International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1604-1616 www.ijaem.net ISSN: 2395-5252

A Comparative Study of Cryptographic Algorithms in Cloud Computing Security

Umesh Gunwantrao Deshmukh, Dr. Hemant S. Mahalle
PhD Scholar At JJT University, Rajasthan
Principal Shri V R College,Sawana
Tq. Mahagaon Dist. Yavatmal, Maharashtra

Submitted: 25-06-2021 Revised: 07-07-2021 Accepted: 10-07-2021

ABSTRACT: Cloud security generally refers to the steps taken to secure the electronic storage of digital assets and data by cloud service providers. A wide variety of applications are available from cloud service providers to artistic, industrial, information storage, and back-up, education, entertainment, management, social networking, etc. The protection of online storage data from robbery, leak and deletion by cloud storage platforms is the cloud security. Cloud computing offers a range of internet-based services, including data storage, servers and databases, networking and applications. This article presents the cryptographic algorithms used to solve data protection issues in the cloud. The main contribution of this work is the comparative study of encryption and decryption algorithms. This study will help the cloud system provide greater protection for noisy storage using encryption and decryption algorithms.

Keywords: Cloud Computing, Cryptography, Encryption, Decryption, Symmetric Key, Asymmetric Key, Cloud Security.

I. INTRODUCTION

Cloud computing is a new area in computer science and a recent advancement in IT that moves data from mobile and compact personal computers to large data centers. The primary benefit is that customers will not be able to pay for the equipment, installation, and staff required to operate the equipment and repair.Cloud computing[1] is simpler than other computing models; there are no maintenance costs since the cloud provider is responsible for resource availability, and users are free of the issues associated with maintaining and managing resource machines.Cloud computing is also known as utility computing or "IT on demand" because of this function.Uses a virtualized environment to delegate resources to cloud providers. Cloud computing is constantly changing the way companies operate. It provides a new way of promoting communication and access to information across large geographic distances, along with reducing overhead and associated resource maintenance.

Cloud Computing is becoming increasingly popular every day. Cloud Computing is a paradigm that allows user-friendly on-demand network access to computer resources. There are many cloud computing services and features, but Cloud security is one of the best features in cloud computing [2]. Cloud security [3-5], also known as cloud computing security, consists of a collection of policies, controls, procedures and technologies that work together to secure cloud services, data and infrastructure. The data is stored within the storage devices, which cannot be hacked and utilized by any other person. The storage service is fast and secure.Cloud security consists of data safety, software and cloud computing infrastructures.High-level security concerns, such as unauthorized data exposure and leaks, weak access controls, attack susceptibility, and availability disruption, affect both traditional IT and cloud systems.Many aspects of cloud protection, be it public, private, or hybrid, are the same as any IT architecture at the web.

Depending on the nature of the company and the supply venue, Cloud services can be provided in various ways. Different models of cloud deployment [6] include public cloud, hybrid cloud, and private cloud. Users can link to the cloud via web browsers in the public cloud. Users just choose to pay for the time the service is used, i.e. pay-per-use service. This type of cloud is also known as external cloud computing and offers all the advantages of cost savings, skill and easy maintenance. Private cloud is used only when a company or an entity operates the cloud infrastructure. [7]. Private cloud is different from public cloud in two ways. Firstly, the private cloud is typically used by a single business and is not

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1604-1616 www.ijaem.net ISSN: 2395-5252

shared with any other company, and is associated with a private cloud.Second, in private cloud implementation, security is considered tighter than in public cloud. Hybrid cloud [8]is a blend of both public and private cloud architectures and models. The ability to expand a private cloud by using the public cloud services will help to maintain the quality of service levels in the face of significant changes [9].

The numerous cryptography techniques used in cloud computing are presented in this paper. A summary of different types of cryptographic algorithms are addressed in order to secure the cloud network. However, a comparative study of symmetric and asymmetric techniques is the main contribution of this paper. The paper consists mainly of five parts. Section I usually emphasizes the importance of security in cloud computing. Section II presents the literature survey of the work. Section III discussed about cryptography along with various encryption and decryption algorithms used to protect cloud system. Section IV deals with the comparative study of different encryption and decryption algorithms. And finally, Section V ends the document.

II. LITERATURE SURVEY

This literature survey discusses security attacks, problems and their relative behavior in the area of cloud computing.

Sajay et al. [10] suggested a hybrid data protection algorithm using an encryption algorithm.Encryption algorithms are mainly aimed at protecting or storing vast amounts of cloud information. In order to improve cloud protection, this study combines homographic encryption with blowfish encryption [11].

Liu [12] proposed an RRA-CPA stable public-key encryption scheme with an efficient decryption algorithm and short cypher text sizes derived from a one-way function with poor RKA protection and in distinguishability obfuscation.RRA-CPA safe public-key encryption scheme against arbitrarily function from every publicly deniable encryption, and RRA-CCA secure public-key encryption scheme against arbitrarily function from IND-CCA public-key encryption scheme with a hardcore function for arbitrarily associated inputs.

Yang et al. [13] suggested a block-chain access management system known as AuthPrivacyChain to address the issue of unauthorized access to resources through cloud attackers. The user is posted to blockchain all authorization-related transactions.This paper implemented the EOS blockchain model and describes blockchain transactions for access authority and other details. It can fulfil the requirements of confidentiality, honesty, availability, authenticity and transparency and avoid attacks by external users as well as internal management.

Iqbal et al. [14] compile and categorize cloud-based security problems and vulnerabilities in relation to their cloud models. This makes them more concrete and strengthens the way they are evaluated in order to present a successful solution architecture. This study also identifies how service delivery models differ from current business applications, classifies them and addresses the safety issues inherent in these models. Amara et al. [15] concentrate on the security challenges that arise at each layer of the cloud service delivery model, as well as emerging solutions and approaches.Moreover, counter-measures are also given for potential security threats for each cloud model.

Swamy et al. [16] briefly discussed security goals, threats to security, security problems, and possible ways to protect the environment in the Internet of Things. In all applications on the Internet, the application layer plays a significant role.The MQTT application layer is the most common protocol used.Explicitly pick and analyze security threats to the MQTT Application Layer Protocol.There is a comparison of the different application layer protocols and the protocol safety steps. Many problems are considered when choosing a particular protocol due to the lack of universal guidelines for IoT protocols.

Dong et al. [17] introduced the state-of-the-art DDoS attacks in SDN and cloud computing scenarios. In particular, the emphasis is on an overview of SDN and cloud computing architecture. Velliangiri et al. [18] is implementing a DDoS attack detection scheme to detect attacker nodes in the cloud world. The proposed framework adopts an in-depth learning approach to discuss the important knowledge on the cloud platform. The scheme initially generated a log file by checking log information at each cloud node, and from that log information the model extracts several helpful features. The features taken from the log file are advanced and passed through the selection of the feature, which means that the features which meet Bhattacharya minimal distance are passed to the next stage.The selected features are provided for the DDoS attack detection by the proposed TEHO-based DBN deep learner. This work produces TEHO-oriented DBN for DDoS attack detection, and the new TEHO algorithm selects optimum

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1604-1616 www.ijaem.net ISSN: 2395-5252

weights for classification. In the Taylor series, the TEHO algorithm modifies the EHO algorithm. Three datasets are considered for the implementation of the proposed Scheme and the precision, consistency and reminder are evaluated.

Devi et al. [19] have identified some of today's major safety threats. The key objective is the overall defense, cloud analysis, and subsequent attacks on the granular stage. One of these attacks is Honey pot, which is considered and its policy on intrusion is analyzed. The security measures or requirements or architectures that are needed to be solved by hypervisor have been introduced by Rama Krishna and Padmaja Rani [19].This article also poses potential problems with a malicious virtual machine that runs over a hypervisor, including using more resources than VM, stolen sensitive data, the removal of isolation by side channel attacks from VM, and attacks to jeopardise the hypervisor.

MahdaviHezavehi and Rahmani [21] introduced a cloud-based anomaly based DDoS attack detection system using a third party auditor (TPA). Second, the authors include a selection of fundamental assumptions and cloud environment settings for the implementation of simulation testing to assess the framework proposed. The simulation results show that the following advantages are our method of identifying DDoS attacks in CSPs: reliability, because of the low overhead of CSPs for attack detection; speed, because of the short time briefing on an attack by the CSP with respect to the maximum time of response specified under the Service Level Agreement (SLA), and precision, without being misleading positive.

III. CRYPTOGRAPHY

Cryptography [22] is a science that uses mathematical functions to encrypt and decrypt data. One can store or transfer data through an insecure network using cryptography in a manner that cannot be interpreted by anyone but the intended recipient. In simple words, it is known as “the art of secret writing”.The main components of cryptography are discussed below in order to understand the concept in depth.

- Plain Text: The original message written by sender, before being transformed, is called as plaintext.
- Encryption Algorithm: An Encryption algorithm transforms plaintext into cipher text.
- Cipher text: This is the output of plaintext after encryption by encryption algorithm.
- Key: Key is any number(s) or character(s) that is used as an input to encryption or decryption algorithm. Key may be same or different for encryption and decryption process.
- Decryption Algorithm: Decryption algorithm transforms cipher text into plaintext. It is basically reverse of decryption algorithm.

Cryptographic algorithms can be classified as follows [23]:

Symmetric Key Cryptography: The symmetric encryption approach is used to encrypt and decipher electronic information using only one key (secret key).In the decryption process, entities that interact through symmetric encryption have to exchange the key.

Asymmetric Key Cryptography: As shown in table 1, different keys are used for encryption and decryption in asymmetric key cryptography or public key cryptography.There are two types of keys: public and private.The public key is made public, while the private key is held by the recipient.The message is encrypted by the sender using the receiver's public key, and the message is decrypted by the receiver using its private key.

Hybrid Cryptography: A hybrid encryption scheme uses public-key encryption to encrypt a random symmetric key. This symmetric key is used for the message encryption. The receiver uses the public key encryption system to decrypt the symmetric key and uses the recovered symmetric key to decipher the message. Hybrid cryptography is a form of encryption technique which combines two or more techniques of encryption.It employs both asymmetric and symmetric key cryptography.It makes use of the strengths of each form of cryptography. These advantages are speed and defense, respectively.

Table 1. Symmetric vs Asymmetric Cryptography

Characteristics	Symmetric Key Cryptography	Asymmetric Key Cryptography
Key used for Encryption/Decryption	Same key used for both	For encryption one key is used and for decryption another another one.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1604-1616 www.ijaem.net ISSN: 2395-5252

Speed	Fast	Slow
Security	Less Secure	More Secure
Size of resulting encrypted text	Same or less	More than original plain text

3.1 Encryption / Symmetric Key Algorithm

Symmetric encryption [24] is a form of encryption that uses only one key (the secret key) to encrypt and decrypt electronic data. The entities communicating using symmetric encryption must exchange the key in order for it to be used in the decryption process. As shown in Figure 1, the same key is used for encryption and decryption in this form of cryptography.

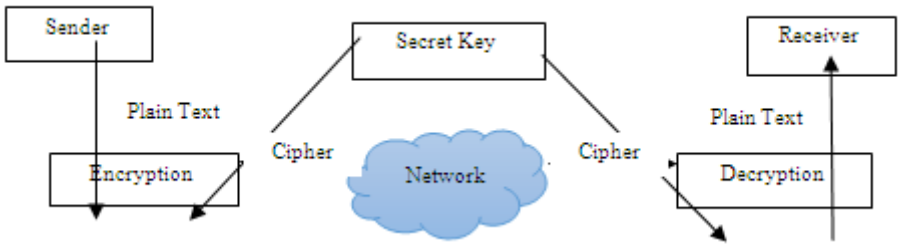

Figure 1. Mechanism of Symmetric Key Cryptography

3.1.1 Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES), formerly known as Rijndael, is the most commonly used symmetric algorithm. It is a symmetrical block cypher that was selected by the United States government to protect classified information.AES [25] is widely used in software and hardware around the world to encrypt sensitive data. It is critical for government information management, cyber security, and the safety of electronic data.It has been discovered at least six times faster than triple DES.AES is made up of three block cyphers: AES-128, AES-192, and AES-256.To encrypt and decrypt a message block, AES-128 uses a 128-bit key length, AES-192 uses a 192-bit key length, and AES-256 uses a 256-bit key length.Using 128, 192, or 256-bit cryptographic keys, each cypher encrypts and decrypts data in 128-bit pieces. AES has the following characteristics:

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

Key sharing is the main problem with AES, which depends on the protected link, and whether that link is compromised by contact. In order to overcome this problem, Farooq and Chawla [26] proposed a novel concept that generates keys for both AES and ECC. Since it inherits the properties of the ECDH algorithm and introduces new concepts for key generation, the algorithm does not require a safe channel at any stage. It is noted that the proposed algorithm generates a 16-byte key that is inheriting the ECC property, so that it can withstand the prime factorization attack and the QC. The key generation algorithm is also less complex than the existing related algorithms.

Chandel et al. [27] suggested a new encryption scheme, AES – CP – IDABE, to protect the privacy of cloud storage data. The data was initially double-encrypted via the ABE, along with the attributes and the user's identity. Secondly, AES is used to encrypt and provide the data for authorized users with encrypted information. A digital signature with the help of user IDs and security keys provides user access control.The configuration also involves the monitoring and control of Denial-of-service (DoS) by IP address. The proposed system was also evaluated for its success in the user-data-holder correspondence and the user running time.

Securing Data and Reducing Time Traffic Using AES Dual Cloud Encryption is done in Sivakumar et al. [28]. HERoku is a multi-layered data encryption cloud platform for processing and deployment. The website application is then run to protect the data. The dual cloud is being used, either one is active or both may function. AES is executed as a data privacy algorithm on the web

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1604-1616 www.ijaem.net ISSN: 2395-5252

page. The advanced table demonstrates that AES encryption can be used to encrypt data and privacy.

Shimbre and Deshpande [29] dealt with some security issues such as fast error tracking, data integrity, and data security. Authors addressed the strategies of third party auditors and hash codes, using these strategies, users are able to receive data assurance in the cloud storage environment. SHA-1 algorithms have been used for this purpose. The proposed design makes it possible for users to check data at low communication and processing costs. Performance and thorough safety analysis show that the proposed systems are effective and highly well organized.

Lee et al. [30] recommended data security under Heroku cloud for cloud computing under AES. Heroku has several stages in its implementation as a cloud platform. The website was then introduced as a data protection program. AES is implemented as a data protection algorithm on the website. Evaluation of performance indicates that AES encryption can be used for purposes of data protection.Besides, delaying the measurement of data encryption shows that the greater data size increases the data delay time for data encryption.

3.1.2 Data Encryption Standard (DES)

The National Institute of Standards and technology has released the Data Encryption Standard (DES), symmetric key block cypher (NIST). The old form of encryption for the data is DES [31]. The symmetric data encryption was identical.In this type of data security, the same key was used for encryption and decryption. This is the Feistel Cipher implementation. It consists of the arrangement of 16 Feistel round. It is 64-bit in block size. Even if the key length is 64-bit, DES has an efficient 56-bit key, as the encryption algorithm does not use 8 of the 64-bit keys.

Sengupta and Chinnasamy [32] suggested the Hybrid DESCAST encryption algorithm, which was designed to provide protection for the large volume of data sent via the media and would remain encrypted in the cloud server. This code is only decrypted if the authenticated user needs to use it. The proposed encryption algorithm has solved DES and CAST block cipher algorithm problems. Complexity and calculation time are greater than the individual DES and CAST Algorithms when the proposed algorithm is encrypted and decrypted. DESCAST is tested on data from the World Bank, Standard & Poor's 500, the Association of Petroleum Exporting Countries (OPEC) and the World Health Organization. In 3 G and 4 G LTE environments the algorithm is available. DESCAST is relatively slow on big data. On big data.

Thnagapandiyan et al. [33] proposed a Modified Elliptic Curve Cryptography (MECC) algorithm to provide privacy for sensitive data. A separate key for all administrators and users to access data is generated in the proposed algorithm.It encrypts and decrypts data with a similar MECC algorithm. If users and other administrators attempt to access cloud data, their identity is checked. After positive verification, requesters are given attributes. The receivers run the MECC algorithm and build a private key to decode your data. This guarantees a high level of cloud encapsulation.

3.1.3 Triple DES

Another DES mode of operation is Triple DES. Three 64-bit keys are required, with a total 192-bit key length. The encryption process is the same as the regular DES, but the term Triple DES has been repeated three times. The first key encrypts the data, with the second key is decrypted and finally the third key is encrypted. Triple DES are much more confident than DES, but run three times slower than single DES encryption.

Fan and Zhao [34] proposed an updated cryptanalysis BP neural network algorithm. The main objective was to simulate the process of DES decryption with a background algorithm. A neural network simulator for the decryption of the target cypher is created by entering a large number of plaintext and ciphertext pairs and decrypting the cypher text.This paper details how the neural background class is changed and how it is used to create a model for regression analysis.

3.1.4 Blowfish

Bruce Schneier invented the Blowfish encryption technique as an alternative to the DES encryption technique in 1993. It is significantly faster than DES and offers a high encryption rate without an efficient, yet developed cryptanalysis technique. It is one of the first secure cyphers which are not patentable and thus free for all to use. The Blowfish algorithm is used in the cloud to identify security and privacy issues.This generates a security key, and for both decryption and encryption a symmetric key block is used.No new user may use a network-accessible file to allow others to access the blow fish key [10].

Park et al. [36] proposed AVX2-optimized Simeck family block cypher implementations that support different numbers of well-performing blocks to ensure the efficiency and availability of

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1604-1616 www.ijaem.net ISSN: 2395-5252

cloud or server-side data encryption. Simeck32/64 has 35417 cycles/byte, while the Simeck64/128 encryption offers the suggested 48-block AVX2-optimized encryption. For powerful large data encryption on the cloud or server side, adaptive encryption based on AVX2-optimized Simeck encryption is also suggested, with a high performance of 4.6146 cycles / byte for 24 blocks.

In order to securely write data and efficiently access control the weighted attribute-based Encryption (BH-WABE) was proposed by Ghosh and Karar [37]. In this case, each attribute is assigned weight based on its value and the data is encrypted using access control guidelines.The cloud service provider retrieves outsourced data and revokes and updates attributes as different weight-based attributes are allocated. The recipient can access the data file corresponding to his weight in order for computational overload to be reduced. The BH-WABE proposed provides collusion resistance, multi-competency security and fine grain access control in confidentiality, trustworthiness and efficiency.In terms of data confidentiality, versatile access monitoring, cooperation with data, complete delegation, partial decryption, authentication and partial signature, performance is contrasted with the traditional hybrid attribute based encryption (HABE) scheme.

Mudepalli et al. [38] proposed effective ciphertext recovery strategies for a large volume of data. Initially, Porter stemming produces an index. The Blowfish algorithm will then be used to encrypt the outsourcing data. For the key generation for approved access is used the public key encryption-based elliptic curve (ECC). When keyword queries are transferred to the cloud, the relevant index contents are scanned and the relevant data is recovered.The algorithm Blowfish Decryption is then used to read the plain text. It offers security against outsourced data and improved productivity with regard to processing and communication costs has been shown in the success of the proposed work.

The new parallel cryptography algorithms that would boost security were suggested by Chauhan and Gupta [39] to fusion and modification of Blowfish and MD5 encryption. Hybrid MD5-Blowfish Cryptographic Calculation is planned to solve the weakness of symmetrical cryptographic block and hash function schemes. On the basis of two parameters, storage and time, the proposed output algorithm is evaluated. The Blowfish-MD5 hybrid execution time is less than the hybrid algorithm RSA-MD5. The simulation results indicate more efficient results in the comparison of parameter output (storage and time). The data is encrypted by generating S-Boxes, as a blowfish algorithm, and its run time is reduced because of its parallel processing. Blowfish-MD5 has therefore been shown to be more efficient than the previous algorithm.

3.2 Decryption / Asymmetric Key Algorithm

The process of changing the cypher text to the plain text of the process is known as decryption. DES [40] works by using the same key, so both the sender and the recipient need to know and use the same private key for their encryption and decryption.Asymmetric [25] is a form of cryptosystem that uses a combination of public key (known to everybody) and private Key for encoding and decryption (Secret Key). It is known as Public Key Encryption.

DES is a block encryption system that encrypts data in 64-bit blocks. This means 64-bit plain text is a DES input that produces 64-bit cypher text. For encryption and decryption, the same algorithm is used, with minor differences.It has a length of 56 bit. DES was developed by Horst Feistel, a 1971 IBM cryptography researcher and was based on the Feistel block cypher known as LUCIFER. DES uses a different key for each round, using sixteen rounds of the Feistel structure.

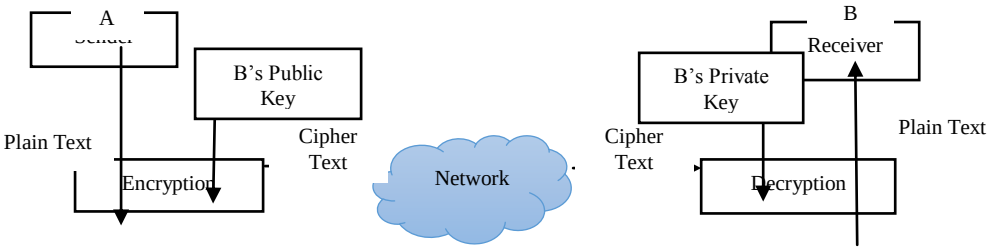

Figure 2. Mechanism of Asymmetric Key Cryptography

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1604-1616 www.ijaem.net ISSN: 2395-5252

3.2.1 Rivest-Shamir-Adleman(RSA)

RSA [41] is an asymmetric algorithm of cryptography.Asymmetric actually means that it runs on two different keys, i.e. Public Key, Private Key. As the name suggests, everybody is given a Public Key and privacy is maintained. RSA is made of the first letters of the surnames of the publisher i.e. "Ron Rivest", "Adi Shamir" and "Leonard Adleman". It was released in 1977.

Ramadan et al. [42] suggested an effective and reliable identity-based encryption scheme based on the premise that the RSA would have an equality test. Evaluation of the performance of the proposed scheme show that one-way defense and selected identity and text (OW-ID-CCA) attacks under DDH assumptions have success and security.

Ambika et al. [43] suggested a scheme that would encrypt the CA key and send it to community users to ensure safe and efficient communication. In this proposed scheme, CA 's key computing time and user key computing time were substantially lessen when compared to GCD, binary tree and MDS methods. The proposed scheme of GCD, binary tree and MDS methods have significantly decreased user key computation. Computational complexity recommends O(n+1) for CA security analysis key encryption and O(n) is proposed to use the security analysis key encryption.

An efficient RSA algorithm is proposed in Raja shree et al. [44] to resolve data integrity issues in the cloud by applying the Cuckoo Search Optimization (CSA) algorithm. This is done by encrypting data and using the RSA cryptosystem generating secret keys to secure data from unauthorised users. The CSA algorithm is used to refine key encryption in order to avoid a brutal force attack.The simulation results demonstrate a faster performance of the proposed algorithm than conventional RSA and Data Encryption Standard (DES) algorithms.The algorithm proposed provides increased performance and increases the algorithm's private key length.

El Makkaaoui et al. [45] presented four integer support schemes for HE encryption, namely the CloudRSA, the MultiPrime Cloud-RSA, the MultiPower Cloud-RSA and the Cloud-ElGamalschemes. The schemesresist more the confidentiality attacks. The multiPrime Cloud-RSA and MultiPower Cloud-RSA versions are stable under the durability of large composite integers and detect decryption exponents in private cases; whereas, when a selected group generator is private, cloud-elGamal system is safe under the durability to remove discrete logarithms over finite groups.

3.2.2 Diffie Hellman Exchange

The Diffie-Hellman key exchange [46] was the first widely used method for securely generating and exchanging keys over an untrustworthy channel.It bears the names of its creators, Whitfield Diffie and Martin Hellman.The Diffie-Hellman algorithm is used to generate a shared password that can be used for secret communications when exchanging data over a public network by using the elliptic curve to generate points and the parameters to obtain the secret key.

The modified cryptogram solution, together with Diffie-Hellman uses the RSA algorithm Reddy et al. [47], to enhance the safety of cloud-based encrypted data. The file is broken down into two to make access to all data difficult, and the split data is encrypted using RSA and Diffie-Hellman until it is stored in two separate cloud accounts. Broken data is then recovered and cypher data restored is decrypted in order to receive the original data.The split process produces no high overheads and ensures data retrievability.As a result, cloud data is more stable, and cloud providers are prohibited from directly accessing cloud data.

Chaudhary and Sharma [48] have studied various algorithms, the Diffie Hellman extended-form genetic algorithm is trying to offer an optimized path by selecting the best path for data transmission without any interruption. It aims to conclude by detecting intruders, which means using the genetic algorithm and extending the Diffie Hellman algorithm, provides the most optimised means of data transmission in a dangerous network before the transmission or data are disrupted.

The new curve and a Diffie-Hellman storage method called EC (DH) 2 was suggested by Kavin and Ganapathy [49]. The simple Diffie-Hellman algorithm is used twice as DH2 and the standard encryption curve algorithm is used for secure storage in cloud-based IoT applications. The experiments were conducted with different sizes of documents and files for assessing the EC (DH) 2 proposed algorithm and have shown improved safety and increased key size.

Talkhaby and Parsamehr [50] suggested a stable method for authentication and distribution of session keys. The Kerberos 5 protocol is chosen for this algorithm.This is one of the most common authentication and key systems for distribution.However, this protocol can attack passwords. The Kerberos 5 is therefore enhanced with the Powerful Diffie-Hellman-DSA key exchange algorithm and the fingerprint samples of

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1604-1616 www.ijaem.net ISSN: 2395-5252

the user. This approach provides a very stable protocol. Using the powerfulDiffie-Hellman-DSA Key Exchange algorithm to overcome the password guessing attack vulnerability.In addition, the use of biometric data is an optional solution that can solve the disadvantage of password-based authentication, such as a user's tendency to choose a simple password.This method is also used in cloud computing systems and uses an improved approach to the security of fingerprint models. Finally, in the last section of this scheme, cloud computing systems can be secured against various attacks.

3.2.3 Homomorphic Algorithm

Homomorphic encryption [51] is a technique of encryption that allows data to remain encrypted throughout processing and handling. It allows you or a third party (such as a cloud provider) to implement encrypted data functions without the need to disclose data values. Homographic encryption offers a new dimension to cloud storage and also provides confidentiality of data, as information is not disclosed in plain text at any stage [10]. A homomorphic cryptosystem is similar to other forms of public encryption in that it encrypts data with a public key and only the individual with the corresponding private key has access to unencrypted data.The most popular use of homomorphic encryption is when the data owner wants to transfer data to the cloud for processing but does not trust the service provider's data.

Jin et al. [52] have created a homomorphic RLWE communication protocol in a cloud based IoT convergence environment for User Authentication and Message Management. The study examined safety and security by conducting a performance analysis of the current IoT communication protocol and the communication protocol proposed.In conjunction with encryption and decoding of the proposed Communication Protocol, the study carried out a comparative review of time complexity and spatial complexity to confirm that it provides a high level of security and equal efficiency.

Key allocation and key organization are two major problems associated with the homomorphic encoding approach. For encoding key generation, the advanced PSO algorithm is implemented in Khan et al. [53]. This key is used to generate encoded data as input to the homomorphic encoding system. For the implementation of the method proposed, MATLAB programming should be used and results examined through resource exploitation and execution time.In comparison with the present homomorphic coding scheme it is evaluated that the extraction and extraction times of the enhanced homomorphic algorithm are small.

Das [54] proposed to use a robust cloud computing model to encrypt the user data followed by data operations while preserving confidentiality and privacy by an efficient crystal technique based on homorphic encryption (HE) and multi-party computer (MPC). The results are the same as if raw data were used to conduct operations.A party can make calculations jointly, without the other party disclosing its data. Here we have designed and installed robust, homomorphic encryption and multiparty computing techniques that have been specially tailored to a private cloud setting. It enables developers, along with the required HE+MPC encryption technologies, to create a private cloud.

Alabdulatif et al. [55] has introduced a groundbreaking Privacy Platform for Cloud-based Distributed Big Data Analytics. Fully Homomorphic Encryption (FHE) is intended to protect the confidentiality of outsourced data stored and processed in the cloud. The Distributed Analytics Approach is proposed,that can be applied to a range of applications distributed. The distributed method improves the scalability of analytical activities to retain a high level of analysis accuracy, while reducing the overall efficiency of encrypted computation.

IV. COMPARATIVE ANALYSIS

This section summarizes and compares all the cryptographic algorithms mentioned in this survey. Tables 2 and 3 include a short summary of the encryption and decryption algorithms used in cloud security, with a focus on their results along with the parameters used in that specific approach.

Table 2. Encryption Algorithms

Encryption Algorithms	Algorithms Employed	Performance Metrics	Findings/ Contribution
AES	AES-ECDH [26] AES-CP-IDABE [27] Time Traffic using AES [28] TPA and AES [29]	• 16-byte key • Encryption/decryption time, execution time • Delay time • Server time, key size,	• Algorithm can operate everywhere whether it is WSN, WBAN, Cloud Computing, Fog

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1604-1616 www.ijaem.net ISSN: 2395-5252

	Data security using AES [30]	token generation • Delay time	Computing or IoT. • AES-CP-IDABE is more effective than ABE over execution, encryption, and decryption time. • Data encryption and privacy AES cryptography can be used. • Highly efficient scheme to collude servers with minimal overhead computation and to attack malicious data alteration. • Delay data encryption calculation shows that greater data size improves data delay time for data encryption.
DES/ Triple DES	Hybrid DESCAST [32] MECC [33] DES + BPNN [34]	• Encryption/ Decryption time • Throughput, Encryption and Decryption time • Mean square error, fitting rate	• Any type of data less than 1 MB can use the DESCAST algorithm. • Modified Elliptic Curve Cryptography provides optimaldata cloud storage security. • Fitting rate is 90% higher than true plaintext.
Blowfish	AVX2-optimized Simeck32/64 encryption [36] BH_WABE [37] Blowfish + ECC[38] Blowfish_MD5[39]	• Encryption time • Throughput, encryption and decryption time • Throughput, encryption and decryption time • Encryption and Decryption time	• Technique balances the load of resulting data and attained 3.5 cycles/byte and 4.6 cycles/byte for Simeck32/64 and Simeck64/128 encryption, respectively. • In terms of safety, reliability, and performance, BH-WABE is efficient. • Better efficiency, low cost and computation time. • Blowfish_MD5 is more efficient than RSA_MD5

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1604-1616 www.ijaem.net ISSN: 2395-5252

Table 3. Decryption Algorithms

Decryption Algorithms	Algorithms Employed	Performance Metrics	Findings/ Contribution
RSA	IBEET-RSA [42] SKT-RSA [43] RSA + Cuckoo Search [44] Cloud-ElGamal + Cloud-RSA + MultiPrime Cloud-RSA + MultiPower Cloud-RSA[45]	• Cost, Encryption/Decryption Time • Computational time • Encryption/ Decryption time, Throughput • Encryption/ Decryption time	• Low computation cost & stable compatibility with WBAN applications • O(n+1) complexity for CA key encryption w.r.t security analysis • Proposed algorithm is faster than traditional RSA and DES algorithm.
Diffie Hellman	RSA + XOR + Diffie Hellman [47] Hybrid Genetic algorithm and extended Diffie-Hellman [48] EC $(DH)^2$[49] Kerberos 5 protocol + Diffie-Hellman-DSA Key Exchange algorithm [50]	• Overhead • Computation time • Size • Encryption/ decryption time	• More secure cloud • No intruders can render the server occupied by this algorithm. • More secure cloud • Security is more than traditional algorithm
Homomorphic	RLWE-based Homomorphic [52] PSO [53] HE + MPC, OAEP [54] FHE [55]	• Time complexity and space complexity • Resource utilization, execution time • Overhead • Accuracy, Euclidean distance	• Secure than RSA and ECC • Better computation time and resource utilization than traditional homomorphic algorithm • Overhead is not more than Homomorphic encryption but beyond multi party computation. • High level of accuracy and reduced overhead

V. CONCLUSION

In cloud cryptography, encryption methods are used to secure information which can be stored or used in the cloud.This allows users to access common cloud services securely and safely as encryption ensures all data hosted by cloud providers.This article is intended to present a summary of the cryptographic schemes practiced in general. In addition to the techniques, it offers some information on the general idea behind the role of protection in cloud computing. The comparative study was presented to help gain insight into the various cloud security encryption and decryption techniques. AES, DES, RSA, Diffie-Hellman, and Homomorphic. Similar studies on cryptographic techniques can provide some valuable insights into potential revisions.Future work consists of machine learning, cloud protection and data deduplication for data security in hybrid clouds. The Improved C4.5 machine learning approach is used to identify users for various access and tasks. The cryptography algorithm used is RSA and the deduplication of data is done using a cosine similarity algorithm.

REFERENCES

[1]. Abbasi, A. A., Abbasi, A., Shamshirband, S., Chronopoulos, A. T., Persico, V.,

&Pescaph, A.,"Software-defined Cloud Computing: A Systematic Review on Latest Trends and Developments," IEEE Access, vol. 7, pp. 93294-93314, Jul. 2019.

[2]. Malik, A., & Om, H., "Cloud Computing and Internet of Things Integration: Architecture, Applications, Issues, and Challenges," Sustainable Cloud and Energy Services, pp. 1–24, Sep. 2017.

[3]. Sun, P. J., "Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges and Solutions," IEEE Access, 2019.

[4]. Ramachandra, G., Iftikhar, M., & Khan, F. A., "A Comprehensive Survey on Security in Cloud Computing," Procedia Computer Science, vol. 110, pp. 465–472, 2017.

[5]. Singh, A., & Chatterjee, K., "Cloud security issues and challenges: A survey," Journal of Network and Computer Applications, vol. 79, pp. 88–115, Feb. 2017.

[6]. Rani, B. K., Rani, B. P., &Babu, A. V., "Cloud Computing and Inter-Clouds – Types, Topologies and Research Issues," Procedia Computer Science, vol. 50, pp. 24–29, 2015.

[7]. Odun-Ayo, I., Ananya, M., Agono, F., &Goddy-Worlu, R., "Cloud Computing Architecture: A Critical Analysis," 2018 18th International Conference on Computational Science and Applications (ICCSA), pp. 1-7, Jul. 2018.

[8]. Alonso-Monsalve, S., García-Carballeira, F., &Calderón, A., "A heterogeneous mobile cloud computing model for hybrid clouds," Future Generation Computer Systems, vol. 87, pp. 651–666, Oct. 2018.

[9]. Khan, N., & Al-Yasiri, A., "Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework," Procedia Computer Science, vol. 94, pp. 485–490, 2016.

[10]. Sajay, K. R., Babu, S. S., &Vijayalakshmi, Y., "Enhancing the security of cloud data using hybrid encryption algorithm," Journal of Ambient Intelligence and Humanized Computing, pp. 1-10, Jul. 2019.

[11]. Altowaijri, S. M., "An Architecture to Improve the Security of Cloud Computing in the Healthcare Sector," EAI/Springer Innovations in Communication and Computing, pp. 249–266, 2019.

[12]. Liu, P., "Public-Key Encryption Secure Against Related Randomness Attacks for Improved End-to-End Security of Cloud/Edge Computing," IEEE Access, vol. 8, pp. 16750-16759, Jan. 2020.

[13]. Yang, C., Tan, L., Shi, N., Xu, B., Cao, Y., & Yu, K., "AuthPrivacyChain: A Blockchain-based Access Control Framework with Privacy Protection in Cloud," IEEE Access, vol. 8, pp. 70604-70615, Apr. 2020.

[14]. Iqbal, S., Kiah, M. L. M., Anuar, N. B., Daghighi, B., Wahab, A. W. A., & Khan, S., "Service delivery models of cloud computing: security issues and open challenges," Security and Communication Networks, vol. 9, no. 17, pp. 4726–4750, 2016.

[15]. Amara, N., Zhiqui, H., & Ali, A., "Cloud Computing Security Threats and Attacks with Their Mitigation Techniques," 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2017.

[16]. Swamy, S. N., Jadhav, D., & Kulkarni, N., "Security threats in the application layer in IOT applications," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017.

[17]. Dong, S., Jain, R., & Abbas, K., "A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments," IEEE Access, vol. 7, pp. 80813-80828, Jun. 2019.

[18]. Velliangiri, S., Karthikeyan, P., &Vinoth Kumar, V., "Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks," Journal of Experimental & Theoretical Artificial Intelligence, pp. 1–20, 2020.

[19]. Devi, B. T., Shitharth, S., &Jabbar, M. A., "An Appraisal over Intrusion Detection Systems in Cloud Computing Security Attacks," 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 722-727, Mar. 2020.

[20]. Rama Krishna, S., &Padmaja Rani, B., "Virtualization Security Issues and Mitigations in Cloud Computing," Proceedings of the First International Conference on Computational Intelligence and Informatics, pp. 117–128, 2016.

[21]. MahdaviHezavehi, S., &Rahmani, R., "An anomaly-based framework for mitigating effects of DDoS attacks using a third party auditor in cloud computing environments," Cluster Computing, 2020.

[22]. Li, Y., Gai, K., Qiu, L., Qiu, M., & Zhao, H., "Intelligent cryptography approach for secure distributed big data storage in cloud computing," Information Sciences, vol. 387, pp. 103–115, 2017.
[23]. Pardeshi, S. R., Pawar, V. J., &Kharat, K. D., "Enhancing information security in cloud computing environment using cryptographic techniques," 2016 International Conference on Communication and Electronics Systems (ICCES), pp. 1-5, Oct. 2016.
[24]. Yassein, M. B., Aljawarneh, S., Qawasmeh, E., Mardini, W., &Khamayseh, Y., "Comprehensive study of symmetric key and asymmetric key encryption algorithms," 2017 International Conference on Engineering and Technology (ICET), Aug. 2017.
[25]. Jayapandian, N., Rahman, A. M. J. M. Z., Radhikadevi, S., &Koushikaa, M., "Enhanced cloud security framework to confirm data security on asymmetric and symmetric key encryption," 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Mar. 2016.
[26]. Farooq, S., & Chawla, P., "A novel approach of asymmetric key generation in symmetric AES via ECDH," International Journal of System Assurance Engineering and Management, vol. 11, pp. 962-971, Aug. 2020.
[27]. Chandel, S., Yang, G., & Chakravarty, S., "AES–CP–IDABE: A Privacy Protection Framework against a DoS Attack in the Cloud Environment with the Access Control Mechanism," Information, vol. 11, no. 8, 372, pp. 1-15, Jul. 2020.
[28]. Sivakumar, P., NandhaKumar, M., Jayaraj, R., & Kumaran, A. S., "Securing Data and Reducing the Time Traffic Using AES Encryption with Dual Cloud," 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN), Mar. 2019.
[29]. Shimbre, N., & Deshpande, P., "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm," 2015 International Conference on Computing Communication Control and Automation, pp. 35-39, Feb. 2015.
[30]. Lee, B.-H., Dewi, E. K., &Wajdi, M. F., "Data security in cloud computing using AES under HEROKU cloud," 2018 27th Wireless and Optical Communication Conference (WOCC), 2018.
[31]. [31] Daemen, J., &Rijmen V., "The Data Encryption Standard," The Design of Rijndael, pp. 83-89,May 2020.
[32]. Sengupta, N., &Chinnasamy, R., "Contriving Hybrid DESCAST Algorithm for Cloud Security," Procedia Computer Science, vol. 54, pp. 47–56, 2015.
[33]. Thangapandiyan, M., Anand, P. M. R., &Sankaran, K. S., "Enhanced Cloud Security Implementation Using Modified ECC Algorithm," 2018 International Conference on Communication and Signal Processing (ICCSP), pp. 1019-1022, Apr. 2018.
[34]. Fan, S., & Zhao, Y. (2019). Analysis of DES Plaintext Recovery Based on BP Neural Network. Security and Communication Networks, 2019, 1–5.
[35]. Gangireddy, V. K. R., Kannan, S., &Subburathinam, K., "Implementation of enhanced blowfish algorithm in cloud environment," Journal of Ambient Intelligence and Humanized Computing, Feb. 2020.
[36]. Park, T., Seo, H., Lee, S., & Kim, H., "Secure Data Encryption for Cloud-Based Human Care Services," Journal of Sensors, pp. 2018, pp. 1–10, 2018.
[37]. Ghosh, S., &Karar, V., "Blowfish Hybridized Weighted Attribute-Based Encryption for Secure and Efficient Data Collaboration in Cloud Computing," Applied Sciences, vol. 8, no. 7, 1119, 2018.
[38]. Mudepalli, S., Rao, V. S., & Kumar, R. K., "An efficient data retrieval approach using blowfish encryption on cloud ciphertext retrieval in cloud computing," 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 267-271, Jun. 2017.
[39]. Chauhan, A., & Gupta, J., "A novel technique of cloud security based on hybrid encryption by Blowfish and MD5,"2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), pp. 349-355, 2017.
[40]. [40] Su, N., Zhang, Y., & Li, M., "Research on Data Encryption Standard Based on AES Algorithm in Internet of Things Environment," 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Mar. 2019.

[41]. Aryanti, A., &Mekongga, I., "Implementation of Rivest Shamir Adleman Algorithm (RSA) and Vigenere Cipher in Web Based Information System," E3S Web of Conferences, vol. 31, 10007, 2018.
[42]. Ramadan, M., Liao, Y., Li, F., Zhou, S., &Abdalla, H., "IBEET-RSA: Identity-Based Encryption with Equality Test over RSA for Wireless Body Area Networks," Mobile Networks and Applications, vol. 25, pp. 223-233, Apr. 2019.
[43]. Ambika, S., Rajakumar, S., &Anakath, A. S., "A novel RSA algorithm for secured key transmission in a centralized cloud environment," International Journal of Communication Systems, e4280, Jan. 2020.
[44]. Raja shree, S., ChilambuChelvan, A., & Rajesh, M., "An efficient RSA cryptosystem by applying cuckoo search optimization algorithm," Concurrency and Computation: Practice and Experience, e4845, 2018.
[45]. El Makkaoui, K., Beni-Hssane, A., &Ezzati, A., "Cloud-ElGamal and Fast Cloud-RSA Homomorphic Schemes for Protecting Data Confidentiality in Cloud Computing," International Journal of Digital Crime and Forensics, vol. 11, no. 3, pp. 90–102, 2019.
[46]. Subramanian, E. K., &Tamilselvan, L., "Elliptic curve Diffie–Hellman cryptosystem in big data cloud security," Cluster Computing, Feb. 2020.
[47]. Reddy, M. R., Akilandeswari, R., Priyadarshini, S., Karthikeyan, B., &Ponmani, E., "A modified cryptographic approach for securing distributed data storage in cloud computing," 2017 International Conference on Networks & Advances in Computational Technologies (NetACT), Jul. 2017.
[48]. Chaudhary, H., & Sharma, A. K., "Hybrid Technique of Genetic Algorithm and Extended Diffie-Hellman Algorithm used for Intrusion Detection in Cloud," 2020 International Conference on Electrical and Electronics Engineering (ICE3), Feb. 2020.
[49]. Kavin, B. P., &Ganapathy, S., "EC (DH)2: an effective secured data storage mechanism for cloud based IoT applications using elliptic curve and Diffie-Hellman," International Journal of Internet Technology and Secured Transactions, vol. 10, no. 5, May 2020.
[50]. Talkhaby, H. R., &Parsamehr, R., "Cloud computing authentication using biometric-Kerberos scheme based on strong Diffi-Hellman-DSA key exchange," 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2016.
[51]. Zhao E, M., &Geng, Y., "Homomorphic Encryption Technology for Cloud Computing," Procedia Computer Science, vol. 154, pp. 73–83, 2019.
[52]. Jin, B.-W., Park, J.-O., &Mun, H.-J., "A Design of Secure Communication Protocol Using RLWE-Based Homomorphic Encryption in IoT Convergence Cloud Environment," Wireless Personal Communications, vol. 105, pp. 599-618, Nov. 2018.
[53]. Khan, S. A., Aggarwal, R. K., & Kulkarni, S., "Enhanced Homomorphic Encryption Scheme with PSO for Encryption of Cloud Data," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Mar. 2019.
[54]. Das, D., "Secure cloud computing algorithm using homomorphic encryption and multi-party computation," 2018 International Conference on Information Networking (ICOIN), vol. 20, pp. 1561-1573, Mar. 2018.
[55]. Alabdulatif, A., Khalil, I., & Yi, X., "Towards secure big data analytic for cloud-enabled applications with fully homomorphic encryption," Journal of Parallel and Distributed Computing, vol. 137, pp. 192-2014, 2019.