International Journal of Electrical and Computer Engineering (IJECE)
Vol. 13, No. 2, April 2023, pp. 1867~1879
ISSN: 2088-8708, DOI: 10.11591/ijece.v13i2.pp1867-1879

Cloud data security and various cryptographic algorithms

Yahia Alemami[1,2], Ali M. Al-Ghonmein[2], Khaldun G. Al-Moghrabi[2], Mohamad Afendee Mohamed[1]
[1]Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Terengganu, Malaysia
[2]Faculty of Information Technology, Al-Hussein Bin Talal University, Maan, Jordan

Article Info

Article history:

Received Jun 10, 2022
Revised Sep 25, 2022
Accepted Oct 21, 2022

Keywords:

Cloud computing
Cloud data security
Cryptographic algorithm
Encryption algorithm
Security algorithm

ABSTRACT

Cloud computing has spread widely among different organizations due to its advantages, such as cost reduction, resource pooling, broad network access, and ease of administration. It increases the abilities of physical resources by optimizing shared use. Clients' valuable items (data and applications) are moved outside of regulatory supervision in a shared environment where many clients are grouped together. However, this process poses security concerns, such as sensitive information theft and personally identifiable data leakage. Many researchers have contributed to reducing the problem of data security in cloud computing by developing a variety of technologies to secure cloud data, including encryption. In this study, a set of encryption algorithms (advance encryption standard (AES), data encryption standard (DES), Blowfish, Rivest-Shamir-Adleman (RSA) encryption, and international data encryption algorithm (IDEA) was compared in terms of security, data encipherment capacity, memory usage, and encipherment time to determine the optimal algorithm for securing cloud information from hackers. Results show that RSA and IDEA are less secure than AES, Blowfish, and DES). The AES algorithm encrypts a huge amount of data, takes the least encipherment time, and is faster than other algorithms, and the Blowfish algorithm requires the least amount of memory space.

Corresponding Author:

Khaldun G. Al-Moghrabi
Faculty of Information Technology, Al-Hussein Bin Talal University
Ma'an, Jordan
Email: Khaldun.g.moghrabi@ahu.edu.jo

1. INTRODUCTION

Cloud computing (CC) technology has gained wide popularity due to its capability to provide enormous resources to individuals and organizations which can be accessed via the internet anytime and anywhere worldwide [1], [2]. Many information and technology (IT) companies have shifted their operations to the cloud, which provides its users with a feature-rich cloud experience, including access to shared resources, which makes resources available when needed at lower costs. These resources may also be swiftly provided and released with minimal administrative effort, and CC provides the ability to share, manage, and store data, which is actually hosted on remote servers rather than using internal resources or personal devices [1]. Clients can use the cloud services of various programs by adopting CC rather than buying or installing the software on their own computers [3]. CC provides clients with virtualized resources using various technologies, such as web services, virtualization, applications, and operating systems [1]. The main advantages of CC can be summarized as cost reduction, increased productivity, stability, scalability easy management, and availability [4], [5].

Despite the above advantages of CC, it has given rise to various problems and challenges. Security is one of the greatest hurdles that hinder the acceptance of CC among users [1], [6]. It is a major concern that must be considered, and data security issues arise because client data and software are located on the provider’s premises [7]. If suitable security measures are not provided for data operations and transmissions, then they will be at great risk [8]. Thus, cloud service providers (CSPs) must protect data, applications, and cloud infrastructure from internal and external threats. The security of cloud information depends on the implementation of suitable information security measures and countermeasures, making the creation and management of a safe cloud environment a difficult operation. Protecting user data against malicious attacks and unreliable servers is crucial. The user data that have to be secured are [3]: i) usage data: data gathered from computers; ii) private data, such as bank account and health information; iii) personally identifiable data: data that might be used to define an individual; and iv) unique device identifiers: data that can be uniquely tracked, such as IP addresses.

Encryption is one of the safest methods that is used to prevent unwanted access. In CC environments, various types of encryption techniques have been used to protect user data and cloud information, which have contributed to reducing hacking to some extent. The data can be transformed into cipher text to increase their security. However, this process may lead to the loss of numerous features. Encrypted text can be obtained by using two popular techniques. The first technique is based on a safety index, which creates a secure cipher text keyword index by checking the keywords’ existence, and the second technique is based on scanning cipher text, which compares each word to ensure that the keywords are in the cipher text [3].

Numerous researchers have focused on finding various answers to the CC data security issue [9]. Further research is needed to understand the cloud’s associated security and privacy problems. This study provided a recent review of cloud security issues, challenges, and threats to cloud adoption, and encryption algorithms that are used in cloud environments. A comparison was made between the most important encryption algorithms that can be used to provide greater cloud security.

The rest of this article is organized as: section 2 describes the architecture of cloud security in detail. Section 3 introduces the security issues in cloud CC. Section 4 conducts a literature review. Section 5 presents the results and discussion of the study. Section 6 provides the conclusion.

2. ARCHITECTURE OF CLOUD SECURITY

2.1. Explaining cloud computing

CC is a metaphor for describing the web as a place where computing has been preinstalled and is available as a service, where data, applications, operating systems, storage, and processing capacity are all available on the web and ready to be shared among customers [2]. CC refers to a collection of data centers that connect to the internet to offer their services, and these data centers are based on the virtualization of their infrastructure [10]. CC is technologically based on infrastructure, software platform, operating system, cloud app development, database management, system and app management software, Internet, and network [2]. CC service providers are companies that provide their customers with CC resources and services that are used dynamically at the request of the customer in accordance with a particular business model. Figure 1 shows the relationship between the most common CC service providers, such as Amazon, Google, Microsoft, and IBM.

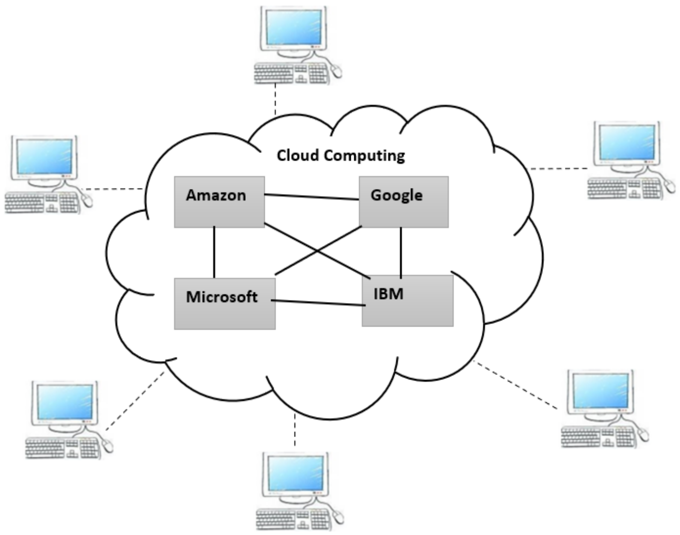

Figure 1. Cloud computing

2.2. Cloud deployment model

CC is classified into three types [9], [11], [12]: private, public, and hybrid cloud. Private clouds are managed and overseen only for a solitary organization, and the assets are not used by other clients, which indicates that they are protected from being accessed by unauthorized users. Public clouds are available to the general public and organizations. The assets are shared between every one of the clients. The clients pay the cloud owner depending on the service provided and the assets they utilize. CSPs manage the physical infrastructure, which is located away from the clients. Hybrid clouds are a mix of the above two types (public and private) [1], [10].

2.3. Service models

CC provides three key services, namely, software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) [1], [9], [11].

- IaaS: It refers to CSP hardware infrastructure, which includes networks, storage, memory, processors, and a variety of other computing resources. The resources are provided as virtualized systems that can be accessed via the internet. The essential resources are under the control of the CSP [1].
- PaaS: It provides integrated development environments, middleware, operating systems, and platform layer resources through a third-party provider who delivers hardware and software tools to users over the Internet. PaaS does not give customers control over the underlying cloud infrastructure, but only over the applications that are moved to the cloud.
- SaaS: It allows consumers to use applications as a service over the internet. Users can simply use the internet to access it rather than buy, install, and maintain software. Customers pay for usage rather than ownership of the software.

The CC system is divided into two sections: the front end and the back end. They communicate with each other through a network, usually over the internet. The front end is the side that cloud clients see. The clients do not normally see the back-end section, which includes network connection, cloud servers, and their applications. Figure 2 shows the categories of cloud services and the architecture of CC.

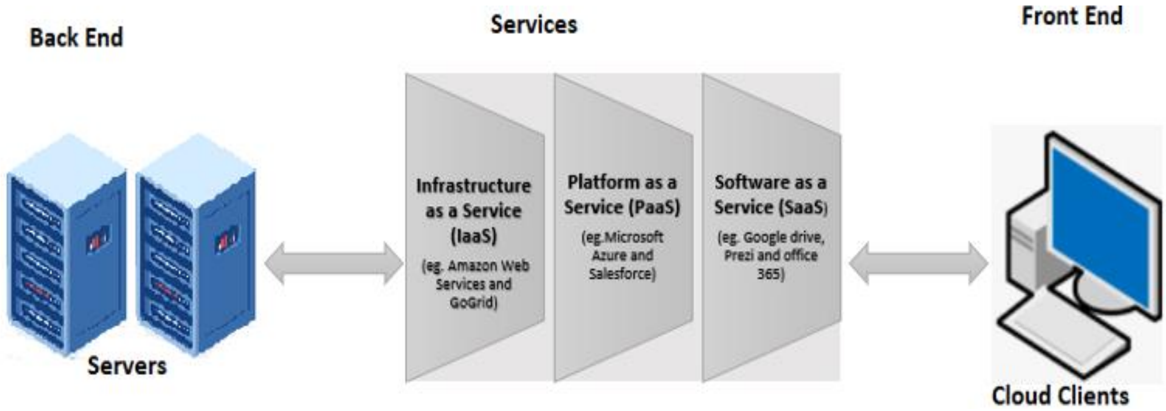
Back End
Services
Front End
Infrastructure as a Service (IaaS)
(eg. Amazon Web Services and GoGrid)
Platform as a Service (PaaS)
(eg.Microsoft Azure and Salesforce)
Software as a Service (SaaS)
(eg. Google drive, Prezi and office 365)
Servers
Cloud Clients

Figure 2. CC service model

2.4. Characteristics of cloud computing

CC satisfies many characteristics, which are [5], [13]–[15]:

- On-demand self-service: Cloud services (such as network storage, network access, and continuous monitoring of the server uptime) do not need any human managers. The clients themselves can provide, supervise, and manipulate computing resources and IT services as needed.
- Resource pooling: A CSP can share CC costs and resources (such as servers, storage, database, applications, networks, and services) among a large pool of users, allowing users connected to the cloud to use data simultaneously and to share cloud services according to their requirements.
- Broad network access: A user can access CC resources over the network from anywhere worldwide with an Internet connection and a device (e.g., smartphone, computer, and PDA).
- Rapid elasticity: Computing services and resources can be scaled up or down quickly and flexibly as needed.
- Economy: CC reduces huge IT expenses for its users. The user pays for the service used without having to invest in the computing infrastructure needed to operate and maintain the resources. No coverage or

additional fees must be paid in addition to allocating some services for free. Figure 3 shows the characteristics of CC.

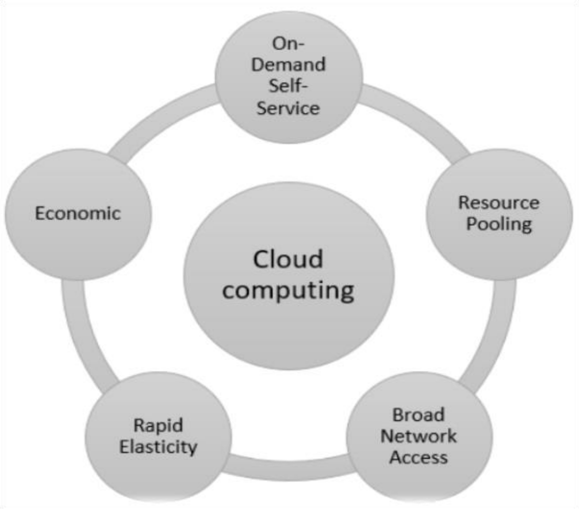

Figure 3. Characteristics of CC

2.5. Challenges of cloud computing

Customers of CC services encounter a variety of challenges, which are [16]–[18]:

- Regulatory compliance: Although client data is held by a service provider, clients are primarily responsible for the protection and integrity of their own information.
- Data isolation: when using the cloud, data is often shared with those other clients. Although encryption is useful, it is not a cure-all.
- Recovery: Although clients are unaware of the location of their data, a CSP should explain what will happen to their data and service in the event of a disaster.
- Location of data: when CC is employed, data are not exactly where they are hosted. Clients are unaware of the location in which their data will be kept.
- Network connection: In a cloud system, slow network connectivity causes performance bottlenecks when transferring data between data hubs and within the data center, and Internet disruption can lead to huge business losses.
- I/O operations do not considerably improve performance in a virtual environment when compared to shared memory and central processing unit (CPU) time. The bulk of high-performance computing applications needs all of the links that make the application run simultaneously.
- When errors occur in a cloud system, which has a wide user base, they can only be fixed in the production environment in real time. Resolving such problems may be difficult.
- Cloud services must always be available. Servers should withstand distributed denial of service attacks and power outages.
- Protecting the confidentiality and privacy measures of sensitive client data is the main challenge of CC because they are under the maintenance and supervision of a third party.
- Abuse of the cloud services for malicious purposes.
- Protect and preserve data from loss, hacking, and theft.

Network security, communication level, big data storage, storage and computational performance, maintenance, edge computing web app protection, confidentiality, reliability, information integrity, access to data, authentication, and data leakage are additional issues that need to be addressed.

3. SECURITY ISSUES IN CLOUD

The security of a cloud data center is mostly identical to those of a noncloud data center [9], [19]. Keeping CC safe from any threats is necessary. Some privacy and security-related issues that are thought to be important for CC are [19]:

- Malicious insiders: a malicious insider is a person who has authorized access to an organization's network and data and uses these powers in a manner that compromises the organization's information and information systems' confidentiality and integrity. Most organizations are aware of this hazard because it is difficult to detect and has a remarkable effect on the organization.
- Account or service hijacking: this threat arises because of fraud and software flaws. In this case, an attacker can gain access to sensitive regions on the cloud, in which he can steal permits and sensitive data.
- Hypervisor vulnerabilities: a hypervisor is the most important piece of software in virtualization. Hypervisors have obvious security vulnerabilities, and remedies are still restricted and often proprietary.
- Insecure interfaces and application programming interfaces (APIs): If a poor set of interfaces and APIs are used, then organizations may face security threats, such as unknown access, reuse of passwords, the transmission of content or clear text authentication, and inflexible access management or invalid authorizations.
- Cyber-attacks: hacking and cyber-attacks on networks have increasingly become a grave threat in recent years.

4. LITERATURE REVIEW

The timely execution of encoding data is one of the most serious challenges encountered during data processing and transmission over the Internet. Focusing on privacy concerns, the researchers introduced the dynamic data encryption strategy (D2ES), a new data encryption strategy that attempts to selectively encrypt data using privacy categorization methods while adhering to time constraints. The privacy of this new method has been improved. However, concerns about maintaining the privacy of data owners are found in accordance with the report. Unencrypted data transmissions are one of the main sources of concern. The suggested method consists of two primary techniques: i) identifying data bundles in accordance with their level of privacy and ii) determining whether data bundles can be enciphered within the time constraints. The dynamic encryption determination algorithm was created to provide alternate data bundles for encipherment under varying timing constraints, and it was the fundamental algorithm underpinning the D2ES architecture. The evaluations reveal that the proposed methodology has a powerful performance [20]. users must utilize an encryption mechanism to keep their data safe in the cloud [21]. The user has no idea where their information is saved on the cloud and is concerned about its information protection. Cyber laws in every country vary. The legality and confidentiality of information are the main concerns. The researchers used homomorphic encryption, which ensures that the data is kept private. The proposed technique is tested in the public cloud of Amazon Web Services.

Vijayakumar *et al.* [22] mentioned that in the current period of information technology, most organizations are moving toward the cloud to save and manage information due to decreased cost, flexibility, regular access, and invigorated programming. They pointed out that healthcare service systems are modifying mechanized stages and winding up being focused on patient-centered information. These systems exhibit an arranging empowered intermediary re-encryption strategy to solve the security flaws for the protection of patient information in healthcare fields, where this method allows authorized people to access the records for a specific timeframe. The suggested framework gives the information owner the ability to select the client who will be granted permission to search directly without disclosing his private key. In an offline state, a key generation attack is a possible threat. The researchers utilized public keyword search with proxy re-encipherment to counteract this threat, which makes keyword guessing more difficult. The Diffie-Hellman algorithm was used by the researchers to produce a shared private key between two parties. It is mostly used to exchange cryptography keys for use in symmetric encryption methods, such as advanced encryption standard (AES). They created a hybrid metaheuristic algorithm to reduce the latency, processing costs, load balancing, and energy consumption of the internet of things (IoT).

Arora and Parashar [23] compared the AES, data encryption standard (DES), Blowfish, and Rivest-Shamir-Adleman (RSA) algorithms to determine the optimum security algorithm for usage in the cloud to keep cloud information safe from hackers. The AES algorithm takes the least amount of time to execute cloud information, the Blowfish algorithm requires the least amount of memory, the DES algorithm takes the least amount of encoding time, and RSA consumes the most memory and encoding time. Singh and Sharma proposed the idea of storing information on many cloud servers utilizing encryption as opposed to putting away a whole record on a single system. For the encipherment of the section of a file in the cloud, a model that combines the AES algorithm and some components of the secure hash algorithms-1 (SHA-1) algorithm was proposed. In the proposed approach, efforts are exerted to diverge the file into distinct pieces, followed by encipherment and storage on a different cloud [24]. Lee *et al.* [25] used Heroku as a cloud system and used the AES algorithm for information security in Heroku, which relies on a managed container framework, coordinated information services, and a strong ecological system for deploying and executing modern apps.

The AES method can be utilized for data security in accordance with the performance evaluation results. They pointed out that Heroku supports the expansion of the cloud platform because it is free. Despite Heroku being free, it can integrate with information services, and developers can construct frameworks using programming languages with Heroku. Heroku supports several programming languages, including Java, PHP, and Python.

Cloud-based encryption and decryption algorithms can improve the online examination system [26]. For this process testing, they did not apply any encryption or decryption algorithms. Although online tests have been widely employed by universities and colleges at all academic levels, they do have one major drawback: the internet connection can be lost. A cutting-edge online examination system capable of overcoming the aforementioned flaw was proposed. Examinees can answer e-question papers without fear of losing Internet connection if the proposed approach is implemented. More *et al.* [27] suggested a crypto framework for secure cloud information, which combines attribute-based encryption (ABE) and byte rotation encryption algorithm (BREA) to provide additional security and protection to cloud information sharing and coordinated activities. The attributes of the information to be uploaded will be recognized by the ABE algorithm. These attributes will aid the BREA in determining the type of information to be enciphered. The BREA will execute single, multi, or hybrid phase encoding after determining the file’s information type. Following the encoding of the data, the ABE will generate a random key that will allow the user to decode the encoded text. This proposed technique has been used in cloud-based banking systems.

Attar and Shahin [28] mentioned that the cloud provides many benefits for businesses and customers, such as lower costs and more flexibility. Integrity, availability, confidentiality, privacy, and confidentiality are the most common security concerns in the cloud. The AES algorithm was employed. The suggested method is divided into two parts. The first part is to load data on a cloud server, and the second part is to download data from a cloud server to the client’s PC. The security of the client’s information was examined in the two areas. The experiments were conducted by using a machine with a dual-core Intel processor running at 2.5 GHz, 4 GB of RAM, a 500 GB hard drive, and a Linux operating system. The proposed algorithm (AES) encrypts files faster and with more security than DES and Blowfish. Abdulhamid *et al.* [29] pointed out that most CC apps do not provide a high level of security, such as data protection, secrecy, and integrity. Thus, users must utilize a cloud encryption system to encrypt data before storing them in the cloud. The Blowfish encryption technique was applied in their study. The suggested encryption architecture was tested on a Microsoft Azure cloud server. Secure communication protocol hypertext transfer protocol secure (HTTPS) was used to send encrypted messages to the cloud by using C# programming language. The proposed method adds an extra layer of security by encrypting data before transferring them to the cloud.

Kumar *et al.* [30] demonstrated that many IT firms and educational institutions are realizing that by simply switching to the cloud, they may instantly access used PC applications and effectively manage infrastructure resources at a low cost. An encryption technique for information security was enhanced to provide security to cloud users. The proposed technique uses a binary tree, where every node contains a letter, integer, or special character, and each link has a binary value of 0 or 1. Hackers will find that the proposed technique is difficult to use because numbers increase security while accessing information. Sajay *et al.* [31] indicated that security is the fundamental issue related to CC. In the cloud, the models of security are confidentiality, verification, information recuperation, and information integrity. The proposed technique, which is a combined algorithm to improve the security of cloud information by applying an encipherment algorithm, including homographic encipherment and Blowfish encipherment, uses Python programming and cryptography to improve the cloud security. The homographic encipherment is applied to the main layer, which is applied to the input text and is then passed to the second layer, which is the Blowfish encipherment layer. The proposed algorithm provides a security strategy and better stockpiling utilizing encipherment algorithms over the cloud architecture. The results show that if the security challenges are fixed, then small and large enterprises will be safe when storing data in the cloud.

Subashanthini and Pounambal [32] proposed a method for resolving the security issue in electronic commerce in the business world and presented a unified system for storing image data in the cloud. Integer wavelet transform (IWT), chaotic maps, and the deoxyribose nucleic acid (DNA) encoding rule were combined in a three-organize picture encoding process. The proposed method employs five degrees of protection by generating five key sequences through five different chaotic maps. A grayscale image was partitioned into 8×8 blocks, and key 1 was formed by randomly selecting 8×8 blocks using a logistic map. Key 2 was created by using a line map. A tent map was used to make key 3, and a Henon map was applied to make key 4. The resulting mixed block is decoded by selecting a DNA rule using key 5, which is generated by using a sine map. The findings of several measurements and analysis metrics on the suggested work are: entropy=7.99, PSNR=9 dB, and correlation is approximately zero. Differential and brute force attacks are likewise resistant to the proposed strategy.

Xu *et al.* [33] stated that despite the improvement of electronic healthcare systems, issues on ensuring the accuracy and protection of doctors' recommendations to users are still found. Two algorithms based on the modified Paillier cryptosystem, truth discovery technology, and the Dirichlet distribution were proposed to protect privacy. The proposed scheme (PPMR) is a privacy-preserving online medical service recommendation schema for electronic healthcare systems that assists users in finding the right doctor. The proposed PPMR scheme is found to be secure after a security analysis. The sensitive data (for example, clients' needs and doctors' data) are protected in the proposed strategy. Client requests and doctor data are compared in ciphertext form in this approach. This method contains three steps: system initialization, doctor suggestion, and user feedback to determine the doctor's reputation. Individual health data are outsourced to be stored in the cloud to ensure that patients retain ownership over their data, and the data should be encrypted and stored in a database in accordance with the information presented. A cloud-based mobile health monitoring system was developed to ensure the privacy of users' data. The SHA 512 algorithm was used for attribute-based encoding and decoding on the basis of specific information. The proposed technology generates medicine that is appropriate for the patient. IBM-Bluemix is an IBM cloud that provides PaaS, IaaS, and SaaS to customers who want to keep their businesses running on the cloud at a cheaper cost. Bluemix provides a variety of services to keep your security up to date. ClearDb is used as a database service for storing client information [34]. Shah and Philip mentioned that authentication plays a vital role in data security. Biometrics were used for authentication to create a biometric-based cloud for online signature acknowledgment on a Windows Tablet PC, making the signature recognition system more scalable, pluggable, and faster. This process was implemented on the Microsoft Azure public cloud. Signature recognition is one of the most important study areas in the realm of biometric-based identity recognition that may be used successfully in banking applications and Internet commerce. Their study aims to promote online signature acknowledgment in banking applications, where it can be simple to reveal erroneous or fraudulent bank checks. The proposed method achieves a 90% increase in execution speed [35].

Malviya and Dave [36] pointed out that information trustworthiness and information privacy are two important things for open cloud environments. A secure data sharing scheme for dynamic groups in open cloud environments was developed. A customer can share information with others in the group by using the suggested system without jeopardizing cloud privacy. Admin, cryptographic server, and user are the three key components of the proposed system. A cloud is a place where safe data sharing is possible. The data owner module was enhanced to handle unexpected client panel operations and to prevent unauthorized users from gaining access to the system. The AES technique was used to encrypt the data, and the homomorphic (Paillier) algorithm was used to encrypt the key in the proposed work. JAVA was used to complete the task, and JSP was used to deploy the web application. The suggested approach is secure and efficient for exchanging data files in the public cloud among several users. Dong *et al.* [37] developed a framework called SecureMR that analyzes and transforms MapReduce applications to work over encoded data. Homomorphic encryption was used by SecureMR, which was assessed on a number of MapReduce benchmarks. According to Wu *et al.* [38] the medical IoT (mIoT), which is backed by the outstanding processing capacity of the cloud and the effective information collection of medicinal sensors, is one of the most prominent breakthroughs. Security remains a major concern in the mIoT because the information is transmitted over an open network. Although encryption techniques may help to maintain patient privacy, they may impede future retrieval of the encrypted data. Public-key encryption with keyword search was proposed to overcome this restriction. The guessing attack in information search was identified as a severe security risk. A reliable public key verified encryption method with a designated tester (CL-dPAEKS) was proposed to address these issues. This method is suitable for the mIoT and contains polynomial-time algorithms. CL-dPAEKS can withstand all types of attacks and is relatively secure.

Namasudra [39] proposed an efficient and secure CC data sharing access control model based on ABE, a distributed hash table (DHT) network, and identity-based timed-release encryption (IDTRE). Information was encoded by using client characteristics, and the encoded information was divided into encapsulated and extracted ciphertexts. IDTRE was used to encrypt the decryption key, and the key's ciphertext was combined with the retrieved ciphertext to generate the ciphertext shares. The DHT network was used to distribute the ciphertext shares, and the ciphertext was stored on cloud servers. The findings indicate that the proposed method is safe, efficient, and has a remarkable effect on the IoT. Sarode and Bhalla [40] indicated that mobile CC (MCC) is a fast-developing invention at present. Data protection and security are important considerations when using a mobile device. Network security, web application security, information access, authentication, authorization, data confidentiality, and data breach are all concerns of MCC's security. Mobile devices lack sufficient storage and processing speed. Thus, a strategy that uses AES and RSA was devised to provide flawless security and to improve the security of the mobile cloud. The AES algorithm was used initially because it is faster than RSA in terms of encoding. The AES will convert the original text into a quick response (QR) code during the encoding stage. This QR code will be scanned with the help of the decipherment technique, and the cipher text will be converted to a QR code by using the RSA algorithm. The AES algorithm will then decode the QR code back to plain text. In the mobile cloud, the proposed technique ensures information security and integrity of data and applications.

Cloud-based electronic health record (EHR) technology has revolutionized health care. A secure EHR searching approach that relies on conjunctive keyword searches and proxy re-encoding for information transfer between medical organizations has been provided. It investigates public key encryption with conjunctive keyword search to encrypt the original material and store it on the cloud, ensuring information security while allowing for searchability. The identity-based access control methodology and proxy re-encoding methods are implemented to ensure the validity of access and the privacy of the original material [41]. Hiemenz and Krämer [42] presented a dynamic searchable symmetric encipherment method permitting clients to safely store geospatial information in the cloud. Geospatial information frequently includes critical data, such as urban infrastructures. The genuine geospatial records are enciphered by utilizing the AES algorithm to guarantee secrecy. Searchable symmetric encipherment is appropriate in geospatial document stockpiling, and the suggested method can protect users' information. Chauhan *et al.* [43] demonstrated many smart learning strategies that aid in the enhancement of the smart virtual interactive environment for work (SVIEW). The proposed method aims to increase efficiency at SRM University's workplace, improve student learning, save power, reduce considerable time, and make life easier for everyone (students, staff, and the board). SVIEW is customizable and can be used at various institutions. In the proposed work, a teacher's fingerprint is used to control the study hall's electrical equipment. The system's goals are to make the university smart and assist lecturers in resolving the concerns raised in the university. AES, which takes less time to encrypt and decrypt, is used to encrypt data.

Xiong and Shi [44] developed two new safe reversible data hiding over encrypted image techniques. The first technique is reversible data hiding by homomorphic encipherment, and the second technique is reversible data hiding in an enciphered domain. These techniques are suitable for preserving image privacy and transferring extra information in cloud data services, where the EIGamal algorithm is employed. Cybersecurity assaults have undermined clients' information privacy and protection in medical cyber-physical systems (MCPSs). Conventional standard encipherment algorithms for information protection (EHR for MCPS), were created depending on the system architecture as opposed to the viewpoint of clients. A safe methodology for data stockpiling and conveying was proposed. This method comprises a selective encipherment algorithm combined with fragmentation and dispersion to ensure information security and protection. The main idea of the SE algorithm is to splinter the digital information in a manner that makes various information parts related [45].

CC is one of the most researched topics in IT, and cloud information security is one of the top concerns for any organization that considers shifting to the cloud. Goyal and Kant [46] created and tested a variety of algorithms for securing cloud data, including AES, SHA-1 (hashing method), and elliptic curve cryptography (ECC). Every encipherment and decipherment procedure in the proposed technique uses two different keys. Kumar and Roberts [47] proposed a new architecture based on digital signatures as a means of reducing the economic denial of sustainability (EDoS) from the cloud. Kumar and Shafi [48] used a modified RSA technique to increase the security for cloud-stored data. Teng *et al.* [49] presented a modified AES by using master choreography and column mixing. Experiments were conducted on the Hadoop platform. Abroshan [50] combined an elliptic curve-based technique with an enhanced Blowfish algorithm. The security and performance are improved by using the two techniques to encrypt the data. Awan *et al.* [51] proposed an improved 128 AES method to accelerate the encryption process. The improved technique uses less power, better load balancing, and improved trust and resource management on the network. Kumar *et al.* [52] developed a novel approach using the autonomic resource provisioning and scheduling (ARPS) framework combined with the spider monkey optimization (SMO) algorithm. The effectiveness of the proposed approach was assessed by using the CloudSim framework. It achieves good results in terms of processing time, cost, and energy consumption.

Mata *et al.* [53] utilized hybrid cryptographic techniques (AES and Blowfish) in their study. Progressively introducing more complicated functions increases the security of data storage in CC. Dubey *et al.* [54] aimed to allocate the best possible resources for IoT applications by combining the features of two metaheuristic-based methodologies, cuckoo search optimization (CSO), and particle swarm optimization (PSO). The simulation outcomes show that the suggested hybrid algorithm may allocate the services more effectively. The computational results in [55] show that the improved binary PSO (BPSO) algorithm, which is based on a transfer function, is more effective in optimizing several quality-of-service metrics, such as makespan time, energy consumption, and execution cost. Goyal and Kant [46] devised a new hybrid algorithm for protecting cloud data and used it in practice. The proposed algorithm combines AES, SHA-1 (a hashing technique), and ECC. Khakim *et al.* [56] secured the password using the MD5 algorithm and encrypted the data using AES with a key length of 256 bits. The proposed method prevents anyone to hack the login data in the cloud. Orobosade *et al.* [57] proposed a method using ECC as the following encryption technique with an AES key, and AES key as the first-level data encryption process before storing data in the cloud. The literature review is summarized in Table 1.

Table 1. Framework and techniques utilized

Research author	Framework	Techniques utilized
Gai *et al.* [20]	Cloud (generally)	D2ES
Potey *et al.* [21]	Amazon Web	Homomorphic
Vijayakumar *et al.* [22]	Healthcare area	Diffie–Hellman, AES
Mathur *et al.* [58]	Cloud (generally)	SHA-1, AES
Lee *et al.* [25]	Heroku	AES
Biswas *et al.* [26]	Online examination system	Not used
More *et al.* [27]	Banking systems	ABE and BRE algorithm
Attar and Shahin [28]	Cloud (generally)	AES
Abdulhamid [29]	Microsoft Azure	Blowfish
Kumar *et al.* [30]	IT organizations	Binary tree
Sajay [31]	Organizations	Homographic, Blowfish
Subashanthini and Pounambal [32]	Electronic commerce	IWT, chaotic maps, and DNA
Xu *et al.* [33]	Electronic healthcare systems	Modified Paillier cryptosystem, truth discovery technology, and the Dirichlet distribution
Naidu *et al.* [34]	Bluemix	SHA 512
Philip and Shah [35]	Microsoft Azure	Biometrics for authentication
Malviya and Dave [36]	Open cloud	Homomorphic, AES
Dong *et al.* [37]	SecureMR	Homomorphic
Wu et al. [38]	mIoT	Public key encipherment with keyword search
Namasudra [39]	IOT	ABE, distributed hash network, and identity-based timed-release encryption
Sarode and Bhalla [40]	MCC	AES, RSA, and QR code
Wang *et al.* [41]	EHR	Public key encipherment with conjunctive keyword search
Hiemenz and Krämer [42]	Geospatial	AES
Chauhan *et al.* [43]	SRM University	Teacher’s fingerprint, AES
Qiu *et al.* [45]	EHR	Selective encipherment algorithm combined with fragmentation and dispersion
Goyal and Kant [46]	IT industry	AES, SHA-1, and ECC
Kumar and Roberts [47]	CC	Digital signatures
Kumar and Shafi [48]	CC	modified RSA
Teng *et al.* [49]	Hadoop	improved AES
Abroshan [50]	CC	Elliptic curve technique and enhanced Blowfish
Awan *et al.* [51]	CC	Enhanced AES (128)
Kumar *et al.* [52]	ARPS and CloudSim	SMO algorithm
Mata *et al.* [53]	CC	AES and Blowfish
Dubey *et al.* [54]	Fog CC	CSO and PSO
Kumar *et al.* [55]	CC	BPSO
Goyal and Kant [46]	CC	AES, ECC, and SHA-1
Khakim *et al.* [56]	CC	MD5 and AES (256)
Orobosade *et al.* [57]	CC	ECC and AES

5. RESULTS AND DISCUSSION

Encryption algorithms play an essential role in cloud data security. International data encryption algorithm (IDEA), AES, RSA, Blowfish, and DES algorithms are compared to determine the best security algorithm. The assessment results are shown in Table 2. Table 2 shows that RSA is an asymmetric algorithm, and IDEA, AES, Blowfish, and DES are symmetric algorithms. RSA and IDEA are less secure than AES, Blowfish, and DES). In this study, the AES algorithm takes the least amount of time to encipher cloud information, the Blowfish algorithm requires the least amount of memory space, and the AES algorithm can be used for encrypting huge amounts of data. The AES is faster than other algorithms and is the best algorithm in terms of authentication parameters. The RSA consumes the most memory and requires maximum encipherment time. Figure 4 shows the comparison of encryption algorithms with respect to the security level, data encipherment capacity, authentication, memory utilization, and encryption time.

Table 2. Assessment results between IDEA, AES, RSA, Blowfish, and DES algorithms

Algorithm					Parameters
IDEA	AES	RSA	Blowfish	DES	
Cloud	Cloud	Cloud	Cloud	Cloud	Platform
Symmetric	Symmetric	Asymmetric	Symmetric	Symmetric	Cipher type
Only secure for the client	Secure for both client and provider	Only secure for the client	Secure for the client and provider	Secure for the client and provider	Security level
Encipherment of small amount of data	Encipherment of huge amount of data	Encipherment of small amount of data	Less than AES	Less than AES	Data encipherment capacity
Less than AES	The best	Strong	Identical to AES	Less than AES	Authentication
Requires high memory space	Requires low memory space	Requires the highest memory space	Requires the least memory space	More than AES	Memory utilization
needs max time	Faster than other algorithms	needs max time	More than AES	More than AES	Encipherment time

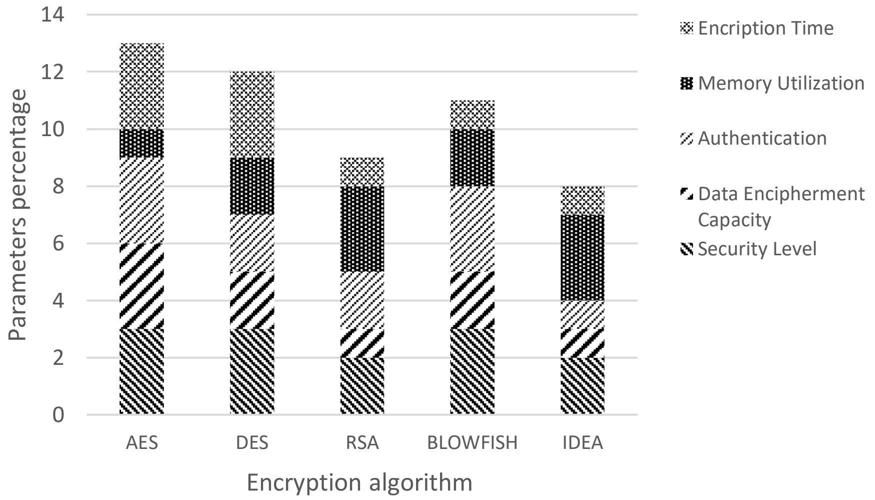

Figure 4. Comparison of algorithms

6. CONCLUSION

CC is one of the latest trends in the IT field and provides a variety of benefits to clients. Cloud information security is one of the top concerns for any organization that considers shifting to the cloud. Therefore, researchers mostly focus on this topic. Encryption is one of the safest solutions for blocking unauthorized access. Different encryption techniques are used in cloud environments to secure cloud data, which contributes to reducing hacking to some extent. This study provided a recent review of cloud security issues, challenges to cloud adoption, and encryption algorithms that are used in cloud environments. The framework and techniques utilized in a number of previous studies were summarized. A literature review was conducted in the field of cloud data security in which the encryption algorithms of RSA, AES, DES, Blowfish, and IDEA were compared, to find the optimal security algorithm for cloud data protection. The results show that RSA is an asymmetric algorithm, and IDEA, AES, Blowfish, and DES are symmetric algorithms. RSA and IDEA are less secure than AES, Blowfish, and DES, and the Blowfish algorithm requires the least amount of memory space. The AES algorithm can be used for encrypting huge amounts of data. The AES is faster than other algorithms and is the best algorithm in terms of authentication parameters. The RSA consumes the most memory and requires maximum execution time. The researchers suggest the use of hybrid encryption algorithms, such as AES and Blowfish, to obtain more security and complexity for hackers.

REFERENCES

[1] M. Ali, S. U. Khan, and A. V. Vasilakos, “Security in cloud computing: Opportunities and challenges,” *Information Sciences*, vol. 305, pp. 357–383, Jun. 2015, doi: 10.1016/j.ins.2015.01.025.

[2] M. N. O. Sadiku, S. M. Musa, and O. D. Momoh, “Cloud computing: Opportunities and challenges,” *IEEE Potentials*, vol. 33, no. 1, pp. 34–36, Jan. 2014, doi: 10.1109/MPOT.2013.2279684.

[3] A. A. Soofi, M. I. Khan, and Fazal-e-Amin, "A review on data security in cloud computing," *International Journal of Computer Applications*, vol. 94, no. 5, pp. 12–20, May 2014, doi: 10.5120/16338-5625.

[4] B. M. Shereek, "Improve cloud computing security using RSA encryption with Fermat's little theorem," *IOSR Journal of Engineering*, vol. 4, no. 2, pp. 01–08, Feb. 2014, doi: 10.9790/3021-04260108.

[5] S. Kamarudin, A. H. A. Khalili, Z. F. Abd. Aziz, K. A. Kamarudin, and A. N. A. Wahab, "Exploring of potential of cloud computing for small and medium enterprises," *Indonesian Journal of Information Systems*, vol. 4, no. 2, pp. 98–108, Feb. 2022, doi: 10.24002/ijis.v4i2.5487.

[6] D. A. B. Fernandes, L. F. B. Soares, J. V Gomes, M. M. Freire, and P. R. M. Inácio, "Security issues in cloud environments: a survey," *International Journal of Information Security*, vol. 13, no. 2, pp. 113–170, Apr. 2014, doi: 10.1007/s10207-013-0208-7.

[7] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A systematic literature review on cloud computing security: threats and mitigation strategies," *IEEE Access*, vol. 9, pp. 57792–57807, 2021, doi: 10.1109/ACCESS.2021.3073203.

[8] R. V. Rao and K. Selvamani, "Data security challenges and its solutions in cloud computing," *Procedia Computer Science*, vol. 48, pp. 204–209, 2015, doi: 10.1016/j.procs.2015.04.171.

[9] S. Singh, Y.-S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *Journal of Network and Computer Applications*, vol. 75, pp. 200–222, Nov. 2016, doi: 10.1016/j.jnca.2016.09.002.

[10] B. S. P. Mishra, H. Das, S. Dehuri, and A. K. Jagadev, *Cloud computing for optimization: Foundations, applications, and challenges*, vol. 39. Cham: Springer International Publishing, 2018.

[11] K. G. Al-moghrabi, A. M. Al-ghonmein, and M. Z. Alksasbeh, "Towards a cloud computing success model for hospital information system In Jordan," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 10, no. 2, pp. 1121–1127, Apr. 2021, doi: 10.30534/ijatcse/2021/891022021.

[12] Z. N. Rashid, S. R. M. Zebari, K. H. Sharif, and K. Jacksi, "Distributed cloud computing and distributed parallel computing: A review," in *2018 International Conference on Advanced Science and Engineering (ICOASE)*, Oct. 2018, no. June, pp. 167–172, doi: 10.1109/ICOASE.2018.8548937.

[13] M. Almubaddel and A. M. Elmogy, "Cloud computing antecedents, challenges, and directions," in *Proceedings of the International Conference on Internet of things and Cloud Computing*, Mar. 2016, pp. 1–5, doi: 10.1145/2896387.2896401.

[14] T. Diaby and B. B. Rad, "Cloud computing: A review of the concepts and deployment models," *International Journal of Information Technology and Computer Science*, vol. 9, no. 6, pp. 50–58, Jun. 2017, doi: 10.5815/ijitcs.2017.06.07.

[15] S. A. Bello *et al.*, "Cloud computing in construction industry: Use cases, benefits and challenges," *Automation in Construction*, vol. 122, Feb. 2021, doi: 10.1016/j.autcon.2020.103441.

[16] N. Subramanian and A. Jeyaraj, "Recent security challenges in cloud computing," *Computers & Electrical Engineering*, vol. 71, pp. 28–42, Oct. 2018, doi: 10.1016/j.compeleceng.2018.06.006.

[17] M. Mohammed Sadeeq, N. M. Abdulkareem, S. R. M. Zeebaree, D. Mikaeel Ahmed, A. Saifullah Sami, and R. R. Zebari, "IoT and cloud computing issues, challenges and opportunities: A review," *Qubahan Academic Journal*, vol. 1, no. 2, pp. 1–7, Mar. 2021, doi: 10.48161/qaj.v1n2a36.

[18] A. T. Atieh, "The next generation cloud technologies: A review on distributed cloud, fog and edge computing and their opportunities and challenges," *Research Berg Review of Science and Technology*, vol. 1, no. 1, pp. 1–15, 2021.

[19] S. S. Khan and R. Tuteja, "Security in cloud computing using cryptographic algorithms," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 03, no. 01, pp. 148–154, Feb. 2015, doi: 10.15680/ijircce.2015.0301035.

[20] K. Gai, M. Qiu, and H. Zhao, "Privacy-preserving data encryptionstrategy for big data in mobile cloud computing," *IEEE Transactions on Big Data*, vol. 7, no. 4, pp. 1–1, 2017, doi: 10.1109/TBDATA.2017.2705807.

[21] M. M. Potey, C. A. Dhote, and D. H. Sharma, "Homomorphic encryption for security of cloud data," *Procedia Computer Science*, vol. 79, pp. 175–181, 2016, doi: 10.1016/j.procs.2016.03.023.

[22] V. Vijayakumar, M. K. Priyan, G. Ushadevi, R. Varatharajan, G. Manogaran, and P. V. Tarare, "E-health cloud security using timing enabled proxy re-encryption," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 1034–1045, Jun. 2019, doi: 10.1007/s11036-018-1060-9.

[23] R. Arora and A. Parashar, "Secure user data in cloud computing using encryption algorithms," *International Journal of Engineering Research and Applications (IJERA)*, vol. 3, no. 4, pp. 1922–1926, 2013.

[24] H. Patel and B. Patel, "Stemmatizer-stemmer-based lemmatizer for Guajarati text," in *Springer*, vol. 841, 2019, pp. 667–674.

[25] B.-H. Lee, E. K. Dewi, and M. F. Wajdi, "Data security in cloud computing using AES under HEROKU cloud," in *2018 27th Wireless and Optical Communication Conference (WOCC)*, Apr. 2018, pp. 1–5, doi: 10.1109/WOCC.2018.8372705.

[26] S. Biswas, R. Roy, M. R. Chowdhury, and A. B. Bhattacharya, "On the advanced strategies of next generation online examination system implementing cloud based standardization: Next generation online examination system," in *2016 IEEE 6th International Conference on Advanced Computing (IACC)*, Feb. 2016, pp. 834–839, doi: 10.1109/IACC.2016.159.

[27] P. More, S. Chandugade, S. M. S. Rafiq, and P. Pise, "Hybrid encryption techniques for secure sharing of a sensitive data for banking systems over cloud," in *2018 International Conference on Advances in Communication and Computing Technology (ICACCT)*, Feb. 2018, pp. 93–96, doi: 10.1109/ICACCT.2018.8529545.

[28] N. Attar and M. Shahin, "A proposed architecture for data security in cloud storage space," *Journal of Biostatistics and Biometric Applications*, vol. 3, no. 2, pp. 1–7, 2018.

[29] S. M. Abdulhamid, N. A. Sadiq, M. Abdullahi, N. Rana, H. Chiroma, and D. E. Gbenga, "Development of blowfish encryption scheme for secure data storage in public and commercial cloud computing environment," in *2nd International Conference on Information and Communication Technology and Its Applications (ICTA 2018)*, 2018, pp. 231–237, doi: 10.26634/jcc.5.2.15690.

[30] S. Kumar, J. Shekhar, and J. P. Singh, "Data security and encryption technique for cloud storage," in *Conference: CSI-2015;50th Golden Jubilee Annual Convention on Digital Life*, 2018, vol. 729, pp. 193–199, doi: 10.1007/978-981-10-8536-9_19/COVER/.

[31] K. R. Sajay, S. S. Babu, and Y. Vijayalakshmi, "Enhancing the security of cloud data using hybrid encryption algorithm," *Journal of Ambient Intelligence and Humanized Computing*, no. 2018, Jul. 2019, doi: 10.1007/s12652-019-01403-1.

[32] S. Subashanthini and M. Pounambal, "Three stage hybrid encryption of cloud data with penta-layer security for online business users," *Information Systems and e-Business Management*, vol. 18, no. 3, pp. 379–404, Sep. 2020, doi: 10.1007/s10257-019-00419-6.

[33] C. Xu, J. Wang, L. Zhu, C. Zhang, and K. Sharif, "PPMR: A privacy-preserving online medical service recommendation scheme in eHealthcare system," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5665–5673, Jun. 2019, doi: 10.1109/JIOT.2019.2904728.

[34] R. C. A. Naidu, A. Srujan, K. Meghana, K. S. Rao, and B. Madhuravani, "Secure privacy preserving of personal health records Using attribute-based encryption in cloud computing," in *First International Conference on Artificial Intelligence and Cognitive Computing*, Springer Singapore, 2019, pp. 59–66.

[35] J. Philip and D. Shah, “Implementing signature recognition system as SaaS on Microsoft azure cloud,” in *Data management, analytics and innovation.*, vol. Springer, Springer Singapore, 2019, pp. 479–488.

[36] S. Malviya and S. Dave, “Secure data sharing scheme using cryptographic algorithm for cloud storage,” *International Journal of Applied Engineering Research*, vol. 13, no. 20, pp. 14799–14805, 2018.

[37] Y. Dong, A. Milanova, and J. Dolby, “SecureMR: Secure MapReduce using homomorphic encryption and program partitioning,” *ACM SIGPLAN Notices*, vol. 53, no. 1, pp. 389–390, Mar. 2018, doi: 10.1145/3200691.3178520.

[38] L. Wu, Y. Zhang, M. Mimi, N. Kumar, and D. He, “Certificateless searchable public key authenticated encryption with designated tester for cloud-assisted medical internet of things,” *Annals of Telecommunications*, vol. 74, no. 7–8, pp. 423–434, Aug. 2019, doi: 10.1007/s12243-018-00701-7.

[39] S. Namasudra, “An improved attribute-based encryption technique towards the data security in cloud computing,” *Concurrency and Computation: Practice and Experience*, vol. 31, no. 3, Art. no. e4364, Feb. 2019, doi: 10.1002/cpe.4364.

[40] R. P. Sarode and S. Bhalla, “Data security in mobile cloud computing,” *SSRN Electronic Journal*, pp. 1–6, 2019, doi: 10.2139/ssrn.3352362.

[41] X. Wang, A. Zhang, X. Xie, and X. Ye, “Secure-aware and privacy-preserving electronic health record searching in cloud environment,” *International Journal of Communication Systems*, vol. 32, no. 8, May 2019, doi: 10.1002/dac.3925.

[42] B. Hiemenz and M. Krämer, “Dynamic searchable symmetric encryption for storing geospatial data in the cloud,” *International Journal of Information Security*, vol. 18, no. 3, pp. 333–354, Jun. 2019, doi: 10.1007/s10207-018-0414-4.

[43] J. Chauhan, P. Goswami, and S. Patel, “Cloud based smart virtual interactive environment for work in Universities using IoT,” *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 8, no. 7S, pp. 250–258, 2019.

[44] L. Xiong and Y. Shi, “On the privacy-preserving outsourcing scheme of reversible data hiding over encrypted image data in cloud computing,” *Computers, Materials & Continua*, vol. 55, no. 3, pp. 523–539, 2018, doi: 10.3970/cmc.2018.01791.

[45] H. Qiu, M. Qiu, M. Liu, and G. Memmi, “Privacy-preserving health data sharing for medical cyber-physical systems,” *arXiv preprint arXiv:1904.08270*, vol. 1904, pp. 1–8, Apr. 2019, [Online]. Available: http://arxiv.org/abs/1904.08270.

[46] V. Goyal and C. Kant, “An effective hybrid encryption algorithm for ensuring cloud data security,” in *Big Data Analytics. Springer, Singapore*, 2018, pp. 195–210.

[47] M. Kumar and N. Roberts, “A technique to reduce the economic denial of sustainability (EDoS) attack in cloud,” *Elsevier*, vol. 7, no. 94, pp. 571–574, 2013.

[48] Y. K. Kumar and R. M. Shafi, “An efficient and secure data storage in cloud computing using modified RSA public key cryptosystem,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 530–537, Feb. 2020, doi: 10.11591/ijece.v10i1.pp530-537.

[49] L. Teng, H. Li, S. Yin, and Y. Sun, “A modified advanced encryption standard for data security,” *International Journal of Network Security*, vol. 22, no. 1, pp. 112–117, 2019, doi: 10.6633/IJNS.202001.22(1).11.

[50] H. Abroshan, “A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms,” *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 6, pp. 31–37, 2021, doi: 10.14569/IJACSA.2021.0120604.

[51] I. A. Awan, M. Shiraz, M. U. Hashmi, Q. Shaheen, R. Akhtar, and A. Ditta, “Secure framework enhancing AES algorithm in cloud computing,” *Security and Communication Networks*, vol. 2020, pp. 1–16, Sep. 2020, doi: 10.1155/2020/8863345.

[52] M. Kumar, A. Kishor, J. Abawajy, P. Agarwal, A. Singh, and A. Y. Zomaya, “ARPS: An autonomic resource provisioning and scheduling framework for cloud platforms,” *IEEE Transactions on Sustainable Computing*, vol. 7, no. 2, pp. 386–399, Apr. 2022, doi: 10.1109/TSUSC.2021.3110245.

[53] F. Mata, M. Kimwele, and G. Okeyo, “Enhanced secure data storage in cloud computing using hybrid cryptographic techniques (AES and blowfish),” *International Journal of Science and Research (IJSR)*, vol. 6, no. 3, pp. 1702–1708, 2017, doi: 10.21275/ART20171804.

[54] K. Dubey, S. C. Sharma, and M. Kumar, “A secure IoT applications allocation framework for integrated fog-cloud environment,” *Journal of Grid Computing*, vol. 20, no. 1, p. 5, Mar. 2022, doi: 10.1007/s10723-021-09591-x.

[55] M. Kumar, S. C. Sharma, S. Goel, S. K. Mishra, and A. Husain, “Autonomic cloud resource provisioning and scheduling using meta-heuristic algorithm,” *Neural Computing and Applications*, vol. 32, no. 24, pp. 18285–18303, Dec. 2020, doi: 10.1007/s00521-020-04955-y.

[56] L. Khakim, M. Mukhlisin, and A. Suharjono, “Security system design for cloud computing by using the combination of AES256 and MD5 algorithm,” *IOP Conference Series: Materials Science and Engineering*, vol. 732, no. 1, Jan. 2020, doi: 10.1088/1757-899X/732/1/012044.

[57] A. Orobosade, T. Aderonke, A. Boniface, and J. Arome, “Cloud application security using hybrid encryption,” *Communications on Applied Electronics*, vol. 7, no. 33, pp. 25–31, May 2020, doi: 10.5120/cae2020652866.

[58] R. Mathur, V. Pathak, and D. Bandil, *Emerging trends in expert applications and security*, vol. 841. Singapore: Springer Singapore, 2019.

BIOGRAPHIES OF AUTHORS

Yahia Alemami received his B.Sc. degree in Computer Science from Al-Hussein Bin Talal University, Jordan, in 2005 and his M.Sc. degree in Computer Engineering from Anadolu University, Turkey, in 2012. He currently serves as a lecturer at the Department of Computer Science, Al-Hussein Bin Talal University. His research interests include cryptography and information security. He can be contacted at yehea_m@ahu.edu.jo.

Ali M. Al-Ghonmein serves as an assistant professor at the Department of Computer Information Systems (CIS), Al-Hussein Bin Talal University, Jordan. He received his bachelor's degree in computer science from Al-Hussein Bin Talal University (2004) and obtained his master's degree in CIS from the Arab Academy for Banking and Financial Sciences in Jordan, 2008. In 2018, he earned his doctorate degree in management information systems (MIS) from Omdurman Islamic University (OIU), Sudan. His research interests include information retrieval, decision support systems, natural language processing, database systems, cloud computing, big data, and IoT. He can be contacted at ali.m.alghonmein@ahu.edu.jo.

Khaldun G. Al-Moghrabi serves as an assistant professor at the Department of CIS, Al-Hussein Bin Talal University, Jordan. He received his bachelor's degree in CIS from Al-Hussein Bin Talal University (2006) and holds a master's degree in CIS from the Middle East University in Jordan, 2009. In 2018, he earned his doctorate degree in MIS from OIU, Sudan. His research interests include E-learning, decision support systems, database systems, CC, big data, and the IoT. He can be contacted at khaldun.g.moghrabi@ahu.edu.jo.

Mohamad Afendee Mohamed received his Ph.D. in Mathematical Cryptography in 2011 and currently serves as an associate professor at Universiti Sultan Zainal Abidin. His research interests include theoretical and application issues in the domain of data security, and mobile and wireless networking. He can be contacted at mafendi@unisza.edu.my.