed size. For decrypting the cipher text, a shared key and secrete token are used. The following figure depicts how CCT works:
Notation
x: Plain Data.
$(x_1, x_2, ...x_n)$: Set of unique alphanumeric letters in the string
K_{CCT}: Key value.
T_{CCT}: Secrete Token.
E(x): Encryption Function that returns Encrypted Data.
D(x): Decryption Function that returns Decrypted Data.
Encryption / Decryption Function:

$$EncryptionFunction: \ E(x) \ = \ (x_1, x_2, ...x_n).(K_{CCT}) \tag{9}$$

$$DecryptionFunction: \ D(x) \ = \ ((x_1, x_2, ...x_n).(K_{CCT})).(K_{CCT}).(T_{CCT}) \tag{10}$$



(a) Encryption using CCT



(b) Decryption using CCT

Fig. 9: Encryption and Decryption using CCT

Algorithm 10 Circular Cryptographic Technique (CCT)
Trigger:When user specifies their requirements

---

1. Generate
   (a) a shared key for the given plain text using keygeneration(String Plaintext) function.
   (b) a secrete token for the given plain text using tokengeneration(String Plaintext) function
2. Encyption/Decryption
   (a) Scan each character in the specified Plain Text one by one
   (b) For each alphanumeric letter, modify the specified character according to the encryption function `encryptedData(`*String input, int Key*`)` or decryption function `decryptedData(`*String enText, int Key, int Token*`)`, based on if the text is being encrypted or decrypted.
3. Return the newly created Alphanumeric

---

8 Results

All the cryptograhic techniques were applied during the request for allocation of VM resources using the code executed on CloudSim environment and later the outputs were collected and compiled to draw comparisons among various techniques used in order to determine which one can prove to b suitable for the purpose of encryption of the cloud broker request. The parameters considered were the execution time, time and space complexities of techniques,and lines of code (LOC).
Following tables (Table 1, Table 2 and Table 3) show the results drawn from the outputs obtained after the performing the simulations on CloudSim. We have considered three different types of Plain text for our simulation.

The bar graphs shown below in Figure 10 and Figure 11 provide a clear comparison among the algorithms. It can be observed that Affine Cipher technique has more number of lines of Code than all other techniques and also, it has the maximum execution time too. The GCT and CCT algorithms

Table 1: Simulation Results for Plain Text: GGSIPU

	Caesar Cipher	Vigenere Cipher	Affine Cipher	GCT	CCT
Cipher Text	KKWMTY	GSABPG	SSOAPW	KMKTWY	GIPSU
Decrypted Text	GGSIPU	GGSIPU	GGSIPU	GGSIPU	GGSIPU
Lines Of Code (LOC)	50	80	90	47	38
Execution Time	1072300.2μs	1050899.6μs	1057900.2μs	1046200.2μs	45237940.2μs
Time Complexity	O(n)	O(n)	O(n)	O(n)	O(n^2)
Space Complexity	O(1)	O(1)	O(1)+key length	O(1)	O(1)+key length

Table 2: Simulation Results for Plain Text: GGSIPU110023

	Caesar Cipher	Vigenere Cipher	Affine Cipher	GCT	CCT
Cipher Text	55!;"'CCBB@A	KKWMTY554467	GSABPG110023	KM54KT56WY47	GIPSU0123
Decrypted Text	GGSIPU110023	GGSIPU110023	GGSIPU110023	GGSIPU110023	GGSIPU110023
Lines Of Code (LOC)	50	80	90	47	38
Execution Time	1035480.8μs	1114639.4μs	1153319.8μs	1114239.8μs	43983960μs
Time Complexity	O(n)	O(n)	O(n)	O(n)	O(n^2)
Space Complexity	O(1)	O(1)	O(1)+key length	O(1)	O(1)+key length

Table 3: Simulation Results for Plain Text: *GGSIPU@110023#

	Caesar Cipher	Vigenere Cipher	Affine Cipher	GCT	CCT
Cipher Text	KKWMTY554467	SOLIBC110023	SSOAPW770041	*WY56KM@47KT54#	GIPSU0123*@#
Decrypted Text	GGSIPU110023	SCDPBQ110023	GGSIPU110023	*GGSIPU@110023#	*GGSIPU@110023#
Lines Of Code (LOC)	50	80	90	47	38
Execution Time	1032100.4μs	1008100μs	1092040μs	1082800μs	44759320μs
Time Complexity	O(n)	O(n)	O(n)	O(n)	O(n^2)
Space Complexity	O(1)	O(1)	O(1)+key length	O(1)	O(1)+key length

have lesser number of lines of codes and execution time as well when compared to all other algorithms. Hence,according to the results it can be concluded that the purposed GCT and CCT algorithms have performed outstanding than other techniques.

9 Analysis of Results

The table 11 displays the temporal and spatial complexity of each cipher, providing valuable insights about their efficiency. Nevertheless, it is crucial to acknowledge that the effectiveness of a cipher is influenced by elements beyond only time and space complexity. Additional considerations, such as the amount of storage space needed to store both the key and the ciphertext, can also hold significance.
Generally, the table offers valuable insights into the temporal and spatial intricacies of various ciphers. Nevertheless, it is crucial to bear in mind that additional aspects, such as security and efficiency, must also be taken into account when selecting a cipher.
Below is an in-depth examination of the data presented in the tables:
The Caesar cipher is the most basic cipher in the table. Additionally, it is the least secure option, as it may be effortlessly compromised by brute force methods. The Caesar cipher has a time complexity of O(n), indicating that the duration required to encrypt or decrypt a message is directly proportional to the length of the message. The Caesar cipher has a space complexity of O(1), indicating that it does not necessitate any supplementary space for key storage.
The Vigenere cipher, while more secure than the Caesar cipher, nonetheless has vulnerabilities that make it susceptible to certain assaults. The Vigenere cipher has a time complexity of O(n), indicating that the duration required to encrypt or decrypt a message is directly proportional to the product of the message length and the key length. The Vigenere cipher has a space complexity of O(1), indicating that it necessitates storage for the key.

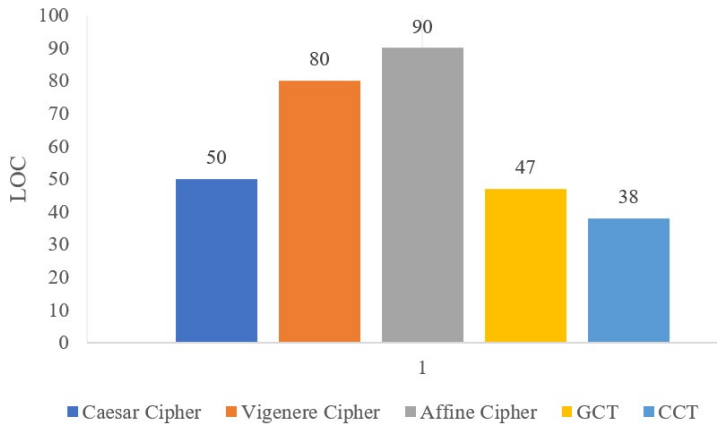


Fig. 10: LOC-based comparison of several algorithms

The affine cipher offers a higher level of security compared to the Caesar cipher and the Vigenere cipher, however it remains susceptible to certain assaults. The affine cipher has a time complexity of O(n), indicating that the time required to encrypt or decrypt a message is directly proportional to the length of the message. The affine cipher has a space complexity of O(1), indicating that it does not necessitate any extra space for key storage.
The Geometrical Cryptography Technique (GCT) cipher is a substitution cipher that offers greater security compared to the Caesar cipher and the Vigenere cipher. However, it remains susceptible to certain attacks. The GCT cipher has a time complexity of O(n), indicating that the duration required to encrypt or decrypt a message is directly proportional to the message's length. The GCT cipher has a space complexity of O(1), indicating that it does not necessitate any supplementary space for key storage.
The Circular Cryptographic Technique (CCT) cipher is a polyalphabetic substitution cipher that offers more security compared to the Caesar cipher, the Vigenere cipher, and the GCT cipher. Nevertheless, it remains susceptible to some forms of attacks. The CCT cipher has a time complexity of O(n2), indicating that the time required to encrypt or decrypt a message is directly proportional to the product of the message length and the key length. The CCT cipher has a space complexity of O(1) + key length, indicating that it necessitates storage space for the key.

10 Conclusion and Future Work

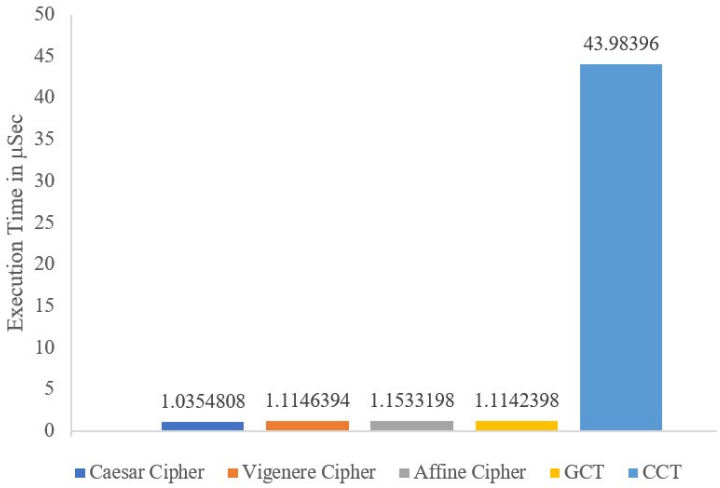
Through the paper, it is inferred that the requests and response can easily be encrypted in order to ensure accurate allocation of the resources to the Users. Various algorithms used in the simulations are compared and contrasted on certain parameters and it is concluded that the GCT and CCT algorithm performed better than others.But, these algorithms are also prone to Brute Force attacks and it is needed that more secure algorithms be tried and implemented.
Further in future, the encryption technique can be used so that same encryption key can be used throughout the allocation process all the way from user to vendor to reduce work load and enhance security.

Declarations and Competing interests

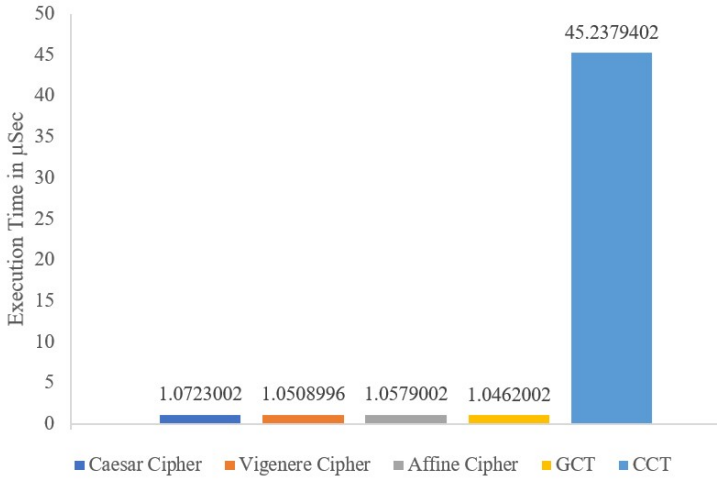
There are no conflicts of interest among the authors.

Acknowledgement

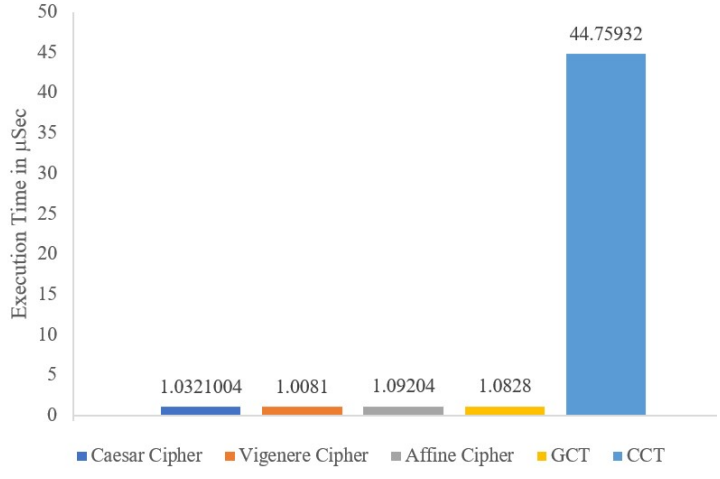
We acknowledge our university, GGSIPU in Delhi, for offering a learning environment that encourages academic research.



(a) Plain Text: GGSIPU



(b) Pain Text: GGSIPU110023



(c) Plain Text: *GGSIPU@110023#

Fig. 11: Execution time-based comparison of several algorithms

References

[1] Mell, P., Grance, T. The NIST definition of cloud computing

[2] Chen, D., and, Z.H.D.: and privacy protection issues in cloud computing. In: In2012 International Conference on Computer Science and Electronics engineeringMar 23 (Vol, pp. 647–651. 1, IEEE (2012)

[3] TS., C.: Security threats on cloud computing vulnerabilities. International Journal of Computer Science & Information TechnologyJun **1**, 5 (2013)

[4] Santos, N., Gummadi, K.P., Rodrigues, R.: Towards trusted cloud computing. HotCloudJun **14**, 9 (2009)

[5] Google, Cloud Computing Services — Google Cloud [Internet]. Google Cloud Available from (2019). https://cloud.google.com/

[6] Amazon.com: Available From:. https://docs.aws.amazon.com/

[7] [Internet], I.C.: Www.ibm.com, Available from. https://www.ibm.com/cloud/

[8] Malhotra, R., and, J.P.S.: and comparison of cloudsim simulators in the cloud computing. The SIJ Transactions on Computer Science Engineering & its ApplicationsSep; **1**(4), 111–5 (2013)

[9] Goyal, T., Singh, A., Cloudsim, A.A.: simulator for cloud computing infrastructure and modeling. Procedia EngineeringJan **1**(38), 3566–72 (2012)

[10] Tabrizchi, H., Kuchaki Rafsanjani, M.A.: survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputingDec; **76**(12), 9493–532 (2020)

[11] Panda, D.R., Behera, S.K., Jena, D.A.: survey on cloud computing security issues, attacks and countermeasures. In: Singapore, S. (ed.) InAdvances in Machine Learning and Computational Intelligence: Proceedings of ICMLCI2021, pp. 513–524 (2019)

[12] Chitturi, A.K., Swarnalatha, P.: Exploration of various cloud security challenges and threats. In: InSoft Computing for Problem Solving: SocProS 2018, Volume 2. Singapore, pp. 891–899 (2020)

[13] and, S.A.S.: and countermeasures in cloud computing: a qualitative analysis. International Journal of Information TechnologyDec; **11**, 683–90 (2019)

[14] Siddiqui, S., Darbari, M., Yagyasen, D.A.: comprehensive study of challenges and issues in cloud computing. Soft Computing and Signal Processing: Proceedings of ICSCSP **2018**, 1325–44 (2019)

[15] Radwan, T., Azer, M.A., and, A.N.C.: and future trends. International Journal of Computer Applications in Technology **55**, 2 (2017)

[16] Tahir, M., Sardaraz, M., Mehmood, Z., CryptoGA, M.S.: a cryptosystem based on genetic algorithm for cloud data security. Cluster ComputingJun; **24**, 739–52 (2021)

[17] Garg, P., Sharma, M., Agrawal, S., Kumar, Y.: Security on cloud computing using split algorithm along with cryptography and steganography. In: InInternational Conference on Innovative Computing and Communications: Proceedings of ICICC 2018, Volume 1. Singapore, pp. 71–79 (2019)

[18] Kopacz, P., MM., C.: Cloud computing security and future. In **2022**, 264–269 (2022)

[19] Shirgaonkar, M., Shinde, A., Sankpal, P., Gutte, V.: Cloud computing security using cryptographic algorithms. In: In2022 6th International Conference on Computing Methodologies and Communication (ICCMC)Mar 29, pp. 31–37. IEEE, ??? (2022)

[20] Jangjou, M., Sohrabi MK., A.: Comprehensive survey on security challenges in different network layers in cloud computing. Archives of Computational Methods in EngineeringJan **24** (2022)

[21] Sharma, D.K., Singh, N.C., Noola, D.A., Doss, A.N., Sivakumar, J.: A review on various cryptographic techniques & algorithms. Materials Today: Proceedings **51**, 104–109 (2022)

[22] Murad, S.H., Rahouma, K.H.: Hybrid cryptography for cloud security: Methodologies and designs. In: Digital Transformation Technology: Proceedings of ITAF 2020, pp. 129–140. Springer, ??? (2022)

[23] Mahato, G.K., Chakraborty, S.K.: A comparative review on homomorphic encryption for cloud security. IETE Journal of Research **69**(8), 5124–5133 (2023)

[24] Bhatia, A., Naveen, N.: Review of modern symmetric and asymmetric cryptographic techniques. In: Intelligent Data Analytics, IoT, and Blockchain, pp. 79–88. Auerbach Publications, ??? (2024)

[25] Calheiros, R.N., Ranjan, R., Beloglazov, A., De Rose, C.A., CloudSim, B.R.: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. Software: Practice and experienceJan; **41**(1), 23–50 (2011)

[26] User, S.: Cloud Computing: A New Vector for Cyber Attacks [Internet], Apriorit Available from (2018). https://www.apriorit.com/dev-blog/523-cloud-computing-cyber-attacks

[27] Roth, T.: Breaking encryptions using gpu accelerated cloud instances. InBlack Hat Technical Security ConferenceJan **6** (2011)

[28] benefits, C.D.C.C.: risks and recommendations for information security. In: InWeb Application Security: Iberic Web Application Security Conference, IBWAS 2009, Madrid, Spain, December, 2009. Revised Selected Papers(pp. 17-17). Heidelberg, pp. 10–11. Springer, Berlin (2010)

[29] CS., A.: Top threats to cloud computing v1. 0. White PaperMar; **23** (2010)

[30] Los, R., Shackleford, D., Sullivan, B.: The notorious nine cloud computing top threats in 2013. Cloud Security AllianceFeb; **2** (2013)

[31] Behl, A.: Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In **2011**, 217–222 (2011)

[32] MM., A.: Elements of Cloud Computing Security: A Survey of Key Practicalities. Springer, International Publishing;Jul 14 (2016)

[33] S. Khan, S., ProfR., R.T.: Security in cloud computing using cryptographic algorithms. International Journal of Innovative Research in Computer and Communication EngineeringJan **30**, 148–54 (2015)

[34] Singh, L., Clct, J.R.: cross language cipher technique. In: InSecurity in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August, 2015. Proceedings 3(pp. 217-227). International Publishing, pp. 10–13 (2015)

[35] Gupta, V., Johari, R., Gupta, K., Bhatia, R., Lbclct, S.S.: location based cross language cipher technique. Smart Cities Performability, Cognition, & Security, 221–34 (2020)

Declarations

- **Ethics approval**
  There is no research with human participants done by any of the authors in this article.
- **Funding**
  Not Applicable
- **Availability of data and materials**
  Not Applicable