HYBRID CRYPTOGRAPHIC MODEL TO ENHANCE THE SECURITY IN THE CLOUD.

A PROJECT REPORT

Submitted by

***M S L V S* LIKHITA**

A SAI TEJA

G VAISHNAVI

K RAVINDHRANATH

In Partial Fulfillment of the award of

the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

Under the Guidance of

Prof. DR. VIPUL DABHI

Department of Computer Science & Engineering

Parul University, Vadodara

February, 2023

PARUL UNIVERSITY

CERTIFICATE

This is to Certify that Project-1 -Subject code 203105328 of 6th Semester entitled "**HYBRID CRYPTOGRAPHIC MODEL TO ENHANCE THE SECURITY IN CLOUD"**
Of Group No. PU CSE_73 has been successfully completed by

M S L V S LIKHITA - 200303124337

A SAI TEJA - 200303124109

G VAISHNAVI – 200303124236

K RAVINDHRANATH - 200303124318

under my guidance in partial fulfillment of the Bachelor of Technology (B.TECH) in Computer Science and Engineering of Parul University in Academic Year 2022-2023.

Project Guide
Dr. VIPUL DABHI

Project Coordinator
Prof. YATIN SUKLA

Head of Department,
CSE
Dr. AMIT BARVE

External Examiner

ACKNOWLEDGEMENT

Behind any major work undertaken by an individual there lies the contribution of the people who helped him to cross all the hurdles to achieve his goal.

It gives me the immense pleasure to express my sense of sincere gratitude towards my respected guide **Prof. Dr. VIPUL DABHI** , (Associate Professor) forhis persistent, outstanding, invaluable co-operation and guidance. It is my achievement to be guided under him. He is a constant source of encouragement and momentum that any intricacy becomes simple. I gained a lot of invaluable guidance and prompt suggestions from him during entire project work. I will be indebted of him forever and I take pride to work under him.

I also express my deep sense of regards and thanks to **Prof. AMIT BARVE**, (Professor and Head of Computer Science &Engineering Department). I feel very privileged to have had their precious advices, guidance and leadership.

Last but not the least, my humble thanks to the Almighty God.

Place: Vadodara

Date:

M S L V S LIKHITA – 200303124337

A SAI TEJA – 200303124109

G VAISHNAVI – 200303124236

K RAVINDRANATH-200303124318

Abstract

The world is developing into a highly technological place where technology wants to optimally improve space and cost. the way for this growth cloud is the acquisition of their richness in technology by the way they render the services. The cloud is the demand of the hour, which needs to be protected. Each and every data entity residing in the cloud is to be authenticated so that there is no escape from critical and sensitive information. One of the primary requirements that are challenging in the cloud sector is the factor of security for the humongous data in the cloud. The cloud network is not a constrained homogeneous one, but a very dynamic and heterogeneous which makes it falls to threats. Data encryption is significant a part of security that has to be concentrated on improving security mechanisms. This research paper combines various cryptographic algorithms such as RSA with a digital signature, SHA-3, and Brotli. This is a hybrid approach where RSA with a digital signature is used for confidentiality and authentication, hashing is done by SHA-3 and Brotli will be used for compression. This paper also provides an analysis of how the various algorithms are selected depending on various factors and the bound through which will provide a better hybrid approach

Keywords: Encryption Algorithms, Cloud Security, Data Security, Information Security.

Contents

Chapter 1

Introduction

Cloud computing is an example that reduces services in several forms to cloud users. The ease of its usage, access, and scalability are the significant features of the cloud. Cloud computing is a massive arena that offers numerous benefits to organizations, but these profits can become a drawback if appropriate information security and privacy are not ensured. The breach of safety in cloud services can result in high costs of failure. There is an important part of the cloud where the security is supposed to be realistic that data storage

Figure 1.1

1.1 Security issues in the cloud

The physical security of the data centers is not under the direct control of the service providers, hence data security trusts the infrastructure providers. Hence the cloud service providers should effectively manage the Infrastructure providers. The vulnerability is more effective in cloud computing because of the humongous data and its interferences. These are some common security issues in the cloud :

- Data Security: The cloud environment poses a lot of data from different users of the cloud and the major concern is the security of this huge amount of data because these data may be personal information.
- Data Integrity: Maintaining the integrity of the data of the cloud user is a big task for cloud providers. To preserve the integrity cloud service provider can encrypt the data before storing it in the database so it could not modify by an intruder easily.
- User Authenticity: Authentication is a significant concern in the cloud environment because of the attacks like session hijacking. For providing authentication cloud service providers can use digital signatures at both side user and service provider to validate the original user identity, like a one-time-password(OTP).
- Disaster Management: In a cloud environment, there is more than one cause producing emergencies such as failure of hardware devices like switches, hubs, etc., and failure due to software like unwanted threats, bugs, low bandwidth, etc. To manage these disasters cloud service providers can use a backup strategy to keep the user's data safe and secure

such as proxy servers and distribute storage.

- Distribution of data: Inappropriate distribution of data rises the load on the cloud server and decreases the server performance and it affects the services consecutively on that server. Cloud computing is an example that reduces services in several forms to cloud users. The ease of its usage, access, and scalability are the significant features of the cloud. Cloud computing is a massive arena that offers numerous benefits to organizations, but these profits can become a drawback if appropriate information security and privacy are not ensured. The breach of safety in cloud services can result in high costs of failure. There is an important part of the cloud where the security is supposed to be realistic that data storage

1.2 Classification based on service and security policy

- Platform as a Service (PaaS)
  This service provides various operating systems, web server technologies, and execution situations. In this type of service, the customer actually sometimes may not be aware of the location of data. Therefore, proper encryption morals and key management standards should be accurately applied.
- Infrastructure as a Service (IaaS)
  In Infrastructure as a service, the customer is delivered with software stacks, middleware, and application. The common nature of cloud services makes it consider adapting the security policies It becomes important that the standard encryption mechanism is functional to handle the data stored and for the user communication.
- Software as a Service (SaaS)

  It offers various software-linked applications to cloud users. The users of this service must ensure the desires of confidentiality, integrity, and availability are satisfied. The client is given the capability of accepting the data encryption standards that are applied to data at rest and in motion. The customer is made to be conscious of how delicate data are distinct in their data organization and is being precise in outdated and by other formation options aim and Objectives

  Algo trading aims to save costs, minimize market impact, and reduce execution risk. It eliminates the need for manual monitoring, allowing trades to be executed at the best possibleprice while avoiding large price fluctuations. With a computer executing trades, there is a lowerlikelihood of mistakes and higher levels of accuracy. Pre-written algorithms allow for increasedspeed in carrying out trades, and lower transaction costs due to reduced monitoring requirements.

1.3 Classification based on service and security policy

- Application layer: It is the top layer in the hierarchy. It affords all the cloud applications

- Platform Layer: It contains the operating systems and application framework. It moderates the problem of deploying applications directly into VM containers
- Infrastructure Layer: It is also known as the virtualization layer. It creates the storage and resources of computing by segregating the physical resources. This dividing is done by the virtualization technologies like Xen, Vmware, etc. It is one of the significant layers in cloud computing as it provides diligent topographies like dynamic resource management
- Hardware Layer: Physical resources are achieved by this layer. This contains routers switches

Chapter 2

Literature Review

Security has been a serious approach to be dealt with in the cloud that disturbs the confidentiality, integrity, and, non-repudiation mechanisms. The most three popular algorithms used for security are AES, Blowfish and, RSA. [1] The comparison is done according to the implementation in java programming language and the RAM used played an important role in determining the effective solution for the comparison. Data security has been a serious issue in the cloud as several algorithms put in place to provide the concerned security. The blowfish, RSA and, AES algorithms are specifically compared for this purpose

2.1 Critical Evaluation of Journal paper

Paper 1: Comparative Analysis of the Performance of Selected Security Algorithms in Cloud computing

The objective of the paper is to use computer networks and the Internet to exchange important messages, files, photos, and other digital resources. However, these data need to be protected against hacking, theft, phishing, and other related cybercrime. In nowadays digital society, people are supported with modern communications through computers, mobile phones, and other devices.

The aim behind implementing this model is to Blowfish exhibited better performance than AES and RSA algorithms. The aspects of key generation, encryption, and decryption were all tested and in all of the results, Blowfish gained the least processing time. This makes it an excellent candidate for being one of the best security algorithms

The three most common security algorithms used in connection computing [5] were selected and compared in this paper. Then a, simulation was done in order for us to record the performance of each algorithm. Two computers have been utilized, both having Intel I3 Processors with 4GB and 8GB RAM, respectively. NetBeans IDE 8.02 was used to run Java programs for the algorithms, all the programs are the same in structures. AES Rijndael, Blow, fish, and RSA cryptographic algorithms were implemented using Java programming language in the same programming environment.

Each algorithm consists of three phases: key generation, encryption, and decryption. The Java program for each algorithm took as individual inputs for five different text data, and the sizes of text data vary from each other. The scheme that was followed in the simulation is the time and efficiency of each algorithm.

Paper 2: Database Security in Private Database Clouds

In this paper, we present multiple database security solutions in private cloud computing and managing high volumes of log data. In our proposed system we enhance Info Fence for securing databases in private cloud systems. Oracle database in a centralized server is used in this system for managing database security and generating reports of audit logs. Our proposed model supports as many databases as needed when there are enough resources (CPU, RAM, Storage, and Network Bandwidth) on a centralized server. That is, our solution is not limited by a number of databases.

The proposed model is designed for multi-database environments. It is expected to work well in all versions of Oracle databases and it is scalable to very big databases. However, analyzing the performance of the proposed model in multi databases and big data database environments has not been done but we consider that a future study. Designing our proposed model with other types of DBMSs (i.e., SQL Server, IBM DB2) and using encrypted logs with timestamps in our solution can be another future research topic

Paper 3: Algorithmic and High-Frequency Trading Strategies. A Literature Review

In this module, Owner creates a file and uploads the file onto the cloud. The details required for registering are Email id, password, name, and mobile no. The owner is responsible for giving permission to the new user as permitted for downloading data for use also the owner is able to see the list of users under him. The owner can generate his keys for the encryption and decryption of a file while storing it in the cloud. While storing the file on the cloud it is stored in the form of blocks, as the operations are going to be performed on the dynamic data therefore it will give better results in case of data integrity issues for finding violated part of the data

Here the analysis is done on the basis of encryption and decryption time and hash calculation time. The cipher text obtained here is in the form of digits. Tables I to III are showing comparative analysis for key sizes of 128,512 and 1024 bits. The time required for computation.

comparative analysis for a key size of 128,512 and 1024 bits. The time required for computation for gaining encrypted and decrypted text is much more in 1024 than 512 bits size and 512 bits size takes much more time to calculate the three parameters than 128 bits size.

The result analysis is shown between the original file having 300kb size and its single division block where the original file gives greater encryption and decryption time as compared to the single division block where the key size used is 512 bits. The hash calculation time and file size after encryption for the single division block is lesser compared to the original file

And they found the Use of the homomorphic encryption technique is giving feature of data integrity against chosen plain text on the data over the cloud. Homomorphic cryptographic algorithms have the property of performing the operations on the encrypted data where it saves time by not decrypting the encrypted data each time. The use of the Paillier algorithm which is a probabilistic algorithm has also obtained the objectives of obtaining data integrity and security in this implementation.

Paper 4: An Enhanced Hybrid Data Security Algorithm for Cl

Cryptographic data Encryption is one of the solutions secure data in cloud computing platforms here are symmetric (e.g. DES, AES) asymmetric (e.g. RSA, EIGamal, ECC), Digital Signature (MD5, SHA) algorithms are present and the combination of these algorithms forms hybrid data security cryptographic algorithm. Here proposing a combination of ECDSA, SHA256, and AES is used for sending and receiving data messages on the cloud.

The study of the cryptographic application of data encryption and decryption algorithm in cloud computing security is analyzed and challenges are identified in cloud data security the proposed algorithm will enhance the security of cloud data. The different message size data security is to be analyzed using this algorithm. The handling of large message sizes may a disadvantage.

In this paper, we have analyzed the data security issues faced by users' private data in the cloud system. Data security can be very well enhanced by the use of the proposed hybrid data security cryptographic algorithm but the massive amount of data in cloud computing put a hindrance to the idea. We will be using the SHA256 hashing algorithm along with the AES data encryption algorithms for the verification process and confidentiality and integrity should be maintained in the cloud. user's private data in the cloud system. Data security can be very well enhanced by the use of the proposed hybrid data security cryptographic algorithm but the massive amount of data in cloud computing put a hindrance to the idea.

We will be using the SHA256 hashing algorithm along with the AES data encryption algorithms for the verification process and confidentiality and integrity should be maintained in the cloud. In the future, the comparisons of different hybrid cryptographic algorithms for data security in the cloud performed, and efficiency analysis of different large file sizes with these algorithms.

Paper 5: An efficient architecture and algorithm for server provisioning in Cloud computing using clustering approach

Cloud Computing is a very efficient technology when resources are distributed according to thuser's/clients' requirements, It maintains stability and scalability play a main task in a complex cloud system because the workload and requests of users are unpredictable. The ability of the node will be varying according to the requirement of hardware and software resources. Load balancing for each cluster to recover the scalability and time complexity. There is less delay in service provisioning due to the expansion of the local networks and easy load distribution over more number of available servers, Fog Cluster is the intermediate layer between End users and cloud servers, which is near close to the end user. The Fog network nodes can effectively be used for data forward and give responses to the client in less time. The Fog Servers containing the replicas and records of the required data can help reduce transaction failures and sustain the Quality of Services to the users.

Here they proposed a basic architecture for load balancing in the network and the Cloud servers using Fog servers. In the Dynamic load balancing approach, there is a single node that maintains a queue and contains the information of heavyweight processes and lightweight processes. Though at rest there is a limitation in that it consumes more time to find the nearest server for transferring the load when the server is overloaded.

And they finally concluded that the Improved Model has been articulated for dynamics distributed computing systems in the perspective of load balancing. Primarily the centralized model was used for the load balancing in a distributed environment. This technique used only a queue to maintain the load balances the of system. Proposed architecture one on two Phases: Interaction between Users and Fog Server shows in First Phase, Fog and Cloud Server in nest segment. This phase occurs only if the Fog Server fails to serve the users with the data requested.

Both phases can happen in sequence depending on server load and data availability. Next The next takes place win in case the requested data and resources go missing in the entire Fog tier. In case of failure, the request will be forwarded to a nearby Cloud server (in the Cloud tier) from the particular Fog server handling the data request in the Fog. So, the new dynamic load balancing technique achieves higher success.

Paper 6: An efficient algorithm for data security in cloud storage.

Cloud computing is a “new” computer model that allows using remote services through a network using various resources. It is basically meant to give maximum with the minimum resources. the user end is having the minimum hardware requirement but is using the maximum capability of computing. This is possible only through this technology which requires and utilizes its resources in the best way. Cloud Computing provides IT services as on-demand services, accessible from anywhere, anytime, and by an authorized user. The following figure (fig 1) shows a cloud computing map. This map presents cloud layers, models, and essential characteristics.

The security of the information acquisition rate may be improved. it absolutely was vital to live and store variables exploitation the borderline quantity of your time doable to allow time to ascertain communications with the association between the hardware and therefore the knowledge acquisition web platform. this could be adequate low to attenuate any vital loss of information that might compromise the system's ability to watch.

Although Cloud storage has many advantages; there are still many actual problems concerning security that need to be solved. If we can eliminate or master this weakness of security, the future is going to be Cloud storage solutions for large as well as small companies.

In this article we have presented the different vulnerabilities related to cloud computing, we have also proposed a solution to improve the security of the storage of data, data security is provided by implementing our algorithm. Only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally if he captures the data, he can't decrypt it and needs two keys coming from two different locations. In the next papers, we will try to offer solutions to protect against DDOS attacks in cloud computing.

Paper 7: Providing security, integrity, and authentication using ECC algorithm in the cloud

Cloud computing is well-defined by the National Institute of Standards and Technology (NIST) It is a computing facilities provision ideal for where simulated resources are delivered a facility above the Internet and animatedly scalable. Cloud is ideal for allowing useful, on-demand network access to a communal pond of the configurable cloud resources (for example applications, storage, services, and, servers) that can be quickly delivered and unconfined with nominal managing exertion or facility supplier contact”. Cloud computing defined and reference designs are definite in NIST publication. NIST has proposed an allusion cloud

computing classic composed of four deployment models and three service models.

Amount of work of the customer and provide security integrity and authentication in an effectual way. As the data is not physically obtainable to the user the cloud should deliver the user a method to check for integrity. We delivered a method that gives evidence of the integrity of data in the cloud which the client employs to check the accuracy of user data in the cloud. To secure the cloud resources and protected the behaviors and storage "of databases the Cloud provider" Three Security goals of the data comprise points namely: Confidentiality, Integrity, and Availability (CIA). Data Privacy in the cloud is achieved by Decryption/encryption process.

Cloud computing is a model for providing IT facilities in which assets are regained from the internet over web-based applications and tools, sooner than a direct linking to a server. In this paper We save our data in the cloud storage using authentication and also provide security and integrity checking for our data to verify and also use Electronic Curve Cryptography algorithm for security in this way that it uses a reduced amount of processing time and CPU Power and also provide an efficient method for clients use small device like PDA and Mobile etc.

Paper 8:Comparative study of different cryptographic algorithms for data security cloud

Cloud computing is the recent trend for the growth in the IT industry. We are able to store any amount of data on the cloud today whether it is text, image, audio, video and many more. Storing data on cloud is easy but it is very important that the data which we store on store is also secure. Many cryptographic algorithms have been implemented to maintain the privacy of data over cloud. In this paper, we will make a comparative analysis of various cryptographic algorithms used over cloud to secure data. This analysis will be made using various performance metric to customers especially for storing data. Sensitive data are prone to be more vulnerable. It is important that sensitive data should be stored confidentially. So, the security of data is the most essential and crucial aspect. Security can be achieved by applying cryptographic algorithms.

The most important aspect of the algorithm depends upon to block size input key size used. Comparative analysis using different parameters of various cryptographic algorithms used to secure data over the cloud was made to identify the pros and cons.

Paper 9: Private Cloud Security : Secured user Authentication by using Enhanced Hybrid

Cloud computing is one of the emerging technologies in the last decade; this technology provides a service model to organizations and public users. Organization users and developers, start and maintain their organization without any hardware

and software infrastructure they can develop their company with the help of cloud technology. Cloud deployment is categorized into three types, private, public, and hybrid cloud environments here public and private clouds are more secure comparatively hybrid cloud because when data is moving from private to public cloud security problems is occurring. Data communication is the most important task in a network environment so the proposed model

is focused on data security in a hybrid cloud environment. In a hybrid cloud, the participation of the private cloud and its nodes is very important after that the data transmission depends on the active node, In this, node selection is based on an a genetic algorithm. The result of the proposed model is going to compare with private and public cloud security parameters.

The proposed secure hybrid cloud environment was constructed using the VMT technique and the hybrid cloud is developed in Amazon's public cloud, within AWS EC2 the private cloud setup OpenStack was implemented. Compute, storage and infrastructure are actively working in the invented model. The model is compared with private and public cloud security parameters and finally the proposed work is more efficient than the existing model. Here the security parameter like data classification, authentication code, and cryptographic technique is evaluated with different work-loads in a proposed hybrid cloud model. The developed hybrid cloud model satisfies all the parameters in a real-time process and it works efficiently.

The genetic algorithm is a heuristic technique that is used to solve search and optimization problems using bio-inspired operators such as selection mutation, cross-over, and termination. This algorithm is an iterative approach that involves the population of candidate solutions in each iteration called generation. An algorithm is said to be genetic, If it is a solution domain That has a genetic representation and a fitness function to evaluate it. The genetic algorithm involves four different stages which are repetitively applied to improve the solution.

Paper 10: Hybrid Cuckoo search - ABC algorithm based vulnerabilities mapping clouds

In this there is a level of abstraction between the infrastructure level and the application user /owner of the information being stored and processed. Such indirect control of recourses / infrastructure environment (storage) introduces vulnerabilities which was unaware in previous settings , So we should concentrate on levels security like portability; governance; interoperability; business

continuity; disaster recovery; data center operations; incident reporting and response; application security; identity and access management; encryption and key management. The objective of the paper is to propose a cloud security framework and an approach for vulnerabilities coverage and cost optimization using Hybrid Cuckoo search - Artificial Bee Colony optimization algorithm and Artificial Bee Colony optimization algorithm. The objective is to mitigate an

identified set of vulnerabilities using a selected set of techniques when minimizing cost and maximizing coverage.

This paper presents compression between ABC and hybrid cuckoo-ABC search(HC-ABC) optimization algorithm which can search best Virtual machine for various vulnerability solutions on Cloud computing, keeping bandwidth constant, Cloud computing needs to be operated in a stable system. Therefore, between HCS-ABC algorithm and ABC algorithm, HCS-ABC algorithm is suitable for Cloud computing environment because it converge maximum vulnerability solutions

Paper 11: Improve data security in a cloud environment by LDAP and two-way encryption algorithm

Cloud computing means distributing computer resources over the network with facilitation of the internet. Cloud computing is very powerful concept and proffer some services the consumers. There are many advantages of cloud computing for consumers because of thservice have on-demand or what you can use pay for that services. Now contemporary year cloud computing has been an up-and-coming computing model in the information technology sectors. It must transmit bulky amount of data to large cloud storage. For safe and sound transmission of critical information in insecure network of cloud computing, encryption of vital information is very important tactic. With the help of encryption we can thwart our data from unauthorized access during transmission.

The data stored without compression in the cloud which lead to large space utilization elucidation for that minimize utilization cloud storage by using compression algorithm. The main problem in cloud computing is security of consumer's significant data. In this paper we provide new security architecture with Lightweight Directory Access Protocol and proposed system contribution is a security architecture that provides a flexible security model with Data compression algorithm and two way encryption algorithm.

Paper 12: Computer-aided system theory.

The concept of CAST as Computer Aided Systems Theory was introduced by Franz Pichler of Linz in the late 80s to name computer theoretical and practical tools for problems in System Science. It was thought as the third component (the other two being CAD and CAM) will provide for a complete picture of the path from

Computer and Systems Sciences to practical developments in Science and Engineering. Franz Pichler organized in the University of Linz the first CAST workshop in April 1988, which demonstrated the acceptance of the concepts by the scientific and technical community. Next, Roberto Moreno-Díaz, of the University of Las Palmas de Gran Canaria joined Franz Pichler, motivated and encouraged by Werner Schimanovich, of the University of Vienna (present Honorary Chairman of

Eurocast), and they organized the first international meeting on CAST, (Las Palmas February 1989), under the name EUROCAST'89 that again proved to be a very successful gathering of systems theorists, computer scientists and engineers from most of the European countries, North America and Japan.

Paper 13: An algorithmic approach to improving cloud security: The MIST and Malachi Algorithm.

Cloud Computing is ever-increasing in popularity in the computer science field. Because of this increased usage, the importance of data integrity and strong security has become paramount. This paper expounds upon security measures and methodologies for strengthening the cloud, including two new security algorithms.

According to the Cloud Security Alliance paper, "The Notorious Nine: Cloud Computing Top Threats 2013", the nine biggest threats to cloud computing are data breaches, data loss, account or service traffic hijacking, insecure interfaces and Application Programming Interfaces (APIs), denial of service, malicious insiders, abuse of cloud services, insufficient due diligence, and finally shared technology vulnerabilities [1]. All nine of these issues would be lessened by properly implementing stricter security on cloud systems. A combination of security measures in concurrence is the basis of the security improvements asserted forthwith. The security algorithms introduced in this paper, the MIST and Malachi are two new ways to protect users .

Paper 14: A Framework for Cloud Data Security.

The execution is performed on a machine with Intel core 2 Duo, 2.4 GHz processor with 4 GB of memory and 500 GB of hard disk which runs Ubuntu 10.04. Three different sized files are taken as an input to the system to perform a comparison based on storage space required for storing a particular file . Its benefits over conventional computing infrastructure would encourage all organizations partially or entirely migrate their processes and data to the Cloud. Considerable effort will be put in place to provide the appropriate security measures to make business on cloud environments. The client-side security of data is as important as the server side security. User must secure their data before storing it in the cloud. This report

provides an approach for securing data before storing it in the cloud as well as reducing the amount of storage space required. However, the management of key needs to be more secure. If the authentication details are hacked, the document

can be hacked, which can be seen as one of the future work, also the entire process of compression and encryption will become sluggish as the size of file increases. The performance will degrade. So, there is need of parallel encryption on data for faster processing.

Paper 15: Enhancing the security of user data using keyword encryption and hybrid cryptographic Algorithm in the cloud.

In this The objective of the proposed work is to improve the security of outsourced data in cloud computing. This is achieved by the efficient hybrid encryption and proxy Re-encryption. The data of the cloud user is encrypted before storing them in cloud storage. In this work the encryption is performed in two phases, In the first the user data is encrypted along with receiver identity. In the second phase the identity (user name, IP address, email id) and the keyword *(Ordinary, secret* and *top secret)* is encrypted using PRE. Finally these two ciphertext is combined and send to the cloud server. The receiver obtains the original message with the private key matching to the identity. This scheme ensures the security of user data and result describes the efficiency of this work.

This paper proposed an identity-based hybrid encryption method (RSA with ECC) [7] [8] for the outsourced computation of encrypted information in cloud computing. The identity-based encryption is combined with hybrid RSA with ECC to encrypt the user data. In standardization to improve security proxy re encryption is utilized to encrypt the user identity and keyword. RSA is a popular encryption technique used to secure data. The encryption techniques such as ECC and proxy re-encryption are also powerful mechanisms to secure the from adversary section describes some related work that uses the above-mentioned encryption algorithm to provide security for user data.

Paper 16: SEED: Enabling serverless and efficient encrypted deduplication for cloud

In this Cloud storage offers ubiquitous file-sharing and backup services to users with abundant storage resources. As cloud storage service such as Google Drive Dropbox and Mozy are getting popular, it is crucial for cloud storage providers (CSPs) to minimize costs of storing outsourced data. Data deduplication, a technique that eliminates data redundancy, can achieve this goal and save more than 90% of resources such as disk space or network bandwidth . The primary security goal of SEED is to protect the confidentiality of users' data in the cloud storage. In our threat model, a CSP is no longer fully trusted even if it is honest. Therefore, information about data should be maintained secret from any adversaries including the CSP and even unauthorized users who have no valid ownership. Since our threat model considers various attacks from inside and outside adversary, we analyze data confidentiality with regard to these attack scenarios. In the analysis, we assume that all public information including the public keys of users are known a priori to the adversaries.

In this paper, they proposed SEED, a novel scheme for serverless and efficient encrypted deduplication. The novelty of SEED is originated from its efficiency enabled by non-interactive file encryption as well as support of lazy encryption. By rigorously analyzing the security of SEED, we showed that even without aid of key servers, the proposed scheme guarantees strong data confidentiality that resists against brute-force attacks, as well as data integrity. We also conducted extensive comparative analysis and performance evaluations. By doing so, it was shown that SEED has advantages in terms of efficiency and security compared to previously proposed schemes. Despite its novelty, however, SEED has a limitation that huge computational burden at server-side is inevitable when running deduplication algorithm. As future work, we will extend our research to optimizing the deduplication algorithm: relieving its computing complexity and minimizing memory access by using Bloom filters.

Paper 17: Designing and analysis of user profiling system for cloud computing security using fuzzy

This paper is the based on the findings from our last paper, where we had found that the designing of User Profiling System based on Artificial Intelligence techniques: Fuzzy and Genetic Algorithms are individually not sufficient to deliver a comprehensive User Profiling System but it might be possible to use these two approaches in a hybrid way to design a comprehensive User Profiling System for Cloud Computing security. Hence, we used hybrid approach Fuzzy guided Genetic Algorithm to design a User Profiling System and found that it covered all the research gaps, which we had analyzed in our previous work and even it fulfill all the seven principles of the evaluating framework. In this paper, we have focused on these research gaps and propose a new hybrid approach to design a User Profiling System, which is evaluated on the same reference model [12] and proved it's comprehensibility in context of designing a User Profiling System for Cloud Computing security. They evaluated experiments on seven principles identified for building a Cloud Computing security risk indicator system [12], which evaluates the integrity and reliability of a security system

Paper 18: Cloud Computing and emerging IT platforms: Vision hype and reality for delivering computing as the 5th utility.

This paper discusses the current trends in the space of Cloud computing and presents candidates for future enhancements of this technology. This paper is primarily divided into two parts. The first part examines current research issues and developments by:

- presenting the 21st-century vision of computing and describing various computing paradigms that have promised or are promising to deliver this grand vision (Section 2),

- differentiating Cloud computing from two other widely explored computing paradigms: Cluster computing and Grid computing.

- focusing on VM-centric Cloud services and presenting an architecture for creating market-oriented Clouds using VMs.

- Provide insights on market-based resource management strategies that encompass both customer-driven service management and computational risk management to sustain SLA-oriented resource allocation.

  Cloud computing is a new and promising paradigm delivering IT services as computing utilities. As Clouds are designed to provide services to external users, providers need to be compensated for sharing their resources and capabilities. In this paper, we have proposed architecture for market-oriented allocation of resources within Clouds. We have also presented a vision for the creation of global Cloud exchange for trading services. Moreover, we have discussed some representative platforms for.

Paper 19: Cloud Computing and grid computing 360-degree compared

This paper strives to compare and contrast cloud computing with grid computing from various angles and give insights into the essential characteristics of both. Cloud computing has become another buzzword after Web 2.0. However, there are dozens of different definitions for cloud computing and there seems to be no consensus on what a cloud is. On the other hand, cloud computing is not a completely new concept; it has intricate connection to the relatively new but thirteen-year established grid computing paradigm, and other relevant technologies such as utility computing, cluster computing, and distributed systems in general.

In this paper, we show that Clouds and Grids share a lot commonality in their vision, architecture and technology, but they also differ in various aspects such as security, programming model, business model, compute model, data model, applications, and abstractions. We also identify challenges and opportunities in both fields. We believe a close comparison such as this can help the two communities understand, share and evolve infrastructure and technology within and across, and accelerate Cloud Computing from early prototypes to production systems.

Paper 20: Top Threats to Cloud Computing.

The threats are not listed in any order of severity. Our advisory committee did evaluate the threats and each committee member provided a subjective ranking of the threats. The exercise helped validate that our threat listing reflected the critical threat concerns of the industry, however the cumulative ranking did not create a compelling case for a published ordered ranking, and it is our feeling that greater industry participation is required to take this step. The only threat receiving a consistently lower ranking was Unknown Risk Profile, however the commentary indicated that this is an important issue that is simply more difficult to articulate, so we decided to retain this threat and seek to further clarify it in future editions of the report.

When adopting a cloud service, the features and functionality may be well advertised, but what about details or compliance with the internal security procedures, configuration hardening, patching, auditing, and logging? How are your data and related logs stored and who has access to them? What information if any will the vendor disclose in the event of a security incident? Often such questions are not clearly answered or are overlooked, leaving customers with an unknown risk profile that may include serious threats.

Chapter 3

Experimental setup and Methodology

According to the cloud computing environment, security for cloud users' data is the main concern. For that several existing cryptographic security algorithms are used to offer high-level security to cloud user data.

3.1 Terminology related to cryptography and security algorithms

3.1.1 Plaintext: It is the original message or data or file given as input to the security algorithms.

3.1.2 Cipher text: It is the converted message which is generated as output from security algorithm.

3.1.3 Encryption: It the process to convert Plaintext in to Cipher text.

3.1.4 Decryption: It is the process to convert Cipher text back to the Plaintext.

3.1.5 Key: A key is either number or combination of number, text and symbol. which is used with plaintext at encryption side and used with cipher text at decryption side.

3.1.6 Key Size: It is the measure in terms of length of the key in bits used in any type of algorithm for encryption and decryption.

3.1.7 Block Size: In cryptography some key cipher works on string of bits. This string of bits is termed as Block Size. This size is different for different algorithms.

3.1.8 Round: It means the number of times the encryption function is going to be executed to finish encryption process to generate the cipher text as output.

3.2 Classification of Security Algorithms

3.2.1 Symmetric/Private key encryption algorithms: It use a single secret key that is known to the sender and receiver. DES, 3DES, Blowfish, RC6 are some examples of this algorithms.

3.2.2 Asymmetric /Public key encryption algorithms: It use a pair of public and private key for encryption and decryption process. RSA, Diffie-Hellman are some examples of this algorithms.

3.3 Analysis of different cryptographic security algorithms

Here, we did this analysis based on number of bytes processed per second in different algorithms with different number of bits and overall time taken for encryption and decryption. For this we use open ssl and crypto library, 'c' language, intel core i7 processor, ubuntu16.04LTS,2.70GHz CPU. Here, in this Table.1 the numbers are in 1000s of bytes per second processed according to different Block size.

	Different Blocksize		
Algorithm	**Type**	**1024 Bytes**	**8192 Bytes**
des-cbc	Symmetric	81937.75k	81988.27k
3-des-cbc	Symmetric	30506.61k	30426.25k
aes-128-cbc	Symmetric	160358.40k	161316.86k
aes-192-cbc	Symmetric	133035.35k	132554.75k
aes-256-cbc	Symmetric	114224.13k	114559.66k
md-4	Message digest	986857.13k	1140222.63k
md-5	Message digest	593053.70k	690225.15k
sha-1	hashing	832123.90k	973383.78k
sha-256	hashing	417715.88k	441262.08k
sha-512	hashing	568224.09k	657555.46k

Table 3.1

3.4 Proposed model

The proposed Hybrid model is for providing security in cloud environment is a combination of Brotli algorithm for compression, RSA and SHA-3 algorithm for hashing.

3.5 Brotli Algorithm for compression

This algorithm is a combination of Huffman coding, second order context modelling, LZ77 lossless compression algorithm. Unlike most general purpose compression algorithms, Compression ratio of Brotli is high and it uses a pre-defined 120 kilobyte dictionary containing 13000 common words, phrases and other substrings derived from a large corpus of text and HTML documents, in addition to the dynamically populated/sliding window dictionary. Here, we are using Brotli Algorithm for compression of our data because it is much faster as compare to other compression algorithms and after compression it also reduces the size of original data to the great extent. Thus, here we first compress our data with Brotli Algorithm and then perform the encryption. The Brotli Algorithm for compression of our data because it is much faster as compare to other compression algorithms and after compression it also reduces the size of original data to a great extent. This helps in reducing the space and additionally helps in the quick retrieval of data.

3.6 SHA-3

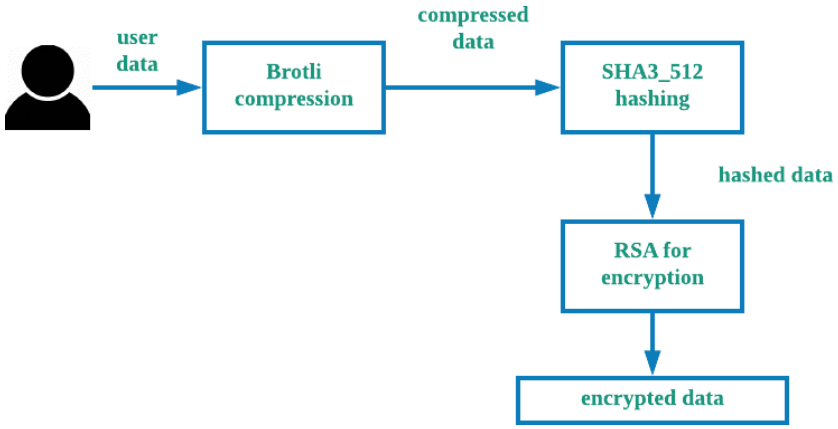
SHA-3 gives out the usage of sponge construction, in which the input is given in as variable size and the output is brought out as fixed size. When the input is taken, it is XORed and transformed as a whole by permutation function. The output is read from the same subset of the state, alternated with state transformation function. Here, we use SHA-3 for hashing because it is faster for hardware implementation and also more time to crack as compare to other algorithms. RSA(Ron Rivest, Adi Shamir, Leonard Adleman) RSA is an asymmetric cryptography which is based on prime numbers. Private key generated is using the prime numbers. Encryption strength is based on the key size. Due to large prime numbers it is not easy to break the RSA without good knowledge of prime numbers and also it takes many years to break it by generating different large prime numbers and testing it. Steps involved in RSA:

I. Select two different large random prime numbers p and q.

II. Then, Calculate n = p*q where, n=modulus for the public key and private keys. I

III. Now, Calculate the quotinent, Ø(n) = (p-1) (q-1).

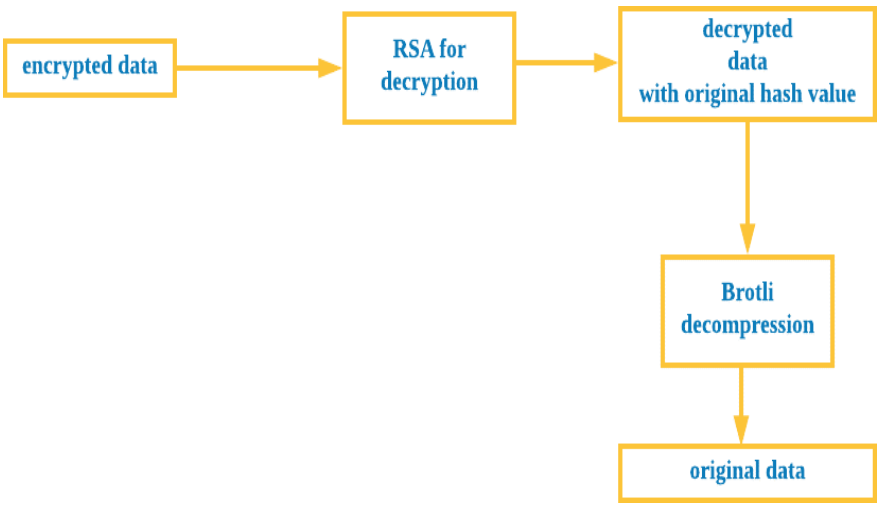
IV. Choose an integer ‘e’ such that, 1<e



3.1 Figure(ENCRYPTION)

STEPS

- Get the input data and compress it using Brotli compression
- Apply hash function SHA-3
- The hashed data is now encrypted using RSA encryption



3.2 Figure(DECRYPTION)

STEPS

- RSA decryption function is applied to the encrypted data
- The data that is retrieved in the above step is verified by applying hash function
- Now the compressed data is decompressed using Brotli decompression and the original data is obtained.

Chapter 4
Future work and conclusion

The designed hybrid model allows the humongous data stored in the cloud to be secure after the implementation of the hybrid algorithm. The RSA is done with the compressed message instead the plain text itself, it needs less time and gives out a reliable approach. RSA has higher security level and takes lower time for verification. In the proposed approach further when the original message is hashed to verify the integrity of the message. The efficiency of the hybrid algorithm brought out is that, the combined algorithms are the best at its time complexity which provides an extra advantage in terms of security.

The proposed system allows users to send and receive data between mobile and cloud in a secure manner without facing the problem of data attack. The proposed system demonstrates that the use of hybrid algorithms increases the level of encryption of encrypted mobile data and also reduces the time required for encryption and decryption.

.

References

[1] R. S. Cordova, R. L. R. Maata, A. S. Halibas, and R. Al-azawi, "Comparative Analysis on the Performance of Selected Security Algorithms in Cloud Computing," pp. 4–7, 2017.

[2] O. Cinar, R. H. Guncer, and A. Yazici, "Database Security in Private Database Clouds," ICISS 2016 - 2016 Int. Conf. Inf. Sci. Secur., 2017.

[3] S. Sawant, "Towards Privacy Preserving for Dynamic Data in Cloud Storage," 2017 Int. Conf. Energy, Commun. Data Anal. Soft Comput., pp. 296–299, 2017.

[4] V. K. Soman, "An Enhanced hybrid Data Security Algorithm for Cloud," no. July, pp. 421–424, 2017.

[5] A. Dixit, A. K. Yadav, and S. Kumar, "An efficient architecture and algorithm for server provisioning in Cloud computing using clustering approach," 2016 Int. Conf. Syst. Model. Adv. Res. Trends, pp. 260–266, 2016.

[6] A. Azougaghe, Z. Kartit, M. Hedaboui, M. Belkasmi, and M. E. L. Marraki, "An efficient algorithm for data security in cloud storage."

[7] A. Bansal and A. Agrawal, "Providing security, integrity and authentication using ECC algorithm in cloud storage," 2017 Int. Conf. Comput. Commun. Informatics, ICCCI 2017, 2017.

[8] P. Semwal and M. K. Sharma, "Comparative study of different cryptographic algorithms for data security in cloud computing," 2017 3rd Int. Conf. Adv. Comput. Autom., pp. 1–7, 2017.

[9] N. Gajra, S. S. Khan, and P. Rane, "Private Cloud Security : Secured user Authentication by using Enhanced Hybrid Algorithm," Int. Conf. Adv. Commun. Comput. Technol. Priv., 2014.

[10] K. Dfhg, "&kdoohqjhv)dfhg %\ &orxg &rpsxwlqj," pp. 50–56, 2017.

[11] S. K. Prashanth, N. S. Rao, and C. S. Kumar, "Hybrid Cuckoo search - ABC algorithm based vulnerabilities mapping and security in clouds," Int. Conf. Electr. Electron. Optim. Tech. ICEEOT 2016, pp. 2569–2572, 2016.

[12] K. V Raipurkar and A. V Deorankar, "Improve data security in cloud environment by using LDAP and two way encryption algorithm," Colossal Data Anal. Netw. (CDAN), Symp., pp. 1–4, 2016.

[13] Q. D. O. Vlv et al., "$qdo\vlv ri 6hfxulw\ $ojrulwkpv lq &orxg &rpsxwlqj," pp. 106– 108, 2016.

[14] J. Lejeune, C. Tunstall, K. P. Yang, and I. Alkadi, "An algorithmic approach to improving cloud security: The MIST and Malachi algorithms," IEEE Aerosp. Conf. Proc., vol. 2016–June, 2016.

[15] A. Grover, "A Framework for Cloud Data Security," pp. 1199–1203, 2016.

[16] G. P. Kanna and V. Vasudevan, "Enhancing the security of user data using the keyword encryption and hybrid cryptographic algorithm in cloud," Int. Conf. Electr. Electron. Optim. Tech. ICEEOT 2016, pp. 3688–3693, 2016.

[17] Y. Shin, D. Koo, J. Yun, and J. Hur, "SEED: Enabling serverless and efficient encrypted

deduplication for cloud storage," Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom, pp. 482–487, 2017.

[18] Sahil, S. K. Sood, S. Mehmi, and S. Dogra, "Designing and analysis of user profiling system for cloud computing security using fuzzy guided genetic algorithm," 2016 Int. Conf. Comput. Commun. Autom., pp. 724–731, 201

.