Journal of Theoretical and Applied Information Technology
15th March 2023. Vol.101. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURITY THREATS, COUNTERMEASURES AND DATA ENCRYPTION TECNHINQUIES ON THE CLOUD COMPUTING ENVIROMENT

[1]ABRAR ALISMAIL, [2] ESRA ALTULIHAN, [3]RAWAN BUKHOWAH, [4]MOUNIR FRIKHA
Networks & Communication Department King Faisal University, Saudi Arabia
E-mail: [1]222401435@student.kfu.edu.sa, [2]221400737@student.kfu.edu.sa,
[3]222402836@student.kfu.edu.sa, [4]mmfrikha@kfu.edu.sa

ABSTRACT

In the world of computing, cloud computing has emerged as one of the fastest-emerging technologies. As more and more businesses store data in the cloud, it's possible to hack, alter, or delete that data since the servers are in remote locations. The main problem with cloud computing is security breaches, which must be solved flawlessly. Since the use of cloud computing is increasing, more security issues are emerging. Therefore, it is necessary to study this topic, analyze the new emerging security issues targeting cloud computing data, and search for solutions to mitigate these issues. It is important to know what types of attacks target the cloud computing data, what techniques are used for such attacks, and how to protect cloud computing users from these security issues. Cloud computing data security can be implemented in a variety of ways, one of which is through data encryption. This paper reviews the major data security issues present in cloud computing. A comparison study was made of several encryption techniques used in cloud computing. Moreover, this paper discusses the encryption platforms available for safeguarding cloud data and compares them to others based on factors such as security, complexity, usability, supported OS, advantages, and disadvantages.
Keywords: *Cloud, Threats, Mmitigation, Techniques, Data Security, Encryption.*

1. INTRODUCTION

In today's world, technology surrounds us. Due to the internet, technology is being used more and more every day. Today, many small and large organizations are moving to the cloud because it provides access to applications quickly and reduces costs. The cloud computing model works as a service provider. By paying nominal fees to the service provider, an individual can easily access different services and resources without having to purchase the whole service [1]. Cloud computing is a rapidly developing technology in computing. In one form or another, everyone uses cloud computing in his or her day-to-day life, such as Microsoft Office 365, Gmail, Dropbox, etc. Cloud computing has many advantages, including accessibility from anywhere with the fastest time, better geographic coverage, less infrastructure investment, etc., but it also has its challenges, including data security, a lack of resources, and expertise [2]. On-demand self-services, resource pooling, broad network access, elasticity, and virtualization are some of the characteristics of cloud computing. A cloud application has been developed for an IaaS (Information as a Service) and PaaS (Platform as a Service) platform. Data security remains one of the biggest problems for cloud users despite this platform's basic security features like firewall policy, user authentication policy, authorization, and secure logging policy. Data security is one of the biggest challenges. The security of data is extremely important in any business, and a leaking or corrupted database can cause the business to collapse. Many businesses are currently using cloud computing, either directly or indirectly, so if any data breaches occur, cloud computing and the business will be affected. It is for this reason that companies offering cloud computing services pay more attention to the security of their data. Therefore, this study aimed:

- To review the most common data security issues in cloud computing environments and discuss the mitigation techniques to mitigate them.
- To identify the common methods that individuals and organizations can use to improve data security in the cloud.

- To review available data encryption algorithms used for data security in the cloud.
- To highlight available encryption platforms that can be used to safeguard cloud data and comparing these platforms to others using some parameters.
- To assist businesses and individuals in selecting a robust, secure, and dependable encryption platform to safeguard their corporate data in the cloud.

Several literature reviews have been conducted to identify and mitigate data security vulnerabilities in the cloud. For instance, Hemalatha et.al [3] discussed major issues related to data security in computing. Additionally, presented an overview of cloud computing technologies, essential characteristics, classifications, delivery models, and encryption mechanisms. For maintaining cloud confidentiality, several encryption techniques are compared. In addition, Harfoushi [4] examined the literature on security issues in cloud computing and discussed SaaS, PaaS, and IaaS configurations and security issues. The challenge of cloud computing was also presented. However, this paper differs from other papers in this area because our review covers a wide range of cloud-related data security topics. In this paper, we will identify the most common data security issues in the cloud computing environment and discuss the most common countermeasures to control these issues. Also, we will describe the mitigation techniques that can be used to mitigate the cloud data security issues by reviewing the related publication. We found that data privacy is the most common threats to the data security and the most suggested techniques to mitigate that is encryption. Therefore, we continue to review available cloud data encryption algorithms. However, a detailed description of how to implement these algorithms will not be included. We will also discuss available encryption platforms for protecting cloud data and compare them. We aim to increase awareness of cloud security and improve it, especially data security, which is a major concern in this environment. Additionally, this paper will help to raise awareness among individuals and organizations who have been or may become victims of cybercrime due to their lack of data security in the cloud and help them choose a robust, secure, and reliable encryption platform for safeguarding their corporate data.

This paper is organized as follows: Section 2 presents methodology. Section 3 presents related works. Section 4 summarizes the results. Section 5 discusses techniques for securing cloud data. In Section 6, we review the algorithms available for encrypting cloud data. Section 7 compares the encryption platforms available to protect data before it is uploaded to the cloud. Section 8 concludes the research.

2. METHODOLOGY

The search is guided by PRISMA, which goes through three stages. During the identification stage, the Saudi digital library and Google scholar databases were searched using the following inclusion criteria: papers describing cybersecurity threats, countermeasures, and encryption techniques on the cloud computing environment, and papers published between January 2011 and December 2022 as well as published in academic journal or conference paper, are listed as the source type.

According to Table 1, there were four exclusion criteria: Papers that do not address risks, countermeasures, or encryption, papers that are not written in English, and papers that are not directly relevant to cloud computing cybersecurity threats, countermeasures, and encryption approaches. Furthermore, documents that are not available online.

Table 1: Inclusion and Exclusion Criteria

Inclusion Criteria	Exclusion Criteria
papers describing cybersecurity threats, countermeasures, and encryption techniques on the cloud computing environment	Papers don't address risks, countermeasures, encryption techniques
papers published between January 2011 and December 2022.	Papers that are not written in English
Papers published in academic journal or conference paper.	Papers not available online.

Figure 1 shows that a total of 3698 articles were recognized during the identification stage, with 3689 papers remaining after duplication was removed. At the screening stage, 1444 of the 1844 articles reviewed for title and abstract were rejected for not closely fulfilling the requirements. At the eligibility stage, 400 studies are eligible to proceed to the final stage. In the Included stage, 400 articles were chosen; 368 were rejected, leaving 32 for review.

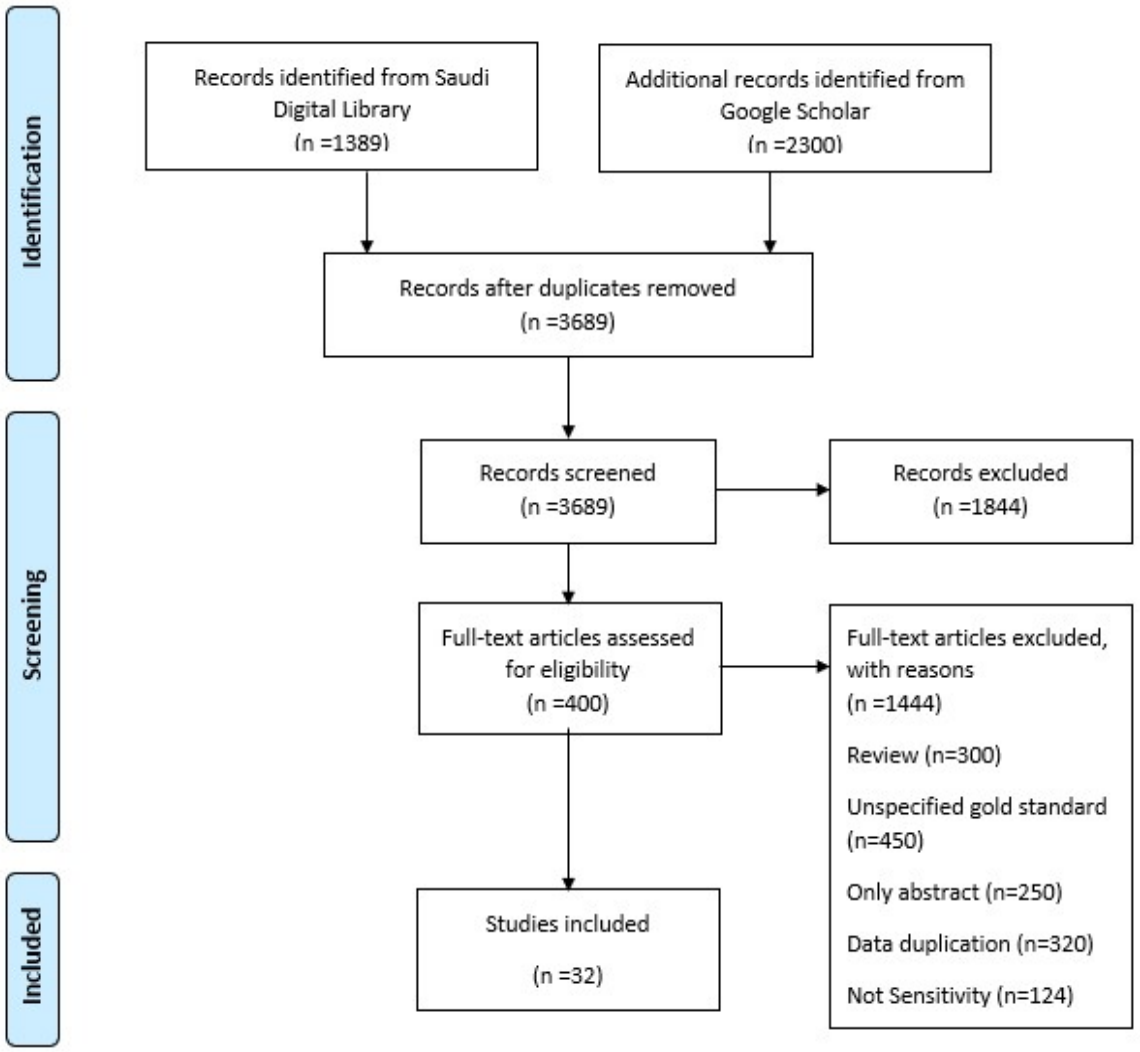

Figure 1 PRISMA Flow Chart

3. RELATED WORKS

Kumar et al. [2] provided an overview of the different data security issues in cloud computing in a multitenant environment, including CIA-related security issues, AAC-related security issues, broken authentication, session and access issues, and other data-related security issues. Then it proposed some methods for overcoming these issues. Cloud computing models, such as deployment models and service delivery models, are also described in the paper.

Anand et al. [5] discussed cloud computing service models and their various issues, as well as data breach issues, and proposed their idea or model for better security. The future of security looks bright. It is impossible to fully secure the data; therefore, security enhancements would have to be continuous. Simulations of the proposed results will be part of the future scope of the paper. Its main purpose was to provide a secure algorithm or idea for data, which is stored in cloud servers, and by using the collaborative model, data security could be enhanced.

Ahmed et al. [6] examined the concept of cloud computing and the related work associated with it. In addition, it discusses security in the cloud industry as a point of interest. It also provided an overview of cloud computing security issues, such as data access control, privacy, legal issues, and open standards. Additionally, it provided an overview of recent privacy and data security solutions. The paper discussed the different aspects of information security in cloud computing as well as the different exchanges and issues involved.

Chahal et al. [7] analyzed the various challenges associated with cloud security. Discuss the security issues of cloud storage. The paper also discussed the issue of insider threats and data breaches, which cover the integrity of data, the confidentiality of data, the availability of data, and the privacy of data. as well as how we can maintain a balance between privacy and security in this digital age. In addition, security challenges, such as data integrity, and solutions in cloud-based environments are discussed.

Vaidya et al. [8] analyzed the data security problem in cloud storage, which is mostly a distributed storage system. To verify erasure-coded data using RSA encryption, existing methods used erasure-correcting code for file distribution preparation. The study addressed a scheme that ensures client privacy and security as well as the integration of data error localization and storage correctness insurance. Security analysis showed that encryption techniques are necessary in cloud computing and are resilient to Byzantine failures, malicious data change attacks, and even collusion attacks by servers.

Hemalatha et al. [3] provide an overview of cloud computing technologies, essential characteristics, classifications, and delivery models. A study was conducted on several encryption techniques used in the cloud to maintain confidentiality. An analysis of the importance of cloud data security was conducted in the paper. A number of major data security issues are discussed, including data authentication, data privacy, data integrity, data location, data availability, data storage, and data backup and recovery. Using symmetric encryption algorithms is advantageous because of their efficiency in handling encryption for large amounts of data and since they are effectively fast at storing data in the cloud. In addition, various encryption techniques used in cloud computing were compared in the paper.

Albugmi et al. [9] have discussed how data is secured in cloud computing. It examined the security aspects of cloud data. A number of data protection methods and approaches are discussed in the paper to ensure maximum data protection by reducing risk and threats. There are many advantages to having data available in the cloud, but it also poses risks because it exposes data to applications with security loopholes. Cloud computing might also be at risk of data breaches when a guest OS is run over a hypervisor without knowing the reliability of the guest OS, which could have security vulnerabilities. Furthermore, the paper discussed data security aspects for data in transit and data at rest. Several levels of SaaS (software as a service), PaaS (platform as a service), and IaaS (infrastructure as a service) services are covered in this study.

Velumadhava et al. [10] demonstrate that the security issues of cloud computing include data leak prevention, data segregation, and data protection. The paper [10] states that to increase the security of data in the cloud, a data security model that includes authentication, data encryption and integrity, data recovery, and user protection must be created. In addition, cloud users are advised to confirm that the data is kept on a backup drive and that the keywords in the files have not changed before uploading data to the cloud.

Shailendra et al. [11] demonstrate that the security challenges of cloud computing include security, storage, locality, integrity, access, inadequate hiring processes and personnel screening, a lack of customer background checks, data breaches, and a lack of security education. The paper [11] presents techniques for encryption and decryption that have been used for a very long time to secure vital data. If properly managed, digital signatures and firewalls could also protect cloud-based data. In the coming days, the government of Nepal will also focus on its data security strategy, legislation, and plans. The nation should begin building its own data bank, and at the appropriate moment, government agencies and other interested parties should implement an integrated data store.

Subramanian et al. [12] categorize the dangers at the data level, including those that affect data integrity, data lineage, data recovery, data leakage, data remanence, data backup, data isolation, data segregation, data lock-in, data provenance, and data placement. The paper [12] provided a method for safely storing data in the cloud and performing performance integrity checks on the data when it was accessed. The security of data saved in the cloud is improved by storing encrypted, hashed, and meta-data files.

Chandramouli et al. [13] mention seven specific safety concerns in the study: privileged user access, legal compliance, data location and segregation, recovery, investigative support, and long-term sustainability. The research [13] suggests

using a technology called Airavat. This solution can stop unapproved privacy leaks during the MapReduce computing process. Additionally, the provable data integrity (PDI) solution, a mathematical technique for confirming the accuracy of data stored dynamically in the cloud, was developed. A client-based privacy management tool has also been presented. It offers a user-centric trust model to assist users in controlling the storage and use of their sensitive data in the cloud.

Nadeem et al. [14] reveal that, in addition to privacy violations, the study reveals that access, compliance, storage, retention, destruction, auditing, and monitoring are other issues associated with cloud data. According to the research [14], the main components to reducing security issues with cloud data are security management (people), security governance, risk assessment, education and training, policies and standards, third-party risk management, vulnerability assessment, security image testing, and data governance.

Bisong et al. [15] identify several data security issues, including platform lock-in, reliability and performance issues, and the security and privacy of corporate data stored in remote third-party data centers.The study [15] states conducting a consultation, a risk-benefit analysis, Applicants with lower risk, candidates with higher risk, alternatives to the "internal cloud," vendor agreements, the proportionality of safeguards, due diligence, an exit strategy, and the proportionality of analysis and review are all ways to reduce the security risks associated with cloud-based data.

Tabrizchi et al. [16] stated that cloud security concerns can be divided into the following five categories: security policies; data storage security; user-oriented security; network security; and application security. The study [16] presented the security threats in cloud computing in terms of spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. The study [16] described cloud computing security attacks in terms of abuse functionality, data structure attack, embedded malicious code, authentication explosion, resource manipulation, and sniffing attack.The study [16] stated that to accomplish cloud security, all cloud components in terms of data and infrastructure must be safeguarded against both known and undiscovered threats.

ShaluMall et al. [17] provide an overview of a new security framework that improves data security and confidentiality, as well as a description of how the new algorithm works and what this new framework uses to improve data security in cloud computing.This paper mentions that as cloud security begins to address the most critical issues of the whole cloud computing environment, the data owner and the cloud service provider must find solutions for security issues like confidentiality, integrity, and access control. In the end section of this paper, they analyzed and simulated the new framework.

Naresh et al. [18] have demonstrated diverse kinds of data security issues with data storage in cloud computing. In fact, this paper focuses on various issues, like issues in cloud data storage, identity management and access control, and contractual and legal issues. Moreover, this paper provides many suggested methods and protocols in order to solve these issues.

Venkata et al. [19] conduct a review study to identify all issues and challenges associated with cloud computing security and big data.Moreover, various advantages and solutions to big data are discussed.

According to Parsi et al. [20], the main concern is the security of people's data in the cloud.In this paper, areas of concern are data location and relocation, data availability, storage, backup, and recovery of data in the cloud environment, and how the use of the RSA algorithm will affect them and reduce threats. In addition, the paper explains the RSA algorithm, which is a block cipher that involves: 1. Key Generation 2. Encryption; 3. Decryption In addition, data security is provided by implementing this algorithm. Although it is vital to note that the authors address experimental results by taking sample data,

Aized et al. [21] present a review that includes the top ten obstacles in cloud computing, then they focus on data security and storage issues. They also discussed and analyzed the primary causes of data security issues, as well as potential solutions.This paper presents attributes of cloud computing and approaches that help increase the data security of cloud computing. Moreover, the paper suggests the future development of cloud computing.

Yunchuan et al. [22] This study discusses various areas related to cloud computing in terms of data security and privacy protections. First, this paper presents the most relevant issues in cloud computing. Second, it reviews different security techniques that enhance the security of data and privacy in the cloud from both hardware and software aspects, also including data integrity, confidentiality, and availability aspects. Moreover, this paper provides a comprehensive analysis of data security and privacy protection techniques and explains the service models in the cloud, which are SaaS, PaaS, and IaaS. Finally, it gives some solutions for data security and privacy protection.

Sabrina et al. [23] provide a review study about privacy risks in managing and accessing data in the cloud. This paper provides different scenarios for different aspects of the privacy problem. In addition, it presents risks, solutions, and some open problems related to the privacy of users when accessing services and resources in the cloud. The research mentions the development of solutions that are willing to address the privacy-aware processing of data.

Mahalle et al. [24]: This paper proposes a hybrid (RSA and AES) encryption technique to protect the security of cloud data.A hybrid encryption technique employing the AES and RSA algorithms is employed to apply security features, using a 128-bit secret key for AES and a 1024-bit key for RSA. In addition, a generation of RSA public key n and RSA public key e is produced by the upload option. When a user attempts to upload data to the cloud, the data is initially stored in a temporary directory. After calling the AES and RSA algorithms and being required to enter the AES secret key, the file is permanently stored in the database corresponding to the user account, and the temporary file is deleted. There are many advantages that deserve mention, like a hybrid encryption algorithm that uses the RSA and AES algorithms to protect user data in the cloud. The major benefit is that the keys are produced based on system time, making them impossible for an intruder to guess, increasing both our security and convenience. After already being uploaded, the data is kept in an encrypted state and can only be unlocked using the user's private key and secret key. The biggest benefit of this is how safe the cloud makes your data.

Tebaa et al. [25] define the idea of cloud computing and outline the requirement of using homomorphic encryption to protect calculations made with data stored on the cloud provider's servers. Therefore, the use of cryptosystems based on homomorphic encryption is necessary to enable the cloud provider to execute actions on encrypted data without first decrypting it. The client is the only one who has access to the secret key in homomorphic encryption systems, which are used to operate on encrypted data without knowing the private key (without decryption). Therefore, cloud computing security, which is based on completely homomorphic encryption, is a novel idea in security that allows for the provision of calculations' results on encrypted data while maintaining the anonymity of the raw data used for the calculation.

Kirubakaramoorthi et al. [26] In this paper, they investigate various encryption methods for securing the cloud storage environment. This paper provides a concise overview of some of the cryptographic techniques that are currently in use and can be used to improve cloud environment security.The encryption techniques listed below are part of advanced cryptographic techniques. When symmetric searchable encryption (SE) is compared to asymmetric searchable encryption (ASE). Moreover, identity-based encryption and attribute-based encryption A single writer or single reader (SWSR) is a term taken from the terminology of cloud storage. It is appropriate for a situation in which the client is both the data searcher and the data producer. In addition to better structures and security terms, SSE schemes were given. The fundamental drawback of ASE schemes is their lack of effectiveness and lower security, while their main benefit is their functionality. ASE permits pre-processing of the data and represents it inefficiently in data structures. For a token, the server can launch a dictionary attack and determine the precise keywords the client is seeking. In addition, the participant's identity is crucial to identity-based encryption. To send the encrypted messages, the sender just needs to be aware of the recipient's identity property. One of the most common uses of identity-based encryption is email encryption. In a cloud computing environment, attribute-based encryption is one of the cryptographic methods employed. The data is encrypted by the data owner using a set of attributes, and only authorized users who possess the predetermined or specific attributes can decode the data. The cloud infrastructure is safer thanks to this encryption method.

Rani et al. [27] In general, this paper presents an investigation of the role of load balancer techniques on the live cloud infrastructure that collaborates with open-source services. This paper proposes a Modified-HBB-LB and Modified-Blowfish that are used in tandem for load balancing and security. In addition, this paper depends on designing and developing a virtual machine with the encryption technique called Diffie-Hellman and Blowfish. The system should achieve the load balancer in cloud computing as a systematic model. Furthermore, Modified-Blowfish Encryption is used, and DES or IDEA could be used and combined with Blowfish, making it a drop-in replacement for symmetric square encryption. Modified-Blowfish encryption uses a key that has a variable length of up to 448 pieces. In addition, there is an enhanced algorithm of modified-blowfish encryption called the enhanced blowfish algorithm (EBA) that concerns encryption information on the cloud. It retains a secret key for encryption and decryption messages. As the Honeybee Foraging Technique works alongside the EBA to develop the honeybee load balancing algorithm, This system is important for cloudlets to map the behavior of honeybees searching for food sources that are in the virtual cloud computing system. As the Modified-HBB-LB technique deals with migration tasks, it does a great job of reducing the number of migration tasks by around 30%, 25%, and 20% compared to other systems. The modified HBB-LB technique maintains higher performance levels on three aspects: makespan, completion, and response time, as compared with other existing comparative techniques. Furthermore, the Modified-Blowfish techniques recover the original files in less time than AES, RSA, and Blowfish, and they execute much faster.

Manreet et al. [28] present a novel cryptographic technique that uses client-side data encryption to encrypt data and make it secure before storing it on the cloud, so this paper presents the design of the new algorithm. The paper compares the proposed technique with the exciting symmetric-key algorithms, which are DNA, AES, DES, and Blowfish. Furthermore, it presents the results of the experiment. The name of the proposed approach is BDNA, or the binary of DNA cryptography, which is a symmetric key algorithm. In the BDNA algorithm, the same key that is used for encryption is also used for decryption. In this approach, the use of the authentication process is essential, and more than 96 characters are used in the encryption, so it will enhance the security of the data and be more efficient and provide better performance. In addition, the BDNA system is strong enough to increase the security of exciting security systems by providing the new possibility of a hybrid cryptographic system.

In this paper, Basri et al. [29] show how the Data Encryption Standard Algorithm (DES) can prevent data cracking attacks in cloud computing.such attacks as the man-in-the-middle attack (MitM) and social engineering. Also, the paper describes how the Last Significant Bit (LSB) works with DES. DES is considered one of the block cipher algorithms that are used as a standard symmetric encryption algorithm. In addition, DES contains and produces only eight blocks of ciphers combined into one ciphertext. LSB is used to convert the ciphertext of DES into eight random images, making it more secure against any brute-force attack. Compared with the RSA algorithm, DES is faster for producers. It is a data encryption standard that is used to protect huge amounts of electronic data.

Singh et al. [30] present how data in the cloud is encrypted using the RSA algorithm to ensure security so that only the concerned user can access it. The proposed work involves implementing the RSA algorithm and analyzing its performance based on different parameters, such as time complexity, space complexity, and throughput. There are steps involved in implementing the RSA algorithm, including: 1: Key generation 2-Encryption 3- Decryption. In addition, the RSA cipher maps every message to an integer. There are two types of keys in RSA: public-key and private-key. Public keys are known by everyone in the cloud, whereas private keys are only known by the user who originally owned the data.Cloud service providers encrypt data, and cloud users and consumers decrypt it. Encrypted data can only be decrypted with the corresponding private key once it has been encrypted with the public key. Some benefits of the RSA algorithm: access to the data is restricted to authorized users; data is encrypted before being stored in the cloud; in spite of the fact that some intruder (unauthorized user) might accidentally or intentionally get the data, he can't decrypt it and get back the original data; and the RSA encryption algorithm provides secure communication in cloud computing.

Thabit et al. [31] focused on enhanced data secrecy in this paper, proposing a novel effective lightweight homomorphic cryptographic

algorithm.Furthermore, the proposed technique uses two levels of encryption in combination to improve cloud computing security. In the first layer, there is a new effective light-weight cryptographic algorithm called NELCA, and in the second layer, there is a multiplicative homomorphic property of the RSA algorithm. In this approach, both symmetric and asymmetric cryptography features are offered, making cloud computing more secure and private. Based on experimental results, the proposed algorithm significantly improved execution time, memory utilization, and encryption throughput. Compared to the cryptographic systems widely used in cloud computing

Gampala et al. [32]: This paper discusses the authentication and encryption for secure data transmission between clouds using elliptic curve cryptography. The elliptic curve cryptography system is a public-key cryptosystem, so each user has a public and a private key, and encryption and signature verification are performed using a public key, but decryption and signature generation are performed with the private key. Currently, elliptic curves are used as an extension of other cryptosystems. It is an elliptic curve Diffie-Hellman key exchange algorithm and an elliptic curve digital signature algorithm. With elliptic curve cryptography, secure and authenticated data is transmitted from one cloud to another. Furthermore, compared to other algorithms, elliptic curve cryptography uses a smaller key to provide the same level of security.

Table 2 gives a full analysis of related works based on their publication year, the threats they address, the ways they suggest dealing with those threats, and future work.

Table 2: Analysis Of Related Works

Author	Publication year	Addressed threats	Suggested mitigation techniques
Kumar et.al [2]	2018	Provides a variety of data security challenges, including those related to the CIA triad, Authentication and Access Control (AAC), broken authentication controls, session controls, and access controls, as well as other security issues related to data location, multi-tenancy, and cloud backup computing.	• For CIA related security issues, it proposed to apply strong encryption algorithms like Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA) algorithms, Third Party Auditing (TPA) can be employed to check for the data integrity. Also, Duplication, redundancy, backups, and resilient systems can be used to address availability issues. • For AAC related security Issues, apply single-sign-on policy, multi-factor authentication, biometric authentication, Intrusion Detection System (IDS) • For broken authentication, session & access, a single set of strong authentication and session management controls should be implemented, avoid Cross-site Scripting (XSS), check Access and apply automated verification.
Anand et.al [4]	2020	Provides an idea for cloud data security	Use of Merging, cryptography, steganography and hashing processes.
Ahmed et.al [5]	2016	Analyzes and break down the essential issues of cloud computing such as such as data access control, privacy, legal issues, and open standards. Also, it illustrates the privacy and security issues associated with cloud.	Homomorphic encryption, KMIP (Key Management Interoperability Protocol) and OASIS (Organization for the Advancement of structured Information Standards) for key management and the public data integrity verification supported by NEC Lab's provable Data Integrity (PDI).
Chahal et.al [6]	2017	Discussed the issue of insider threats and data breaches, which covers the integrity of data, the confidentiality of data, the availability of data, and the privacy of data.	Making use of encryption and anonymity tools and encouraging your friends to follow suit.
Vaidya et.al [7]	2020	Focuses on cloud data storage security for client.	• Proposed a cryptographic algorithm to encrypt client data in the cloud, ensuring the correctness of cloud clients' data in the cloud predecessors. RSA encryption and distributed

			verification of erasure coded data are used. • An authentication system for clients to upload and retrieve data has been proposed with an integrated storage correctness insurance and data error localization.
Hemalatha et.al [8]	2014	Several important data security issues are discussed, including authentication, privacy, integrity, availability, storage, and backups and recoveries.	A symmetric encryption algorithm can be used to encrypt large amounts of data and can be used to store data in the cloud at an effective speed.
Albugmi et.al [9]	2016	Discussed data security issues in the cloud including, virtualization, storage in public cloud and multitenancy. Also, discussed data security aspects for data-in-transit and data-at-rest	Proposed efficient techniques for encrypting cloud data. Described block ciphers, stream ciphers, and hash functions used to encrypt the data in the cloud.
Velumadhava et.al [10]	2015	Demonstrate that the security issues of cloud computing include data leak prevention, data segregation, and data protection	• To increase the security of data in the cloud, a data security model that includes authentication, data encryption and integrity, data recovery, and user protection must be created. • In addition, cloud users are advised to confirm that the data is kept on a backup drive and that the keywords in the files have not changed before uploading data to the cloud.
Shailendra et.al [11]	2019	Demonstrates that the security challenges of cloud computing include security, storage, locality, integrity, access, inadequate hiring processes and personnel screening, a lack of customer background checks, data breaches, and a lack of security education.	• Techniques for encryption and decryption have been used for a very long time to secure vital data. • If properly managed, digital signatures and firewalls could also protect cloud-based data. In the coming days, the government of Nepal will also focus on its data security strategy, legislation, and plans. • The nation should begin building its own data bank, and at the appropriate moment, government agencies and other interested parties should implement an integrated data store.
Subramanian et.al [12]	2018	Categorizes the dangers at the data level, including those that affect data integrity, data lineage, data recovery, data leakage, data remanence, data backup, data isolation, data segregation, data lock-in, data provenance, and data placement.	• Provided a method for safely storing data in the cloud and performing performance integrity checks on the data when it is accessed. • The security of data saved in the cloud is improved by storing encrypted, hashed, and meta-data files.
Chandramouli et.al [13]	2017	Mentions seven specific safety concerns are mentioned in the study: privileged user access, legal compliance, data location and segregation, recovery, investigative support, and long-term sustainability.	• suggests using a technology called Airavat. • This solution can stop unapproved privacy leaks during the Map-Reduce computing process. • Additionally, the provable data integrity (PDI) solution, a mathematical technique for confirming the accuracy of data dynamically stored in the cloud, was developed. • A client-based privacy management tool has also been presented. • It offers a user-centric trust model to assist users in controlling the storage and use of their sensitive data in the cloud.
Nadeem et.al [14]	2016	Reveals that in addition to privacy violations, the study reveals that access, compliance, storage, retention, destruction, audit, and monitoring are other issues associated with cloud data.	• The main components to reducing security issues with cloud data are security management (people), security governance, risk assessment, education and training, policies, and standards, third party risk management, vulnerability assessment,

			security image testing, and data governance.
Bisong et.al [15]	2011	Lists several data security problems, including platform lock-in, reliability and performance challenges, as well as the security and privacy of corporate data stored in distant third-party data centers.	• Conducting a consultation, a risk/benefit analysis, Applicants with lower risk, candidates with higher risk, alternatives to the "internal cloud," vendor agreements, the proportionality of safeguards, due diligence, an exit strategy, and the proportionality of analysis and review are all ways to reduce the security risks associated with cloud-based data.
Tabrizchi et.al [16]	2020	Presented the security attacks of cloud computing in terms of abuse functionality, data structure attack, embedded malicious code, explosion of authentication, resource manipulation, and sniffing attack.	Stated that to accomplish cloud security, all cloud components in terms of data and infrastructure must be safeguarded against both known and undiscovered threats.
ShaluMall et.al [17]	2018	Data security issues of data owner that stored in the cloud computing.	They present a new security framework that has new techniques for data of data owner that is stored in the cloud.
Naresh et.al [18]	2016	They have presented a taxonomy of issues in three sections: **1.** Cloud Storage issues, Data privacy and Integrity, Data recoverability and vulnerability, Improper media refinement and Data backup. **2.** Identity Management and Access Control, Malicious Insiders, outside Intruder **3.** Contractual and Legal issues, Service level agreements, Legal issues.	The paper explains the research work solutions, it provides a protocol that known as a storage security protocol also SecCloud protocol and Files Assured Deletion protocol that helps to improve the security of data and other schemes such as timePRE which is a scheme for secure data sharing in the cloud. For identity management and access control the paper proposed five solutions.
Venkata et.al [19]	2014	Big data is considered one of the data security issues in the cloud environment because most businesses deal with big data.	There is a Java-based programming framework called Hadoop that is used to process large sets of data. Hadoop lowers the risk of an entire system failure and it has two sub-projects, Map Reduce, and Hadoop Distributed. Another application used is Bioinformatics.
Parsi et.al [20]	2012	This paper disuses about big concerns of data security in the cloud computing which they are privacy and confidentiality, data integrity that service provider must insure that data integrity. Data store in some place, different servers where the user don't know, and it will move from one place to another, so in this case, data availability becomes a major issue.	Only the RSA algorithm included in this paper as a solution. Which is a block cipher that involved key Generation, encryption and decryption and data security is provided by implementing this algorithm.
Aized et.al [21]	2014	Most users who used cloud computing are concerned about their private data. the other issues are isolation failure, data protection, management interface compromise, insecure data deletion and the malicious insider.	Approaches that have been used to ensure data security for users in the cloud encryption, Homomorphic token, Guidelines that some guidelines are mentioned in the paper to ensure data security in the cloud, harmonizing scheme, data concealment, token, framework, and stripping algorithm.
Yunchuan et.al [22]	2014	some of the cloud computing security issues are resource security, resource management and resource monitoring, other issues are that there are no standards or regulations to deploy applications in the cloud, also there is a lack of standardization control in the	Some techniques are used: 1. Homomorphic Encryption, it is usually used to ensure the confidentiality of data. 2. Cryptographic algorithm named Diffie-Hellman is proposed for secure communication.

		cloud. The paper includes other issues which are data privacy, data protection, data availability, data location, secure transmission and some challenges like data loss, service disruption, outside malicious attacks and multitenancy issues.	3. RSA, 3DES. 4. In-Memory Database encryption technique 5. Data concealment approaches merge real data with the visual fake data to falsify the real data's volume
Sabrina et.al [23]	2012	Privacy risks in managing and accessing data in the cloud.	The paper explains some design techniques that are used to protect sensitive data from any exploit and build a framework for formally analyzing possible information leakages. In addition, this paper presents other solutions.

4. RESULTS AND ANALYSIS

In the previous section, the results showed common data security threats in cloud computing. The most common threats, as shown in Figure 2, are privacy data location, cloud backup, data access controls, authentication, database availability, data integrity, data protection, and malicious insider attacks, where privacy is posing the greatest threat to the security of data in the cloud.

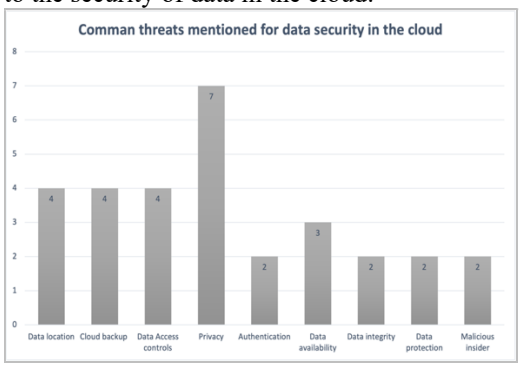

Figure 2: Common Security Threats on Data Cloud

The common technologies used to address cloud data security threats according to analyzed studies are encryption, data backups, hashing, authentication, and an intrusion detection system (IDS). As shown in Figure 3, the most frequently suggested technology is encryption. However, there are many encryption algorithms that can be used for that purpose.

Figure 3: Common Mitigation Techniques for Cloud Data Security

5. TECHNIQUES TO IMPROVE THE DATA SECURITY IN THE CLOUD

Encryption [10] is recommended as a better way to secure information. It is preferable to encrypt data before storing it on a cloud server. Encryption will be a strong solution that helps to safeguard the confidentiality of digital data stored in the cloud. It is recommended that data be encrypted before being uploaded to the cloud. Encryption is a way of preventing other users from accessing data by applying encryption to it, which makes the data completely unusable, whereas normal encryption can complicate availability. Data encryption for information stored on the cloud network ensures that even if the data is lost, stolen, or inadvertently shared, the contents are rendered virtually useless in the absence of the encryption key. Keys, once again, are only made available to authorized cloud users. Encryption helps to ensure privacy and data security, and it can be used as a service.

To improve data security in the cloud, a data security model [10] that includes authentication, data encryption and integrity, data recovery, and user protection must be designed. A data-driven framework can be created to enable secure data processing and sharing among cloud users. This model contributes to the processes of cloud user authentication, cloud data encryption, and cloud data integrity. Furthermore, this model facilitates cloud data recovery and cloud user protection.

If properly maintained [11], digital signatures and firewalls can also protect data in the cloud. The digital signature mechanism ensures data authenticity and integrity through authentication and non-repudiation. Prior to transmission, a message is assigned a digital signature, which is then rendered invalid if the message is subsequently modified without authorization. Cloud firewalls are software-based, cloud-deployed network devices designed to prevent or mitigate unauthorized access to private networks. They are a new technology that is designed for modern business needs and sits within online application environments. Additional security solutions, such as firewalls as a service (FWaaS) and web application firewalls (WAF), help to detect and block malicious traffic.

Performing performance integrity checks [12] on the cloud data when it is accessed performance Integrity-checking tools can detect whether any critical cloud files have been changed, allowing the cloud administrator to look for unauthorized system changes. Integrity checkers examine stored files or network packets to see if they have been altered or changed.

Using a technology called Airavat [13], This solution can stop unapproved privacy leaks during the MapReduce computing process. Airavat is a MapReduce-based system that ensures high security and privacy for distributed computations on sensitive data. Airavat is an innovative combination of mandatory access control and differential privacy [17]. Data providers are in charge of their sensitive data's security policy, which includes a mathematical limit on potential privacy violations. Users with no security expertise can perform computations on the data, but Airavat limits these computations, preventing information leakage beyond the policy of the data provider. This technology contributes to mitigating cloud data leakage and enhancing cloud security.

Reducing cloud data security issues [14] demands main components in terms of security management (people), security governance, risk assessment, education and training, policies and standards, third-party risk management, vulnerability assessment, security image testing, and data governance. These components are required to address cloud security issues. SaaS providers will need to incorporate and improve security practices used by managed service providers, as well as develop new ones, as the cloud computing environment evolves. Early detection of cloud issues and treatment by providing visibility into files, applications, and users, potential breaches are avoided. continuous cloud monitoring to ensure real-time file scanning. Security standards are maintained through regular auditing and reporting. The main objective of regular cloud auditing is to ensure data availability in terms of the performance and security provided by the cloud computing service provider. It targets potential customers and ensures they have access to performance and security information.

Conducting a consultation [15], cloud consultants assist providers in identifying and addressing their cloud requirements, allowing them to leverage cloud computing for safer, more efficient operations. Cloud consultants educate businesses on the various cloud computing services available and assist them in making operational decisions. Cloud consultants possess in-depth technical knowledge and play critical communication roles in cloud-based solutions.

Conducting a risk-benefit analysis [15], The main advantage of cloud risk-benefit analysis is that it identifies risk levels and, as a result, areas where intervention is required. Because cloud resource limitations prevent the development of risk reduction strategies for all consumption activities, this type of screening is critical for cloud providers.

Securing cloud components in terms of data and infrastructure must be safeguarded against both known and undiscovered threats [16]. The practice of securing cloud infrastructure resources and supporting systems is known as "cloud infrastructure security." When implementing cloud technology, it is critical to consider cloud infrastructure security as one of the most important responsibilities. The term "cloud computing infrastructure security" refers to the entire infrastructure that improves data security and

provides DDoS protection, threat detection, and compliance supervision.

6. DATA ENRYPTION ALGORITHMS

Mahalle et.al [24] proposed a hybrid encryption technique employing the AES and RSA algorithms to apply security features, using a 128-bit secret key for AES and a 1024-bit key for RSA. A generation of RSA public key-n and RSA public key-e is produced by the upload option. When a user attempts to upload data to the cloud, the data is initially stored in a temporary directory. After calling the AES and RSA algorithms and being required to enter the AES secret key, the file is permanently stored in the database corresponding to the user account, and the temporary file is deleted. A hybrid encryption algorithm that uses the RSA and AES algorithms to protect user data in the cloud The major benefit is that the keys are produced based on system time, making them impossible for an intruder to guess, increasing both our security and convenience. After already being uploaded, the data is kept in an encrypted state and can only be unlocked using the user's private key and secret key. The biggest benefit of this is how safe the cloud makes your data.

Tebaa et.al [25] investigated various encryption methods for securing the cloud storage environment. This paper provides a succinct overview of some of the cryptographic techniques now in use that can be applied to enhance cloud environment security. The encryption techniques listed below are part of advanced cryptographic techniques. Comparing symmetric searchable encryption (SE) versus asymmetric searchable encryption (ASE). A single writer or single reader (SWSR) is a term taken from the terminology of cloud storage. It is appropriate for a situation in which the client is both the data searcher and the data producer. In addition to better structures and security terms, SSE schemes were given. The fundamental drawback of ASE schemes is their lack of effectiveness and lower security, while their main benefit is their functionality. ASE permits pre-processing of the data and represents it inefficiently in data structures. For a token, the server can launch a dictionary attack and determine the precise keywords the client is seeking.

Kirubakaramoorthi et.al [26] investigated various encryption methods for securing the cloud storage environment. This paper provides a succinct overview of some of the cryptographic techniques now in use at can be applied to enhance cloud environment security. Moreover, identity-based encryption and attribute-based encryption the participant's identity is crucial to identity-based encryption. To send the encrypted messages, the sender just needs to be aware of the recipient's identity property. One of the most common uses of identity-based encryption is email encryption. In a cloud computing environment, attribute-based encryption is one of the cryptographic methods employed. The data is encrypted by the data owner using a set of attributes, and only authorized users who possess the predetermined or specific attributes can decode the data. The cloud infrastructure is safer thanks to this encryption method.

Rani et.al [27] presented an investigation of the role of load balancer techniques on the live cloud infrastructure that collaborates with open-source services. Specifically, this paper suggests a Modified-HBB-LB and Modified-Blowfish that used together for load balancing and their security. In addition, this paper depends on designing and developing a virtual machine with the encryption technique called Diffie-Hellman and Blowfish. The system should achieve the load balancer in cloud computing as a systematic model. Modified-Blowfish encryption is used, and DES or IDEA could be used and combined with Blowfish, so it is a drop-in replacement for symmetric square. Modified-Blowfish encryption uses a key that has a variable length of up to 448 pieces. In addition, there is an enhanced algorithm of modified-blowfish encryption called the enhanced blowfish algorithm (EBA) that concerns encryption information on the cloud. It retains a secret key for encryption and decryption messages. The Honeybee Foraging Technique works alongside the EBA to develop the honeybee load balancing algorithm. This system is important for cloudlets to map the behavior of honeybees searching for food sources that are in the virtual cloud computing system. As the Modified-HBB-LB technique deals with migration tasks, it does a great job of reducing the number of migration tasks by around 30%, 25%, and 20%, respectively, compared to other systems. The modified HBB-LB technique maintains higher performance levels on three aspects: makespan, completion, and response time, as compared with other existing comparative techniques. SECURITY The modified-Blowfish techniques take less time to recover the original files than AES, RSA, and Blowfish, and they are much faster in execution than others.

Manreet et.al [28] presented a novel cryptographic technique that uses client-side data encryption to encrypt data and make it secure before storing it on the cloud, so it presents the design of the new algorithm. The paper compares the proposed technique with the exciting symmetric-key algorithms, which are DNA, AES, DES, and Blowfish. Furthermore, it presents the results of the experiment. The name of the proposed approach is BDNA, or the binary of DNA cryptography, which is a symmetric key algorithm. In the BDNA algorithm, the same key that is used for encryption is also used for decryption. In this approach, the use of the authentication process is essential. In this enhanced approach, more than 96 characters are used in the encryption, so it will enhance the security of data. The BDNA technique is more efficient and provides better performance. A BDNA system strong enough to increase the security of exciting security systems through the new possibility of a hybrid cryptographic system.

M Basri et.al [29] presented how the Data Encryption Standard Algorithm (DES) can prevent attacks from cracking data in cloud computing. such attacks as the man-in-the-middle attack (MitM) and social engineering. Also, the paper describes how the Last Significant Bit (LSB) works with DES. DES is considered one of the block cipher algorithms that are used as a standard symmetric encryption algorithm. DES contains and produces only eight blocks of ciphers combined into one ciphertext. LSB is used to convert the ciphertext of DES into eight random images, making it more secure against any brute-force attack. Compared with the RSA algorithm, DES is faster for producers. It is a data encryption standard that is used to protect huge amounts of electronic data.

Singh et.al [30] proposed implementing the RSA algorithm and analyzing its performance based on different parameters, such as time complexity, space complexity, and throughput. The steps involved in implementing the RSA algorithm are: 1: Key generation 2- Encryption 3- Decryption. The RSA cipher maps every message to an integer. There are two types of keys in RSA: public-key and private-key. Public keys are known by everyone in the cloud, whereas private keys are only known by the user who originally owned the data. Cloud service providers encrypt data, and cloud users and consumers decrypt it. Encrypted data can only be decrypted with the corresponding private key once it has been encrypted with the public key. Access to the data is restricted to authorized users. Data is encrypted before being stored in the cloud. In spite of the fact that some intruder (unauthorized user) might accidentally or intentionally get the data, he can't decrypt it and get back the original data. The RSA encryption algorithm provides secure communication in cloud computing.

Thabit et.al [31] proposed technique uses two levels of encryption in combination to improve cloud computing security. In the first layer, there is a new effective light-weight cryptographic algorithm called NELCA, and in the second layer, there is a multiplicative homomorphic property of the RSA algorithm. In this approach, both symmetric and asymmetric cryptography features are offered, making cloud computing more secure and private. Based on experimental results, the proposed algorithm significantly improved execution time, memory utilization, and encryption throughput. Compared to the cryptographic systems widely used in cloud computing.

Gampala et.al [32] proposed authentication and encryption for secure data transmission between clouds using elliptic curve cryptography. The elliptic curve cryptography system is a public-key cryptosystem. Each user has a public and a private key. Encryption and signature verification are performed using a public key. Decryption and signature generation are performed with the private key. Currently, elliptic curves are used as an extension of other cryptosystems. It is an elliptic curve Diffie-Hellman key exchange algorithm and an elliptic curve digital signature algorithm. With elliptic curve cryptography, secure and authenticated data is transmitted from one cloud to another. As compared to other algorithms, elliptic curve cryptography uses a smaller key to provide the same level of security.

7. AVAILABLE ENRYPTION PLATFORMS

There are a variety of encryption platforms available to secure cloud data. These platforms are Cryptotor, Boxcryptor, Encrypto, EncFSMP, Odrive. Based on our experience with these platforms, we compare them in terms of complexity, security, encryption algorithm, advantages, disadvantages, operating systems supported, and usability of each platform (Table 4).

6.1 Boxcryptor platform

Boxcryptor is a platform that provides an additional degree of security for cloud storages by encrypting files on user device. Boxcryptor was designed from the outset to be cloud-optimized, so all files are encrypted, and access can be shared. This indicates that each file is encrypted separately from the others.

6.2 Cryptomator platform

Cryptomator is a platform that enables users to encrypt their data on their local workstation, removable media, and in the cloud. The Cryptomator platform creates a virtual drive via which encrypted data can be seen, altered, and enhanced. The vault (the encrypted data) can be stored on any linked storage device, such as a local drive, a network drive, or a USB flash drive. Cryptomator External Link is optimized for usage with cloud-based synchronization services like OneDrive.

6.3 Encrypto platform

Encrypto is platform that allows user to send and share encrypted files, as well as encrypt local and cloud storage. It's as easy as dragging and dropping any file onto the app window, setting a password, and adding a password hint that only sender and the recipient know. Once encrypted, user can store the file on your computer and/or send it via email, Dropbox, or even a USB stick. AES 256-bit encryption is used by Encrypto. To share files, both the sender and recipient must have Encrypto installed. Encrypto software is available for free on both Windows and Mac.

6.4 EncFSMP platform

This platform uses many of the same open-source components as BoxCryptor. Place any file or folder you want to encrypt on your local drive, and it will be automatically encrypted. These folders allow you to create, edit, and export passwords. It is completely free and does not contain any nags or other downloads. Shared files and file management aren't included. Despite being available for Windows, Mac and Linux systems, EncFSMP is compatible with Linux.

6.5 ODrive Platform

ODrive is a platform that as a desktop and web-based tool that users can link all of his/her cloud storage account together. Odrive uses the encryption add-on for creating encryption folders, and these encryption folders are automatically encrypted before data is moved to the cloud. This platform has zero-knowledge encryption for the secret passphrase, and only users who own the secret passphrase know it. In addition, AES encryption is used by add-on encryption.

Table 2: Available Encryption Platforms

Platform	complexity	Security	Algorithm	Advantages	Disadvantages	Supported OS	Usability
Boxcryptor	AES 256-bit encryption is harder to crack	Secure for local and cloud storage	Combined RSA and AES-256	• Robust encryption • User-friendly • Capability to share files	• No regular payment plans • Few features for individual plan	Windows, Mac, Android, iOS	Registration is required
Cryptomator	AES 256-bit encryption is harder to crack	Secure for virtual drive Encrypted contents	256-bit AES encryption	• pay asyou go • User-friendly	• Online customer service is limited. • Missing file sharing	Windows, MacOS, iOS, and Android	No registration is required
Encrypto	Impossible to crack the 256-bit AES encryption	• Secure for local and • cloud Storageprivate keys are stored offline	256-bit AES	• Free • Client-Side encryption. • It will never mash or corrupt your files	• No built-in file sharing feature • It can be difficult to give the password even when hints are embedded in the password	Windows and Mac OSX	Very easy to download and use.
EncFSMP	AES 256-bit encryption is harder to crack	Create an encrypted folder anywhere on your local drive	256-bit AES encryption	• The most minimalistic tool. • Free • Can create, edit, export and change the password of EncFS folders	File management and sharing aren't included.	Linux, Windows and Mac	No registration is required
ODrive	AES 256 bit encryption is harder to crack	Even though that Odrive is used zero-knowledge encryption and has only one authentication process, it is completely safe as you know your password (your own passphrase). Odrive provided increased encryption that keeps the security of data and files	256-bit AES encryption	• zero knowledge ” encryption • Capabilities to share files • Encrypt folders in any storage • Back up important files to any storage • Sync unlimited data	• Only one step for the encryption, so there is one code • Lacks two factors authentication • No cloud-to-cloud sync	Windows, Mac, and Linux.	Sign in through one of OAuth provider like Facebook or Dropbox so registration is not required

We can conclude from this experiment that all these platforms or tools can be used to encrypt data before uploading it to the cloud. In addition, there is no obvious best choice among them since each of them has advantages and disadvantages, and the decision will depend on the company's or individual's requirements.

The paper covers its subjects in a good way, it presents data security issues in cloud computing in details. Even though there is a need of more related studies and realistic experiences to be sure that the encryption technique is the most frequently suggested technology. In addition, the encryption techniques section, clarifying which advantages and disadvantages are for each platform and why we choose these platforms specifically will add more value to the paper. Comparing these encryption platforms widely can create new ideas for researchers.

8. CONCLUSION AND FUTURE DIRECTIONS

In recent period, most people use cloud computing even indirect way, and they have a lot of interest to increase data security of cloud computing. As increased use of cloud computing, hack, alter, or delete data by malicious attackers increase. In this paper, we demonstrate experimentally how to construct a platform for cloud environments that encrypts the cloud data before it is uploaded to the platform. Afterwards, we were tempted to gather information in order to identify less secure Web services and expose the connections responsible for data breaches. Overall, cloud computing has become a huge concern these days. Related threats and risks of data security in the cloud are presented in the paper. After analyzing all risks defined, the paper conduct results. In addition, the paper discusses some techniques to improve the data security in the cloud computing so then encryption algorithms are defined as the best solution then compared some of encryption platforms. Moreover, encryption is recognized as the most suitable technique for mitigating data breach attacks on cloud platforms. Encrypting data before uploading it to a cloud platform will mitigate data breaches in most cases. Therefore, even if the attacker obtains the data, it will be in an unreadable format. Encryption systems could be used and are suggested while utilizing cloud computing platforms. We should implement access rules, a daily check-maker, and encryption mechanisms for all characteristics located in the on-premises datacenter, in the cloud, and in remote locations, together with the installation of advanced security software and hardware that can mitigate the risk level. With the speed changing of technology the privacy may not be the most threat because it is may change and should always review all security policies and producers and daily incidents to be update and focus more on what is more important whether privacy data location, cloud backup, data access controls, authentication, database availability, data integrity, data protection, or malicious insider attacks. Cloud computing is constantly evolving in order to provide users with various levels of on-demand services. While consumers profit from cloud computing, security in clouds is a major concern. Clouds are still vulnerable, and hackers are exploiting these security flaws. Security issues must be detected in order to provide better service to cloud users. In this paper, we discuss cloud computing cybersecurity concerns, countermeasures, and data encryption techniques. In the future, we will continue to contribute to initiatives to analyze cloud security threats and responses to cloud security breaches. Furthermore, we intend to build and develop unique security countermeasures that will allow IT firms to use cloud technology without concern, as well as to construct a security model that will use various encryption techniques for data concealment in cloud computing.

FUNDING: This work was funded by King Faisal University, Saudi Arabia [Project No. GRANT2,519].
ACKNOWLEDGMENTS: This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Project No. GRANT2,519].
CONFLICTS OF INTEREST: All authors declare no conflict of interest.

REFRENCES:

[1] Suthar, F., Khanna, S. V. O., & Patel, J. (2019). A survey on cloud security issues. International Journal of Computer Sciences and Engineering, 7(3), 120–123. https://doi.org/10.26438/ijcse/v7i3.120123
[2] Kumar, P.R., Raj, P.H. & Jelciana, P., 2018. Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 125, pp.691–697.

[3] Hemalatha, N., Jenis, A., Cecil Donald, A., & Arockiam, L. (2014). A comparative analysis of encryption techniques and data security issues in cloud computing. International Journal of Computer Applications, 96(16), 1–6. https://doi.org/10.5120/16875-6873

[4] Harfoushi, O., Alfawwaz, B., Ghatasheh, N. A., Obiedat, R., Abu-Faraj, M. M., & Faris, H. (2014). Data security issues and challenges in cloud computing: A conceptual analysis and Review. Communications and Network, 06(01), 15–21. https://doi.org/10.4236/cn.2014.61003

[5] Anand, Abhineet & Trivedi, Naresh & Kumar, Ajay. (2020). DATA SECURITY ISSUES AND THEIR SOLUTIONS IN CLOUD COMPUTING. Journal of Critical Reviews. 7. 2597-2604.10.31838/jcr.07.14.509.

[6] Shihab Ahmed, H. A., & Zolkipli, M. F. (2016). Data security issues in Cloud computing: Review. International Journal of Software Engineering and Computer Systems, 2, 58–65. https://doi.org/10.15282/ijsecs.2.2016.5.0016

[7] Chahal, Deepak & Kharb, Latika & Punia, Tarun. (2017). Data security in Cloud Computing.

[8] Vaidya, Chandu. (2020). Data Security in Cloud Computing.

[9] Albugmi, A., Alassafi, M. O., Walters, R., & Wills, G. (2016). Data Security in cloud computing. 2016 Fifth International Conference on Future Communication Technologies (FGCT). https://doi.org/10.1109/fgct.2016.7605062

[10] Rao, R. and Selvamani, K., (2015). Data Security Challenges and Its Solutions in Cloud Computing. Procedia Computer Science, 48, pp.204-209.

[11] Giri, S., (2019). Cloud Computing and Data Security Challenges: A Nepal Case. International Journal of Computer Trends & Technology, 67(3), pp.146-150.

[12] Subramanian, N. and Jeyaraj,(2018). Recent security challenges in cloud computing. Computers and Electrical Engineering, 71(1), pp.28-42.

[13] Chandramouli, N., (2017). A Study on Data Security and Privacy Protection Issues in Cloud Computing. International Journal of Computer Sciences and Engineering, 5(9).

[14] Nadeem, M., 2016. Cloud Computing: Security Issues and Challenges. Journal of Wireless Communications, 1(1).

[15] Bisong, A. and M. Rahman, S., (2011). An Overview of The Security Concerns In Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1), pp.30-45.

[16] Tabrizchi, H. and Kuchaki Rafsanjani, M., (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The Journal of Supercomputing, 76(12), pp.9493-9532.

[17] Mall, S. and Saroj, S., (2018). A New Security Framework for Cloud Data. ResearchGate 143:765-775

[18] Vurukonda, N. and Rao, T., (2016). A Study on Data Storage Security Issues in Cloud Computing. Procedia Computer Science. 92 , pp.128-135.

[19] Inukollu, V., Arsi, S. and Ravuri, S., (2014). Security issues in cloud computing in big data. Academia,6(2), pp1-13.

[20] Kalpana, P. and Singaraju, S., (2012). Data Security in Cloud Computing using RSA Algorithm. International Journal of Research in Computer and Communication technology, 1(4), pp 143-146.

[21] Soofi, A. and Amin, F., (2014). A Review on Data Security in Cloud Computing. International Journal of Computer Applications, 94(5), pp 12-20.

[22] Sun, Y., Zhang, J., Xiong, Y. and Zhu, G., (2014). Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks , 10(7), pp 1-9.

[23] Vimercati, S., Foresti, S. and Samarati, P., (2012). Managing and Accessing Data in the Cloud: Privacy Risks and Approaches., pp1-9

[24] Mahalle, V. S., & Shahade, A. K. (2014, October). Enhancing the data security in Cloud by imple menting hybrid (Rsa & Aes) encryption algorithm. In 2014 International Conference on Power, Autom ation and Communication (INPAC) (pp. 146-149). IEEE.

[25] Tebaa, M., El Hajji, S., & El Ghazi, A. (2012, April). Homomorphic encryption method applied to C loud Computing. In 2012 National Days of Network Security and Systems (pp. 86-89). IEEE.

[26] Kirubakaramoorthi, R., Arivazhagan, D., & Helen, D. (2015). Survey on encryption techniques use d to secure cloud storage system. Indian J. Sci. Technol, 8(36), 1-7.

[27] Rani, Preeti & Singh, Prem & Verma, Sonia & Ali, Nasir & Shukla, Prashant & Alhassan, Musah. (2022). An Implementation

of Modified Blowfish Technique with Honey Bee Behavior Optimization for Load Balancing in Cloud System Environment. Wireless Communications and Mobile Computing. 20 22. 10.1155/2022/3365392.

[28] Manreet &Sohal, Sandeep & Sharma. (2022). BDNA-A DNA inspired symmetric key cryptographi c technique to secure cloud computing,Journal of King Saud University, Computer and Information S ciences.34(1), 1417-1425

[29] M Basri, H Mawengkang, E & M Zamzami, (2018), Cloud Computing Security Model with Combin ation of Data Encryption Standard Algorithm (DES) and Least Significant Bit (LSB), Department of C omputer Science

[30] Singh, Santosh & Manjhi, Pankaj & Tiwari, R. (2016). IJARCCE Data Security using RSA Algorith m in Cloud Computing. 3297. 10.17148/IJARCCE.2016.5803.

[31] Thabit, F., Can, O., Alhomdy, S., Al-Gaphari, G. H., & Jagtap, S. (2022). A novel effective lightwei ght homomorphic cryptographic algorithm for Data Security in cloud computing. International Journal of Intelligent Networks, 3, 16–30. https://doi.org/10.1016/j.ijin.2022.04.001

[32] Gampala, Veerraju & Inuganti, Srilakshmi & Satish, Muppidi. (2022). Data Security in Cloud Com puting with Elliptic Curve Cryptography.