Security for Cloud Computing

Shahrin A. Nazeer

Department of Computer Science, Faculty of Science, Northern Border University, Arar, Saudi Arabia

Summary
Although cloud computing is the new emerging technology that presents a good number of benefits to the users, it faces a lot of security issues and challenges. Protection of data is the most important challenge since in cloud computing multiple organizations share the same resources. Data is at high risk since it is open to data loss or data leakage that can severely impact on an organization. Furthermore, it is a big target for malicious individuals and may have disadvantages because it can be accessed through an unsecured internet connection. Hence, strong security measures are to be implemented for data operations and transmissions. A proposed cryptosystem for cloud computing with strong security measures on confidentiality, data integrity, and authentication is presented. For confidentiality, advanced encryption technology is used to provide secure data access for storing and retrieving data from the cloud. For data integrity, a hash function is used to calculate the hash of the file before uploading to cloud servers to ensure that the data is not altered. For authentication, proper key management technique is used to distribute the key to the cloud users such that only authorized persons can access the data. With the security measures in place, the proposed cryptosystem for cloud computing would provide a secure cloud computing environment for data operations and transmissions.

Key words:
Cloud security, Cryptosystem, Cryptographic algorithms, Confidentiality, Data Integrity, Authentication

1. Introduction

Cloud is the data center of hardware and software that offers the computing resources and services; whereas, cloud computing represents both the cloud and the provided services. It is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources including networks, servers, data storage, services, and specialized corporate and user applications that can be rapidly provisioned and released with minimal management effort or service provider interaction over the Internet on a pay-for-use basis [1]. Cloud computing significantly minimize the organization's expenditure towards managing resources and also reduces the burden and complexity of maintaining software or hardware since the organization need not invest on information technology infrastructure, procure hardware or software licenses. It also allows access to information and computer resources from anywhere that a network connection is available. Its benefits also include low up-front costs, rapid return on investment, rapid deployment, customization, flexible use, and solutions that can make use of innovations [3].

Cloud computing provides cloud services such as online file storage, social networking sites, webmail, and online business applications which allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. The cloud services can be customized and flexible to use, and providers can offer advanced services that an organization unable to afford or expertise to develop. The service model for cloud services includes Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service [1]:

- Software as a Service (SaaS): The service provider in this context provides the capability to use one or more applications running on a cloud infrastructure. These applications can be accessed from various thin client interfaces such as web browsers, and the user does not need to maintain, manage or control the underlying cloud infrastructure such as network, operating systems, and storage.
- Platform as a Service (PaaS): The service provider in this context provides useful resources to deploy onto cloud infrastructure, supported applications that are designed or acquired by the user. The user has control over deployed applications and application hosting environment but has no control over infrastructures such as network, storage, servers, and operating systems.
- Infrastructure as a Service (IaaS): The user is provided with the power to control process, manage storage, network, and other fundamental computing resources which are helpful to manage arbitrary software and this can include operating systems and applications. By using this kind of service, a user has control over the operating system, storage, deployed applications, and possibly limited control over selected networking components.

The cloud services can be deployed on one or more deployment models such as public cloud, private cloud, community cloud, and hybrid cloud to use features of cloud computing. Each of these deployment models is explained as follows [2]:

Manuscript received July 7, 2020
Manuscript revised July 20, 2020

- Public cloud: This type of infrastructure is made available to large industrial groups or public. These are maintained and owned by an organization selling cloud services.
- Private cloud: This type of cloud deployment is just kept accessible to the organization that designs it. Private clouds can be managed by a third party or the organization itself. In this scenario, cloud servers may or may not exist in the same place where the organization is located.
- Hybrid cloud: In this deployment model, there can be combinations of two or more clouds used, such as 'private and public', 'public and community'. These constituting clouds remain different but yet bound together by standardized or preparatory technology that enables application and data portability.
- Community cloud: This type of cloud infrastructure is shared by several organizations and supports a specific community with shared concerns. I can be managed by an organization or third party and can be deployed off or in the organizational premise.

Despite its growing influence, concerns regarding cloud computing remain. The protection of data is the most important challenge. In cloud computing multiple organizations share the same resources; therefore, data is at high risk since it is open to data loss or data leakage that can severely impact an organization. Furthermore, the information housed on the cloud is often seen as valuable to individuals with malicious intent. There is a lot of personal information and potentially secure data that people store on their computers, and this information is now being transferred to the cloud. Since the cloud is a big target for malicious individuals and may have disadvantages because it can be accessed through an unsecured internet connection, thus it is critical to implement strong security measures for data operations and transmissions.

Various researches have been conducted which discussed the cloud computing security issues and challenges [4, 5, 6, 7, 8, 9]. Popovi and Hocenski [4] discussed the security issues, requirements, and challenges that are faced by cloud service providers during cloud engineering. Behl [5] explored the security issues related to the cloud environment. He also discussed existing security approaches to secure the cloud infrastructure and applications and their drawbacks. Sabahi [6] discussed the security issues, reliability, and availability of cloud computing. He also proposed a feasible solution for a few security issues. Mohamed *et al* [7] presented the data security model of cloud computing based on the study of cloud architecture. They also implemented software to enhance the work in the data security model for cloud computing. Liu [8] introduced some cloud computing systems and analyzed cloud computing security problems and its strategy according to the cloud computing concepts. Mathisen [9] discussed some of the key security issues that cloud computing is bound to be confronted with, as well as current implementations that provide solutions to these vulnerabilities.

This research paper aims to present a proposed cryptosystem for cloud computing with strong security measures which include confidentiality, data integrity, and authentication. For confidentiality, advanced encryption technology is used to provide secure data access for storing and retrieving data from the cloud. Whereas, for data integrity, a hash function is used to calculate the hash of the file before uploading to cloud servers to ensure that the data is not altered. Meanwhile, for authentication, proper key management technique is used to distribute the key to the cloud users such that only authorized persons can access the data. The remaining parts of the paper are organized as follows: Section 2 presents the cloud computing security issues and challenges. Section 3 describes the cryptographic algorithms. Section 4 explains the proposed cryptosystem for cloud computing with security measures on confidentiality, data integrity, and authentication. The conclusion of the paper is presented in Section 5.

2. Cloud Computing Security Issues

The current trend of cloud computing allows accessing business applications from anywhere just by connecting to the Internet. However, there are security issues and challenges that come along with various benefits of cloud computing. Thus, the security issues and challenges need to be addressed first, before implementing cloud computing in an organization. Cloud computing security issues and challenges include [4, 5, 6, 9, 10]:

- Authentication and Identity Management: By using cloud services, users can easily access their personal information and make it available to various services across the Internet. Thus, authentication and identity management mechanism is required to authenticate users and services based on credentials and characteristics.
- Access Control and Accounting: Access control system is required to manage the cloud and its privilege distribution efficiently. Hence, the cloud delivery models must provide generic access control interfaces for proper interoperability, which demands a policy-neutral access control specification and enforcement framework that can be used to address cross-domain access issues.
- Trust Management and Police Integration: In cloud computing environments, the interactions

between different service domains driven by service requirements can be dynamic, transient, and intensive. Thus, a trust framework should be developed to allow for efficiently capturing a generic set of parameters required for establishing trust and to manage evolving trust and interaction/sharing requirements.

- Secure-Service Management: Many cloud service providers use the Web Services Description Language (WSDL) that partially meets the requirements of cloud computing services description. In clouds, issues such as quality of service, price, and SLAs are critical in-service search and composition. These issues must be addressed to describe services and introduce their features, find the best interoperable options, integrate them without violating the service owner's policies, and ensure that SLAs are satisfied.
- Privacy and Data Protection: By migrating workloads to a shared infrastructure, customers' private information faces an increased risk of potential unauthorized access and exposure. Thus, cloud service providers must assure their customers and provide a high degree of transparency in their operations and privacy assurance. Privacy-protection measures must be embedded in all security solutions.
- Organizational Security Management: The information security area has faced significant problems in establishing appropriate security metrics for consistent and realistic measurements that help risk assessment. Best practices must be reevaluated and standards should be developed to ensure the deployment and adoption of secure clouds which requires a well-structured cyber insurance industry.

Among the security issues and challenges, data security is the major security concern for the cloud computing environment. A virtual cloud environment provides a lot of scopes for the intruders to attack the cloud data and user data. Cloud computing process and transfer data electronically via the public network. Data transmitted through the network is vulnerable to many passive and active attacks such as Distributed Denial of Service (DDoS), and Man-in-the-Middle. For stopping DDoS attack, SYN cookies as well as authenticating the users to access the server of the cloud computing could be used as measures. Meanwhile, for the Man-In-The-Middle attack, Secure Socket Layer (SSL) is used to overcome this kind of attack. However, if SYN cookies and SSL is not configured properly, authentication of the users to the server will not perform as it should protect the users and server of the cloud computing from DDoS and Man-in-the-middle attacks. Furthermore, when multiple organizations share resources there is a risk of data misuse. To avoid risk it is necessary to secure data repositories and also the data that involves storage, transit, or process.

To protect and secure the data, encryption or cryptographic algorithms should be applied. Encryption ensures the privacy, confidentiality, integrity, and authenticity of data since it can convert the data in a form that is unreadable to anyone other than the intended person, and not comprehensive to unauthorized users with unauthorized access before data transmission and data storing [4, 5, 6].

3. Cryptographic algorithms

Cryptographic algorithms or encryptions are techniques used for securing communication and data in the presence of adversaries by constructing and analyzing protocols that prevent third parties or the public from reading private messages with various aspects of information security [19]. They are designed based on the computational hardness assumptions to make the algorithms hard to break in practice by any adversary. There are mainly three (3) different types of cryptographic algorithms which are symmetric key algorithms, asymmetric key algorithms, and hash functions.

3.1 Symmetric Key Algorithm

The symmetric key algorithm is an encryption technique based single or one key for encryption and decryption. It is categorized into two (2) categories which are block cipher and stream cipher. A block cipher encrypts and decrypts a block of the text at a time. Meanwhile, stream cipher encrypts and decrypts the text by taking the one byte of the text at a time. Block cipher takes a message and break it into a fixed size of blocks and converts one block of the message at an instant [20]. Block cipher is used for file transfer over the communication network, whereas, a stream cipher is used for streaming audio or video.

Some of the most popular block ciphers include Data Encryption Standard (DES), Blowfish, RC5, Triple DES (3DES), and Advanced Encryption Standard (AES). DES established in 1977, was the first encryption standard to be approved by NIST, and highly influential in the advancement of present-day cryptographic systems. DES is an algorithm that encrypts a fixed-length string of 64-bit block plaintext using a 56-bit key and changes it into a series of muddled operations into another cipher-text series of bits with the same length [11]. It includes a key generation block and round function which contains many operations like permutation, expansion, substitution, and XORing. There are 16 rounds in DES where a new key is generated for each round. DES algorithm was used with a destruction-editing approach for providing data security with integrity [12].

Blowfish developed by Bruce Schneider is a symmetric encryption algorithm or block cipher that deals with a 64-bit block and has 16 rounds. Its key lengths can differ from 32 to 448 bits in range. Blowfish, accessible easily and developed as an alternate for DES which is in use in a large number of production [12].
RC5 It is a symmetric encryption algorithm or block cipher that deals with a 128-bit block and has 12 rounds. The utilization of the RC5 algorithm for encryption can be connected to the data transmission security [11].
3DES is a block cipher encryption that uses a block size of 64 bits, 168-bit keys, and operates 48 processing round corresponding to DES. In 3DES, three times iteration is produced to improve the encryption and security level of DES [11].
AES is known as 'Rijnadael', is a block cipher proposed by Joan Daemen and Vincent Rijmen. AES is a block cipher with variable key lengths of 128,192 or 256 bit applied on the same size blocks using varying from 10 to 14 rounds depending on the key sizes used. It uses a few substitutions, permutations, and direct changes. The use of the AES encryption algorithm is highly securable with no inclined to any of the cryptanalysis attacks [12].

3.2 Asymmetric Key Algorithm

The asymmetric key algorithm has two keys, one is a private key and another is a public key. The private key is used for decryption whereas the public key is used for encryption [6]. A scenario for using the public and private key; for example, a client sends its public key to the server and requests for some data. The server encrypts the data using the client's public key and sends the encrypted data to the client. The client receives this data and decrypts it using his private key. Thus, nobody else except the client can decrypt the data even if a third party has the public key.
The popular asymmetric key algorithms are Ronald Rivest Adi Shamir and Leonard Adleman (RSA), Digital Signature Algorithm (DSA), Diffie-Hellman, and El-Gamal. RSA is designed in 1977 uses the properties of the generative homomorphism encryption. The key size for RSA key size is 1024 or 2048 bit long, and only has one round [8]. RSA is one of the first asymmetric or public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and distinct from the decryption key which is kept secret. The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is the multiplication of two large prime numbers, and the private key is also derived from the same two prime numbers. Thus, if the large number can be factorized, the private key is compromised. Therefore, the encryption strength lies in the key size where if the key size is increased, the strength of encryption increases exponentially. RSA is generally used to maintain encryption and digital signatures.
RSA provides the best security plan by encrypting the data that is confidential which motivation enormous administration suppliers like Google mail, Yahoo Mail, and so on to use this algorithm to give their clients the protection of secrecy in utilizing their administrations [14]. RSA today is utilized as a part of a few programming items and it can be utilized for digital signatures, key exchange, or encryption of a little block of data. RSA uses a changeable size key and a variable size encryption block. However, encrypting and decrypting data in RSA require extensive computational time [10].
DSA introduced by the NIST (National Institute of Standards and Technology) is a Federal data processing Standard for digital signatures that are used for the authentication of messages. It is used to detect the unauthorized alterations to the data sent by the source to the receiver [8].
Diffie–Hellman is a public-key protocol used to secure exchanging cryptographic keys over a public channel. It was one of the earliest practical examples of public key exchange methods implemented within the field of cryptography. Traditionally, secure encrypted communication between two parties required that they first exchange keys by some secure physical means [15]. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel where the key can then be used to encrypt subsequent communications using a symmetric key cipher. It is used to secure a variety of Internet services. However, the parameters in use for many of its Internet applications at that time are not strong enough to prevent compromise by very well-funded attackers, such as the security services of large governments [21].
El Gamal described by Taher Elgamal in 1985, is an asymmetric cryptographic algorithm that is based on the Diffie–Hellman key exchange. It is defined over any cyclic group (G), as a multiplicative group of integers modulo n. Its security depends upon the difficulty of a certain problem in G{¥displaystyle G} related to computing discrete logarithms.{¥displaystyle G} It is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems [22].

3.3 Hash Function

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but the output is always of fixed length [24]. It maps data of arbitrary size to a bit array of a fixed size output of enciphered text called a hash value. The enciphered text can then be stored, and later used for verification. It is a

one-way function, that is, a function that generates a hash value that is unique and practically infeasible to invert [23]. It is used to produce digests that appear to be random and to maintain the integrity of the message while it is transferred via a medium. The hash function should meet two requirements: first, that an attacker can't generate a message matching a specific hash value; and second, that an attacker can't create two messages that produce the same hash value. Mostly used hash functions are SHA and MD5 hash respectively.

SHA-1 was published in 1993 under the title Secure Hash Standard, FIPS PUB 180, by U.S. government standards agency NIST (National Institute of Standards and Technology). It was withdrawn by the NSA shortly after publication and was superseded by the revised version, published in 1995 in FIPS PUB 180-1 and commonly designated SHA-1 [23]. SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA), first published in 2001, and are built using the Merkle–Damgård structure, from a one-way compression function itself, built using the Davies–Meyer structure from a (classified) specialized block cipher. SHA-2 consists of two hash algorithms: SHA-256 and SHA-512. SHA-224 is a variant of SHA-256 with different starting values and truncated output. SHA-384 and the lesser-known SHA-512/224 and SHA-512/256 are all variants of SHA-512. SHA-512 is more secure than SHA-256 and is commonly faster than SHA-256 on 64-bit machines [23]. SHA-3 (Secure Hash Algorithm 3) released by NIST on August 5, 2015, is a subset of the broader cryptographic primitive family Keccak. The Keccak algorithm is the work of Guido Bertoni, Joan Daemen, Michael Peeters, and Gilles Van Assche. Keccak is based on a sponge construction which can also be used to build other cryptographic primitives such as a stream cipher. SHA-3 provides the same output sizes as SHA-2: 224, 256, 384, and 512 bits [23].

MD5 message-digest algorithm was designed by Ronald Rivest in April 1992. It is a widely used cryptographic hash function or a one-way function that accepts a message of any size as input and produces as output a fixed-length message digest. It produces a 128-bit hash value. It uses a 512-bit block-size with 4 rounds of iteration, and its structure is based on Merkie-Damgard construction [23].

4. Proposed Security Model of Cryptosystem for Cloud Computing

The proposed cryptosystem for cloud computing with security measures on confidentiality, data integrity, and authentication is a hybrid of symmetric key algorithms, asymmetric key algorithms, and hash function. The security measure on confidentiality is provided using the AES algorithm, on data integrity is provided using the MD5 hash function, and on authentication is provided using the RSA algorithm. The proposed cryptosystem is used for uploading and storing data into the cloud, and retrieving and downloading data from the cloud. The process flow for uploading and storing data into the cloud is depicted in Fig. 1. The steps for uploading and storing data into the cloud are as follows:

1. Select the plaintext file to be uploaded by the user
2. Encrypt the plaintext file into a cipher-text file using the AES algorithm for confidentiality.
3. Apply MD5 hash function on the cipher-text file to generate the message digest/hash for integrity
4. Encrypt message digest to create a digital signature using RSA algorithm for authentication
5. Transfer the data to the cloud via the public network
6. Encrypt the arrived data using AES algorithm in the cloud for confidentiality
7. Store the encrypted data into the cloud storage server

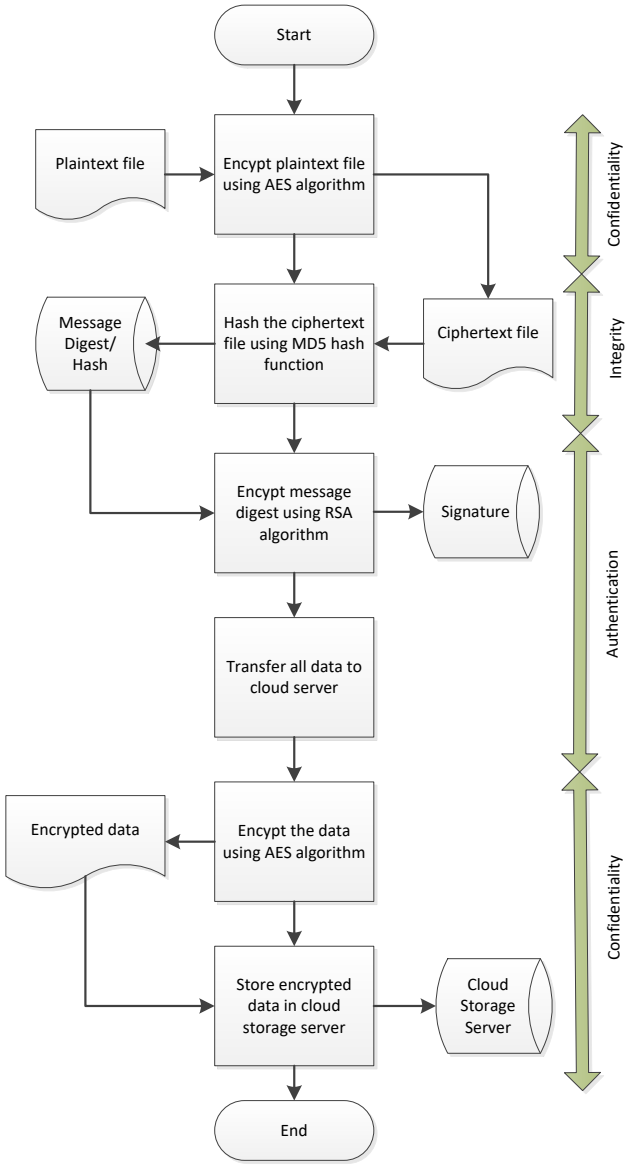

Fig. 1 Process flow for uploading and storing data into the cloud

The process flow for retrieving and downloading the data from the cloud is shown in Fig. 2. The steps for retrieving and downloading data from the cloud are as follows:

1. Retrieve the encrypted data from the cloud storage server
2. Decrypt the encrypted data in the cloud using the AES algorithm
3. Transfer the data from the cloud to the client via the public network
4. Authenticate digital signature using RSA algorithm
5. Apply MD5 hash function on the downloaded data to get the hash value
6. Compare the hash value with the stored hash value to determine its integrity. If the hash values matched, the downloaded data is not altered, else it has been changed.
7. Decrypt the data using the AES algorithm for plaintext files.

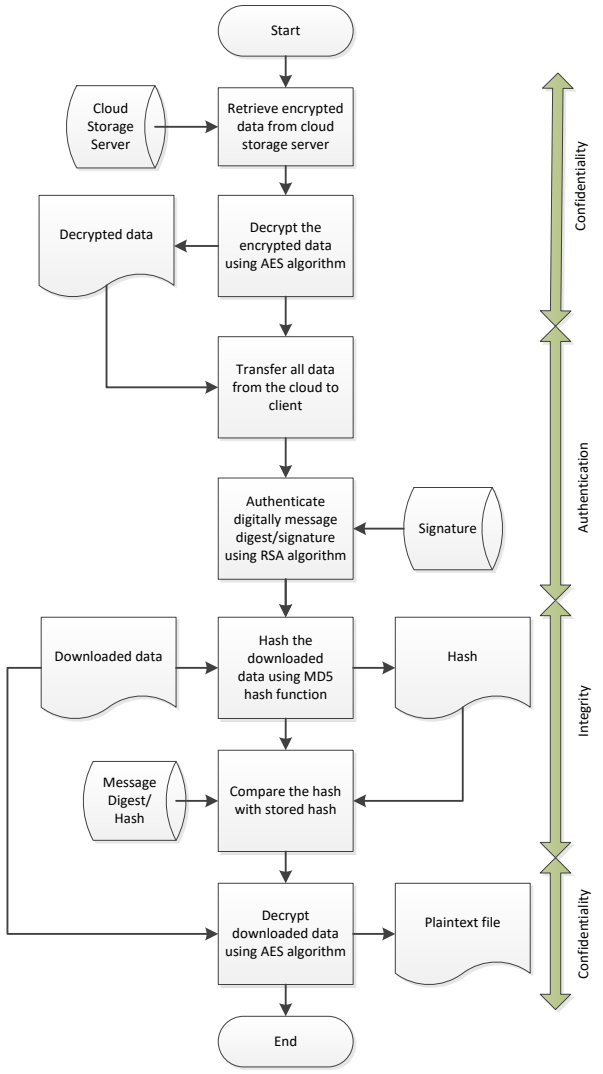

Fig. 2 Process flow for retrieving and downloading data from the cloud

4.1 Confidentiality

Confidentiality is a set of rules or a promise usually executed through confidentiality agreements that limit access or places restrictions on certain types of information. Confidentiality is one of the most important security measures for data security to protect and to ensure the data is secure via a public network and also in the cloud. It protects the data from being modified or read when stored in the cloud. For the confidentiality of the data, the proposed cryptosystem applies the AES

algorithm. The confidentiality measure is conducted twice, one before sending or transmitting the data over the public network to the cloud and another after arriving at the cloud that is before storing the data into the cloud storage server.
The operation of the AES algorithm for encryption and decryption is illustrated in Fig. 3. The AES algorithm used is based on block length of 128-bits and key lengths of 128-bit with 10 rounds of processing. For a 128-bit key, the key is arranged in the form of an array of 4 × 4 bytes or four words. The four words of the original 128-bit key are expanded into a key schedule consisting of 44 words. For the input block, the first word from the key fills the first column of the array, and so forth. Each round of processing includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key. The order in which these four steps are executed is different for encryption and decryption.
The steps for encryption process are as follows:

1. The plaintext state array is XORed with the first four words of the key schedule.
2. Perform the round sub-processes until it reaches the 10th round. Each round consists of the following except for the last round which does not involve the "Mix columns" step
    a. Substitute bytes,
    b. Shift rows,
    c. Mix columns,
    d. Add round key.
3. XORing the output of the previous three steps with four words from the key schedule.
4. The cipher-text of the plaintext is generated

The steps for the decryption process are as follows:

1. The cipher-text state array is XORed with the last four words of the key schedule.
2. Perform the round sub-processes until it reaches the 10th round Each round sub-processes consists of the following four steps except for last round which does not involve the "Inverse mix columns" step.
    a. Inverse shift rows,
    b. Inverse substitute bytes,
    c. Add round key, and
    d. Inverse mix columns.
3. XORing the output of the previous two steps with four words from the key schedule.
4. The plaintext of the cipher-text is generated.

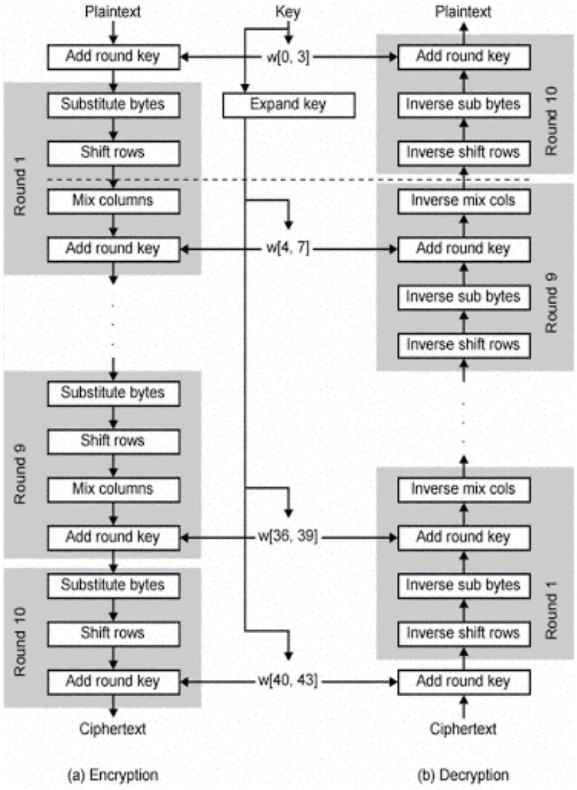

Fig. 3 AES encryption and decryption operation. Adopted from [18]

Each of the rounds has four (4) sub-processes which are:

(i) Substitute Bytes: The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.
(ii) Shift Rows: Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of the row. The shift is carried out as follows:
    a. The first row is not shifted.
    b. The second row is shifted one (byte) position to the left.
    c. The third row is shifted two positions to the left.
    d. The fourth row is shifted three positions to the left.
    e. The result is a new matrix consisting of the same 16 bytes but shifted for each other.
(iii) Mix Columns: Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.
(iv) Add Round Key: The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128

bits are interpreted as 16 bytes and we begin another similar round.

4.2 Integrity

Data integrity is used to ensure data is recorded exactly as intended and upon later retrieval, ensure the data is the same as it was when it was originally recorded. It aims to prevent unintentional changes to information. The proposed cryptosystem security measure on data integrity is based on the MD5 hash function. The MD5 message-digest hashing algorithm processes data in 512-bit blocks, broken down into 16 words composed of 32 bits each. The output from MD5 is a 128-bit message digest value.

Computation of the MD5 digest value is performed in separate stages that process each 512-bit block of data along with the value computed in the preceding stage. The first stage begins with the message digest values initialized using consecutive hexadecimal numerical values. Each stage includes four message-digest passes that manipulate values in the current data block and values processed from the previous block. The final value computed from the last block becomes the MD5 digest for that block. MD5 operation for a single 512-bit block is depicted in Fig. 4.

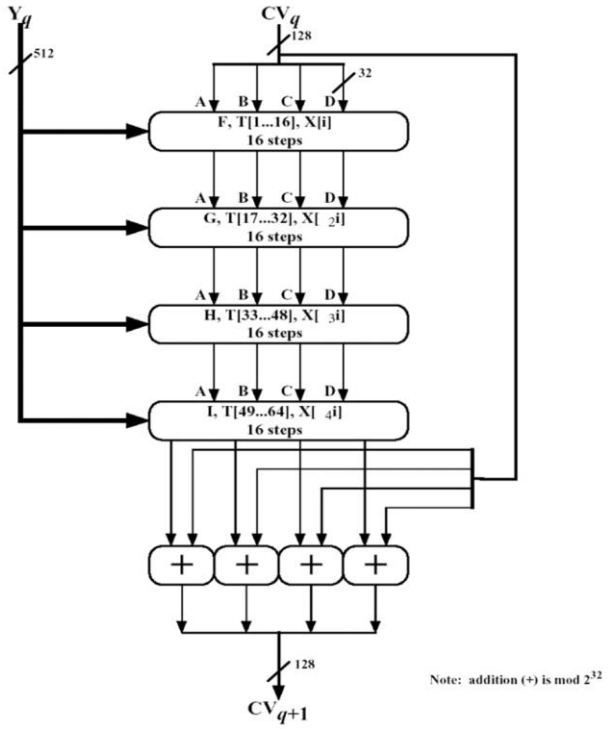

Fig. 4 MD5 Operation for a single 512-bit block. Adopted from [18]

The steps for MD5 Operation are as follows:

1. Pad message so that the length mod 512=448 or equivalently length ≡ 448 (mod 512)
2. Append a 64-bit length value to message
3. Initialize 4-word (128-bit) MD buffer (A,B,C,D) to given values for A, B, C and D, and save the values in the least significant byte of a word in the low-address position.
4. Process message in 16-word (512-bit) blocks using 4 rounds of 16-bit operations on message block and buffer, and add output to buffer input to form new buffer value.
5. After all L 512-bit blocks have been processed the output from Lth stage is the 128-bit message digest(hash code).

4.3 Authentication

Authentication is the process of verifying the identity of an entity. In cloud computing, it ensures that the proper person is getting access to the provided data from the cloud technology provider. When authentication is ensured in the cloud computing, it means that the user's identity is proved to the cloud service provider when accessing the stored information in the cloud. Authorization in cloud computing is important for the users when they login to some cloud service because it enables prove of their identities. So, authorization is usually employed after the authentication.

RSA algorithm is used for authentication. RSA algorithm is used to encrypt the data to provide security so that only the concerned user can access it. By securing the data unauthorized access is blocked. RSA digital signature scheme applies the user's private key to the data to generate a signature. The signature can then be verified by applying the corresponding public key to the data and the signature through the verification process, providing either a valid or invalid result. These two operations' signature and verification comprise the RSA digital signature scheme. User data is encrypted first and then it is stored in the cloud. When required, the user places a request for the data from the cloud provider. The Cloud provider authenticates the user and delivers the data.

In the cloud environment, the public key is known to all, whereas the private key is known only to the user who creates the data. The data is encrypted using the public key and decrypted using the private key. The process flow for data transmission using the RSA algorithm is depicted in Fig. 5. The RSA operation involves the key generation, encryption, and decryption. The steps for the RSA operation are as follows:

(i) Key Generation: The key generation generates the public key and private key. The steps to generate the public key and private key are as follows:
- Use a Random Number Generator to get two prime numbers, P and Q.
- From these numbers, calculate the modulus, n = P X Q.

- Next, generate a public key exponent (e) such that gcd(e, φ (n)) = 1
- The public key pair (n, e) is made of n and e.
- Next, calculate Φ(n) such that Φ(n) = (P-1)(Q-1).
- Determine private key exponent (d), such that: e x d ≡ 1 mod φ (n)
- The private key pair (n, d) is made of n and d.

(ii) Data Encryption

- Get the plaintext, p.
- Convert the plaintext to a string of numbers, s
- Encrypt the string of numbers using public key pair (n, e) to get the cipher-text, c = s.e mod n

(iii) Data Decryption

- Get the cipher-text, c
- Decrypting cipher-text using the private key pair (n, d) to get the string of numbers, s = c.d mod n
- Convert the string of numbers to letters to get the plaintext.

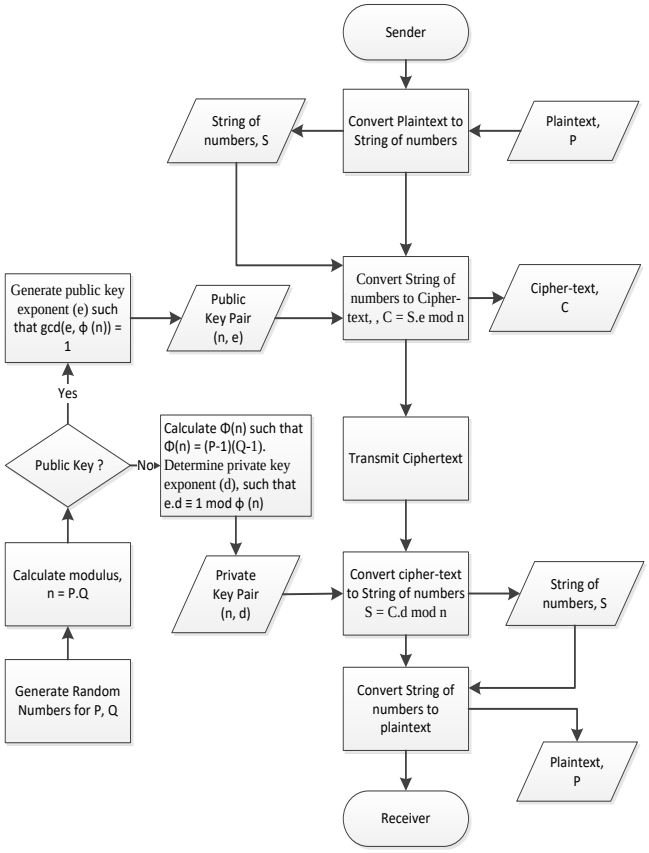

Fig. 5 Process flow for data transmission using the RSA algorithm

5. Conclusion

The paper has discussed cloud computing security which is the major issue and challenges for cloud computing. Since in cloud computing, multiple organizations share the same resources, data is at high risk and is open to data loss or data leakage that can severely impact on an organization. Besides that, cloud computing is a big target for malicious individuals and may have disadvantages because it can be accessed through an unsecured internet connection. Cryptographic algorithms or encryption schemes are identified to overcome security issues. For that reason, the paper has presented a proposed cryptosystem for cloud computing with strong security measures on confidentiality, data integrity, and authentication. For confidentiality, the AES encryption algorithm is used to provide secure data access for storing and retrieving data from the cloud. For data integrity, the MD5 hash function is used to calculate the hash of the file before uploading to cloud servers to ensure that the data is not altered. For authentication, RSA key management technique is used to distribute the key to the cloud users such that only authorized persons can access the data. With the security measures in place, the proposed cryptosystem for cloud computing would provide a secure cloud computing environment for data operations and data transmissions.

Acknowledgment

The author would like to acknowledge the Northern Border University (NBU) for the financial support under the Deanship of Scientific Research (Research Project No.:7696-SCI-2018-3-9-F)

References

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “A break in the clouds: towards a cloud definition”, ACM SIGCOMM Computer Communication Review, pp.50-55, 2008.

[2] M.B. Mollah, K.R. Islam, and S.S. Islam, “Next generation of computing through cloud computing technology”, 25th IEEE Canadian. Conference on Electrical Computer Engineering (CCECE), pp.1-6, May 2012.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable and fine-grained data access control in cloud computing”, INFOCOM, Proceedings IEEE, pp.1-9, 2010.

[4] K. Popovic and Z. Hocenski, “Cloud computing security issues and challenges”, MIPRO, Proceedings of the 33rd International Convention, pp.344-349, 2010.

[5] A. Bhel, “Emerging Security Challenges in Cloud Computing, Information and Communication Technologies”, World Congress on, Mumbai, pp.217-222, 2011.

[6] F. Sabahi, “Cloud Computing Security Threats and Responses”, IEEE 3rd International Conference on Communication Software and Networks (ICCSN), pp.245-249, May 2011.

[7] E.M. Mohamed, H.S. Abdelkader, S.E. Etriby, “Enhanced Data Security Model for Cloud Computing”, 8th International Conference on Informatics and Systems (INFOS), Cairo, pp.12-17, May 2012.
[8] W. Liu, “Research on Cloud Computing Security Problem and Strategy”, 2nd International Conference on Consumer Electronics. Communications and Networks (CECNet), pp.1216-1219, April 2012.
[9] E. Mathisen, “Security Challenges and Solutions in Cloud Computing”, International Conference on Digital Ecosystems and Technologies (IEEE DEST), pp.208-212, 2011.
[10] P.K. Tiwari and B. Mishra, "Cloud Computing Security Issues, Challenges and Solution", IJETAE, Volume 2, Issue 8, August 2012.
[11] N. Jain and G. Kaur, ‘Implementing DES Algorithm in Cloud for Data Security’, VSRD-IJCSIT, Vol. 2 (4), pp.316-321 2012.
[12] K. Nikhitha K and K.S. Navin, “Survey On Various Encryption Techniques For Enhancing Data Security” In Cloud. International Journal of Advanced Research Trends in Engineering and Technology pp.194– 197, 2015.
[13] R. Kaur and S. Kinger, ”Analysis of Security Algorithms in Cloud Computing”. International Journal of Application or Innovation in Engineering & Management 3: pp.171–176, 2014.
[14] P. Kalpana and S. Singaraju, ‘Data Security in Cloud Computing using RSA Algorithm’, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.
[15] W. Diffie and M.E. Hellman, ‘New directions in cryptography’, IEEE, ISSN - 0018-9448, Vol: 22, Issue: 6. 1976.
[16] K. Nasrin and Z. Mohd, “A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services”. IEEE Conference on Systems, Process, and Control pp.58-62. 2014.
[17] S. Sindhu, “A survey of security algorithms in cloud computing”. International Journal of Advanced Research in Computer Engineering & Technology, 2015.
[18] W. Stalling, “Cryptography and Network Security: Principle and Practice”, Pearson Education, 2003.
[19] Wikipedia,“Cryptography”.https://en.wikipedia.org/wiki/Cryptography
[20] TechDifferences, “Difference Between Block Cipher and Stream Cipher”.https://techdifferences.com/difference-between-block-cipher-and-stream-cipher.htm
[21] Wikipedia, “Diffie–Hellman key exchange”. https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellmankey_exchange
[22] Wikipedia, “ElGamal encryption” https://en.wikipedia.org/wiki/ElGamal_encryption
[23] ikipedia. “Cryptographic hash function” https://en.wikipedia.org/wiki/Cryptographic_hash_function
[24] Tutorialpoints. “Cryptography Hash functions” https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm

Shahrin A. Nazeer received his B.Sc degree from Clarkson University, U.S.A in 1990, M.Sc. degree from UMIST, Manchester, U.K. in 1997, and a doctorate from Universiti Teknologi Malaysia, Skudai, Malaysia in 2008, respectively. He is currently an associate professor at Northern Border University, Arar, Saudi Arabia. His research interest includes intelligent systems, information security, artificial intelligence, image processing, software engineering, and web development.