Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.199

IJCSMC, Vol. 9, Issue. 3, March 2020, pg.211 – 220

Review of Cryptography in Cloud Computing

Samar Zaineldeen[1]; Abdelrahim Ate[2]

[1]School of Management, Jiangsu University, China

[2]Mechanical and Electrical Engineering Department, Dezhou University, Dezhou, Shandong, China

[2]Control Department, Faculty of Engineering, Alneelain University, Khartoum, Sudan

[1] smrzainaldeen@gmail.com; [2] wadalroob@gmail.com

Abstract— Cloud computing offerings a distinctive way to share distributed resources, cloud computing is a type of Internet-based sharing of distributed assets through web. It is a model that empowerment prevalent, on-demand access to a shared mutual pool of configurable processing property and computing resources. Consequently, security becomes a critical issue in cloud computing. Securing information is the key issue in the field of network security. Cryptography is stand out among the best method to improve data security. This paper discusses the role of cryptography in cloud computing to enhance the information and data security.

Keywords— Cloud computing, Security, Cryptography

I. INTRODUCTION

Cloud computing is a concept of evolving huge number of computers linked, virtualized and organized in terms of manageable workloads. It's a service and an application that runs on a broadcasted network and utilizing virtual assets accessed by networking standards and common IP. As indicated by National Institute of Standard and Technology, it's a paradigm for empowering on-demand and convenient network access to a shared pool of configurable computing resources that can be swiftly released and provided with slightest service provider alliance and management effort [1]. As seen in figure 1. Cloud computing schematic definition can be simple.

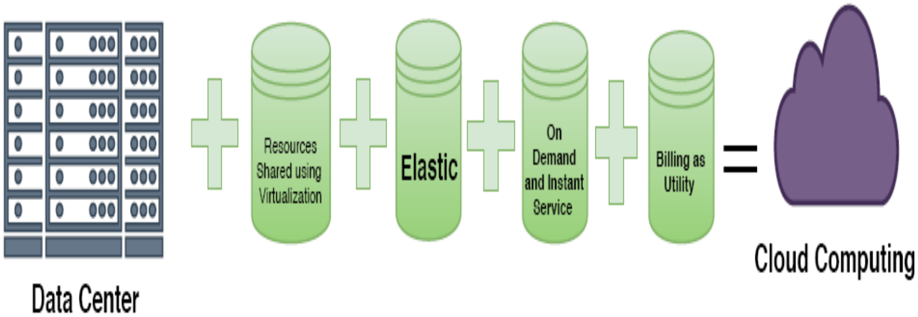
Data Center
Resources Shared using Virtualization
Elastic
On Demand and Instant Service
Billing as Utility
Cloud Computing

figure 1. cloud computing Schematic definition [2]

Cloud computing distinguish by divers scientist [3],[4] by resource pooling, broad network access, immediate flexibility, on-demand self-service, and measured service are considered as fundamental characteristics of cloud computing, but another academics [5],[6] consider that multi-tenancy is a key characteristic of cloud computing.
It's deployment as one of the 4 models: the hybrid, private and public cloud.
Private clouds are Clouds within society like a company, which provides cloud computing services to its consumers only.[7]. The Internet also is known by the name of external cloud is Public Clouds [7]. A mixture of several public and private clouds are hybrid clouds[7].The cloud services are delivered in various forms [8]:- Infrastructure-as-a-Service , Platform-as-a-Service, and Software-as-a-Service
Cloud storage products are launched by some master vendors and IT companies. Amazon has launched the EC2. IBM Corporation suggested "The Enterprise Intelligent Cloud Storage" strategic plan in 2009. There's CloudEx that is cloud storage service computing platform, etc based in China. Microsoft Corp.'s Amazon Web Service', Office 365 MSFT Azure and Google Drive are some examples of cloud computing products. companies like Yahoo, Salesforce, and Facebook are also transmitting a number of their services to cloud for their customers.

Cloud computing serves storage resources, computation, data access, and software without exhausting users to perceive the location and alternative specifics of the computing framework. Users reach cloud-based applications via a network program or portable application during the business software and data are stored on servers at a remote site [9].
Cloud computing huge opportunities for businesses, but with these opening, there are many security disputes and challenges that should be addressed and viewed.
Security is the number one challenge cloud computing as indicated by IDC. Experience proof that attacks may never be fully blocked or detected minutely and on time.
There sits plenty security challenges for distributed computing as it controls a variety of technologies like databases, storage managing, resource distribution, and virtualization.

II. CLOUD SECURITY ISSUES

The various security concerns relating to cloud computing are given below:-
3 vital properties of data are Confidentiality, Integrity, and Availability (CIA). 3 other properties for people who use the data are authorization, non-repudiation, and authentication, the confidentiality of the data has appertained to data privacy, where unauthorized parties are not able to see or get data for any reason. The guarantee information is absolute and valid is data integrity. It includes controlling the data and network devices from illegal access and preserves them accurately. The assurance of data being available to the customer whenever they request it is the availability of data, Data is stored in different locations in cloud so its availability is a big issue. In the public model of cloud deployment model three properties of data security are testified exceedingly. The person accessing their own particular data is authentication. The process of finding out if a particular person has the permit to carry out an activity on data or not is Authorization. The declaration that an authentic user cannot retract after doing a job is nonrepudiation

Cloud computing is adopted by a lot of organizations, hence the security dilemmas are rising as a result of the aggregations of digital resources [10]. It is unsurprising that cloud security has seen substantial research attentiveness recently [11][12],[13], [14],[15] . The necessity to secure the cloud contents becomes the most important concern to the users since the data is vulnerable to intruder's attack [16], [17], [18].

The merits of cloud computing over traditional computing include device independence, agility, scalability, lower entry cost, and location independence, [53].

Cloud computing provides countless shared configurable resources to the user payable on demand according to the size of the resources consumed by the user [19], [20].

In cloud computing, Classical security procedures won't be efficient because the operating environments (virtualization, multi-tenant, heterogeneity, etc.) are absolutely dissimilar to common computing. There is a clear difference between outsiders and insiders In traditional computing, and the security administrator takes all accountability for the security methods, defense of assets and data. Cloud computing is literally prone to malware side attacks from outsiders and inside attackers as a result of multi-tenancy.

Several researchers have provided several solutions and numerous are still working. In this paper, the vital goal is to seek an integrated framework/solution for accomplishing the cloud environment data security utilizing the cryptographic technique.

In the presence of the third party, one of the major methods for confident communication is cryptography.

Cryptography is the science of keeping message or information secure by altering the raw data into a configuration that is not easily readable [21]. A particularly promising method to accomplish privacy and security in cloud computing is through cryptography [22][23].

The cryptographic system identified in [24] as " cryptographic algorithms with the key management procedure that strengthening the employ of the algorithms in a number of application context." This explanation gives the entire mechanism that layout the core level of security composed of data encryption algorithms and network protocols. Data must constantly be encrypted when stored and transferred [25] If this is implemented properly, even if another occupant can access the data, all that will appear as gibberish.

In[26], distinctive encryption types strategies are defined. One of the most capable encryption algorithms is utilized by Amazon S3, 256-bit AES [27].

. To maintain authentication, non-repudiation from unauthenticated users, confidentiality and data integrity are the main requirements of cryptography

The cryptography notion is based on two principle terms encryption and decryption. Encryption's procedure of transformation of data known as plain text for an unreadable configuration known a ciphertext, ciphertext can't be comprehended by unapproved individuals. Making the interpretation of encoded information or data again into its earlier form so it can be read by the people who are authorized or allowed to use that data is Decryption. There are different encryption algorithms widely employed for info security.

III. TOWARD HOMOMORPHIC ENCRYPTION

Three forms of cryptography algorithms (i) Hashing. (ii) Symmetric algorithms (iii) Asymmetric algorithms

A. Symmetric Key Cryptography

"Secret Key Encryption Algorithm" (Symmetric algorithm), the only private key is used for encoding and decoding [28]. These algorithms are separated for 2 types: Block and Stream cipher Input are taken as a block of fixed size plaintext is taken of fixed size in block cipher consequently to the type of asymmetric encryption algorithm, the fixed-size key is implemented on plain text block and then same size the output block as plaintext is acquired. At a time one bit is encoded in case of Stream Cipher

The usefulness of utilizing Symmetric-key encryption is that it actually works with high speed in encryption and does not excessively use computation power

AES, DES, BLOWFISH, RC5, and 3DES some of the regular symmetric key algorithms.

Brief definitions of the most widely recognized Symmetric algorithm are given as follows:

1) DES

Data Encryption Standard is a symmetric block encryption standard. It was suggested in the 1970s by IBM organization, The identical key is utilized for encoding and decoding, with marginal alterations. DES receptive input of 56-bit key (8 parity bits) and 64-bit plaintext and reproduce 64-bit block output. Since the introduction of DES, there has been a number of attacks on systems utilizing it, exposure its vulnerabilities, making it an unconfident block cipher [54] [55]. To decisively this, 3DES encryption technique was suggested to overcome this shortcoming of the DES in [56] this technique stretched the length of key from the original 56 to 112 bits, but, the software application of the algorithm is unproductive. With encryption techniques development, Data Encryption Standard has progressively been substituted by the AES, which is exceedingly safe, accomplished and trustworthy.

2) Advanced Encryption Standard (AES)

In cryptography, Advanced Encryption Standard is a symmetric block encryption standard recommended in 2001 by NIST, utilize for assurance the information. All ciphers have a fixed 128-bit block size [29], It has different key lengths of 256, 128, or 192 bits; default 256 [30 Its key length varies between 256, 192, or 128 bits. It encodes 128 bits data blocks in 10, 12 and 14 rounds according to key length., AES encryption is fast and elastic.

DES algorithm is gradually superseded by AES and has emerged as a modern generation data encoding standard [12]. It’s an iterative block cipher algorithm, in which key and packet length are the variables.256 192 and 128 bits are the optional key length which is equivalent to 14, 12 and 10 rounds respectively. (DES) has been the standard for long-time substitute by AES since (NIST) selected the Rijndael algorithm to be approved as Advanced Encryption Standard (AES).

B. Asymmetric Key Cryptography

Asymmetric – double unique keys are utilized. The public key is accessible to anybody on the network. The public key gets utilized to encode data. The only private key can decode that data. The private key is reserved secret and it needed in keeping information secure.

The pros of utilizing asymmetric key encryption are that it gives better scalability and distribution of key relative to symmetric systems. A few standard Asymmetric Key Algorithms are El Gamal, ECC, RSA, DSA, Diffie-Hellman. The asymmetric encoding algorithm needs more computational processing power if we evaluate it compare to symmetric encoding algorithm. Symmetric approximately 1000 times faster compare to Asymmetric techniques [32].

Brief definitions of the most widely recognized Asymmetric algorithm are given as follows:

1) RSA

It's one of the oldest and early asymmetric cryptosystems. It's still the most employed and used cryptosystem. Len Adleman, Ron Rivest, and Adi Shamir made this system and named it as RSA cryptosystem. It encompasses 2 keys, a private and public key. Messages scrambled with public key can get decoded private key. The server actualizes authentication of public key in this verification procedure by inscribing a distinct message with its private key, that’s known as digital signature. Then signature is returned back to the client. After that using the server’s public key it verifies

2) ElGamal

Elgamal is an asymmetric algorithm utilized for exchanging digital signatures as well as for key exchange. El Gamal is based on the applicability of discrete logarithms. It is based on the logarithmic qualities or estimations of these numbers. [33]. ElGamal is an expanded and updated version of Diffie-Hellman.

C. Hashing Key Cryptography

Hash functions are termed one-way encryption other than the message digests. To ensure it inconceivable for the details or length of the plaintext to recapture hash value’s computed on the basis of plaintext rather than fixed length.To encode passwords a lot of OS frequently employ hash function. In addition it gives a mechanism to confirm software integrity checking *[59]* it used to defend the file from not been adjusted by virus or hacker. To give a digital fingerprint of a file's contents hash methods are frequently adopt[60].

SHA-1, MD5, SHA-2, MD5, MD4 and SHA-3 and some of the regular Hash key algorithms.

Brief definitions of the most widely recognized hash key algorithm are given as follows:

1) MD5

With a 128-bit hash value, MD5 is widely utilized hash function and procedures message of a variable-length into a fixed-length output of 128 bits. Beginning the info message is separated into pieces of 512bit blocks and after that message is cushioned so its whole length's distinguishable by 512 bit. The public key is utilized by the sender for data encoding, and the private key used by receiver decoding data.

MD5 is performing preferable in terms of protection and speed [61] The MD5 hash function was extremely popular since 1992 and is still in use. It has been utilized for a lot of applications, for illustration, it is available as a native tool in approximately all versions of Linux and Unix [62].

2) SH-1

SHA-1 is described as protected because of its impossible computation to figure out a message which conforms to a specified MD or to discover 2 distinct messages which create a similar MD.

The signature will fail to verify if any modifications to a message in transfer because of changing lead to a diverse message [63] SHA-1 \ 160-bit hashes. The structure of the functions is similar to MD5, but several changes and modifications have been introduced to increase their security [62].

SHA-1 was initially available as FIPS PUB and produces a 160-bit hash value [63] SHA-1 was deprecated by NIST as of the end of 2013 although it is still extensively used.

IV. HOMOMORPHIC ENCRYPTION(HE)

It's [34],[35] a method of encryption technique that executes computation on ciphertext and result thus generated matches with the result of an operation that is executed on the plaintext when decrypted. Generally, the homomorphic technique is to preserve the integrity of data over the cloud.

The plaintext is deployment with an algebraic operation like multiplication and addition in homomorphic encryption. These operations act dependably which implies the plaintext is reformed according to operations in the ciphertext. This category of encryption9 has been in existence since the emerging of public-key cryptography [36]. Homomorphic encryption is asymmetric key algorithm utilizes two diverse keys for encoding and decoding as public and private key [37].

There are certain known encoding algorithms that come under the homomorphic encryption paradigm. Based upon operations that can implement on raw info or data, we can categorize The homomorphic encryption to [37] :

- Additive Homomorphic Encryption- Raw data addition
- Multiplicative Homomorphic Encryption- Raw data product.

Relying upon the operations executed on data we can differentiate (HE) systems to three classifications:

A. Partially Homomorphic Encryption

Permits carry out operations on scrambled data, multiplication either addition, however not both[64].

RSA is a multiplicative homomorphism encoded system, which is a public key cryptosystem [38]. Goldwasser and Micali in 1982 suggested (GM) encryption system, it's an add-on homomorphism encoded, however single bit can be encoded [65]. ElGamal (multiplicative homomorphic encryption system). Proposed in 1984 by T.Elgamal, it is a public-key cryptosystem[66].

B. Somewhat Homomorphic Encryption

Many operations are permitted to run, except for a restricted number of multiplication and addition operations [64].

Boneh, Goh, and Nissim innovated In 2005 an encoded system (BGN), can execute an infinite number of additions, excluding with single one multiplication [67].

C. Fully Homomorphic Encryption (FHE)

schemes can execute both operations, i.e. addition and multiplication to the data. In [39] a scheme to running algebraic query processing over encoded data is proposed, to make sure the data all the way through phases of the sharing process base on fully homomorphic encryption.

FHE system can execute an unrestrained number of equally multiplications and additions [64].

A fully homomorphic encryption scheme was implemented in 2009 by Craig Gentry that could perform many multiplication and additions using ideal lattices with the bootstrap technique [68]. EHES method was proposed by

Gorti VNKV Subba Rao in 2013 for homomorphic decryption and encryption with the security system of IND-CCA. Homomorphic encryption permits to execute multiplication, mixed and addition operations 69].

V. LITERATURE REVIEW

cloud computing comes in most emerging fields of research where loads of work is done in this field, as cloud security becomes a bigger and bigger concern, and all of these works include using a cryptographic method. Current methods have some cons to tackle these issues.

We must find a way to secure private data stored in cloud, taking into consideration that some applications must be developed and execute hybrid encryption mechanism utilizing tough cryptographic algorithms.

Researchers believe that system security would strengthen if we make a combination n of several cryptographic algorithms. The classic encryption algorithms are not sufficient for present info security on internet, so a lot of researchers propose hybrid Cryptography Algorithm [40]. It is a design for transmission data with blends of at least two cryptographic algorithms to provide security.

In [41] presents anxious about the security element in the environment of the cloud. It recommended technique to improve the security of cloud database. This technique utilizing multiple encryption algorithms such as 3DES, arbitrary number generator, RSA, and are clubbed together to give security yet this scheme makes overhead on the performance.

In [42] is focused on how can expansions the security of data transmission during transfer extremely sensitive data such as Military information and Banking transactions, and many more conclude that hybrid algorithm can fulfill these criteria to some extent.

In [43] the drawback of Security in RSA was excluded by a hybrid approach for providing data security in the cloud. Used Feistel Cipher Algorithm and RSA in two phases. the probability of man-in-the-middle attack was reduced since two algorithms were used in two phases.

In [44] proposed a mechanism e while data is transmitting encryption is utilized to provide security which applied the concept of RSA algorithm, Hash function, only in encoded form is transferred over the channel, which decreases the issue of data revelation.

The two basic features that differentiate and recognize one encryption algorithm from another are its ability to secure the ensure data against assaults and its rapidity and efficiency in doing so.

Equally Symmetric and Asymmetric Key algorithms are very proficient in securing the transmitted data over any communication medium. In [45] they considered the conventional algorithms, along with the proposed algorithms in light of their cons and pros recognized with Symmetric and Asymmetric Key Cryptography. They have additionally analyzed the significance of both these cryptographic techniques. Between Blowfish, AES, RSA and DES, algorithms assessments have been made to discover best security algorithm, that will be utilized in cloud computing to make cloud data secure and not prone to hackers[14]

In [46] demonstrate evaluation Symmetric and Asymmetric with a concentrate on Symmetric Algorithms for security regard as which one has to be utilized for Cloud-based applications and services that need link data and encryption. A concise relative comparison plus outline of Cryptographic algorithms, which focuses on Symmetric method which ought to use for Cloud-based applications and services that need link data and encryption is shown in the paper.

In [47] deliberated the principal vital point of AES concerning to DES, as well as its constraints. deduce that AES can be relatively better in implement at low-level or high-level languages.

In [28]gave a fair comparison and measurement of three well-known symmetric key cryptography algorithms: Blowfish, AES, DES. The evaluation of performance for algorithms was under diverse settings took into consideration the manners of the algorithm when a variety of data loads are executed.

In [48] Conducted a study to compare the performance in term of dissimilar hardware's having dissimilar processing speed where different size of the file is processed to measure the Encoding and Decoding processing time of each algorithm for diverse Hardware. Indicated that the AES (Rijndael) algorithm has taken less execution time and the best throughput over other hardware processors.

TABLE I
comparison study for different algorithms, tools, and results

NUM	COMPARISON STUDY	TOOLS	RESULTS
49	Obtainable a comparison of 3DES, DES, AES, RC6, RC2, and Blowfish .	Employ differently settings for all algorithms as -dissimilar data blocks sizes -diverse battery power utilization, data types -various sizes of keys and decoding /encoding speed.	They concluded that - if there's event of changing the size of packet Blowfish showed preferred performance over other algorithms followed by RC6. - Advanced Encryption Standard had preferable performance than RC2, 3DES, and DES. - if there should arise an occurrence of changing the size of key – it was concluded that the lengthy size of key prompts a change in time and battery consumption.
50	The assessment carried out for encryption algorithms (DES, AES,RC4, RC6, MARS, 3DES, Blow-Fish, and Two-Fish) as indicated by randomness testing.	-NIST statistical testing. - Pseudo-Random Number Generator PRNG. - Java Cryptography Extensions (JCE).	They conclude that - Blowfish is better when an emphasis on time taking for encoding. AES encryption method is a suitable algorithm for Amazon DES, EC2 - The RC6 encoding algorithm is the appropriate algorithm for conventional PC environment, however, Blow-Fish is reasonable when we mind the time of the encryption method.
28	The comparative is done base on the key size, block size and speed.	Emulators program utilized Java programming.	The submitted simulation outcomes showed : -Blowfish has an enhanced performance compared to known encoding algorithms used. -AES revealed poor performance consequences since it requires additional processing power compared to other algorithms.
51	Comparison of both asymmetric and symmetric encryption algorithms computation has many security issues	Compared with different cryptographic algorithms on various factors.	-Advanced Encryption Standard requires less memory. offers higher security, flexibility performance, the algorithm is best compared to other symmetric algorithms and -RSA algorithm is best in contrast to other asymmetric algorithms. It is efficient and faster
11	Evaluations have been made between, DES, Blowfish, RSA, AES HOMOMORPHIC Encryption, IDEA algorithms goal to find the best security algorithm.	Compared diverse encoding algorithms.	-AES and Homomorphic secure for both user and provider, RSA and IDEA secure for the user only. -AES used for encryption of huge amount of data, best authenticity provider, Low RAM needed and Faster than others

52	Comparison among four encoding algorithms: DES, AES, BLOWFISH, and 3DES. To evaluate the speed of encoding and decoding for each algorithm. According to the analysis of performance of these algorithms in different software and hardware platform by running a variety of setting to process size diversification of data blocks.	-diverse Software and Hardware platforms are taken. - C# and Java.	It's deduced that Blowfish is preferable in terms of speed taken security into consideration.

VI. CONCLUSION AND FUTURE WORK

Cloud computing has developed as a promising technique that significantly vicissitudes the modern Information technology manufacturing, it depends on sharing resources and assets that have never shared prior, prompting a new set of security challenges. There is a variability of information security risks that need to be sensibly considered, Risks will vary depending on the sensitivity of the data to be stored or processed. In this paper methods to solve some problems of cloud computing security was introduced form both perspectives client and provider by using encryption techniques.

REFERENCES

[1] P. M. Mell and T. Grance, SP 800-145. *The NIST Definition of Cloud Computing: National Institute of Standards & Technology*, 2011.

[2] M. T. Khorshed, A. B. M. S. Ali, and S. A. Wasimi, "*A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing*," Future Generation Computer Systems, vol. 28, pp. 833-851, 2012.

[3] S. Subashini and V. Kavitha, "*A survey on security issues in service delivery models of cloud computing*," Journal of Network and Computer Applications, vol. 34, pp. 1-11, 2011/01/01/ 2011.

[4] Z. Xiao and Y. Xiao, "*Security and Privacy in Cloud Computing*," IEEE Communications Surveys & Tutorials, vol. 15, pp. 843-859, 2013.

[5] S. Aldossary and W. Allen, "*Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions*," International Journal of Advanced Computer Science & Applications, vol. 7, 2016.

[6] D. Catteddu, *Cloud Computing: Benefits, Risks and Recommendations for Information Security*: Springer Berlin Heidelberg, 2009.

[7] L. Yan, C. Rong, and G. Zhao, "*Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography*," in International Conference on Cloud Computing, 2009, pp. 167-177.

[8] S. Hashemi, "*DATA STORAGE SECURITY CHALLENGES IN CLOUD COMPUTING*," International Journal of Security Privacy & Trust Management, 2013.

[9] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, et al., "*The Eucalyptus Open-Source Cloud-Computing System*," in Ieee/acm International Symposium on CLUSTER Computing and the Grid, 2009, p. 2008.

[10] I. Khalil, A. Khreishah, and M. Azeem, "*Cloud Computing Security: A Survey*," Computers, vol. 3, pp. 1-35, 2014.

[11] T. Mohanaprakash, A. I. Vinod, S. Raja, A. P. Kalyan, C. Babu, and G. Vivek, "*A Study of Securing Cloud Data Using Encryption Algorithms*," 2018.

[12] F. Li, Y. Rahulamathavan, M. Conti, and M. Rajarajan, "*Robust access control framework for mobile cloud computing network*," Computer Communications, vol. 68, pp. 61-72, 2015.

[13] K. K. R. Choo, J. Domingo-Ferrer, and L. Zhang, "*Cloud Cryptography: Theory, Practice and Future Research Directions*," Future Generation Computer Systems, vol. 62, pp. 51-53, 2016.

[14] R. Arora, A. Parashar, and C. C. I. Transforming, "*Secure user data in cloud computing using encryption algorithms*," Bulletin of Kawasaki College of Allied Health Professions, vol. 20, pp. 33-40, 2013.

[15] P. Samarati, S. D. C. di Vimercati, S. Murugesan, and I. Bojanova, "*Cloud security: Issues and concerns*," Encyclopedia on cloud computing, pp. 1-14, 2016.

[16] H. Wang, S. Wu, M. Chen, and W. Wang, "*Security protection between users and the mobile media cloud*," IEEE Communications Magazine, vol. 52, pp. 73-79, 2014.

[17] S. Ramgovind, M. M. Eloff, and E. Smith, "*The management of security in cloud computing," in Information Security for South Africa (ISSA)*, 2010, 2010, pp. 1-7.

[18] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "*An analysis of security issues for cloud computing*," Journal of Internet Services & Applications, vol. 4, p. 5, 2013.

[19] M. K. Neha, "*Enhanced Security using Hybrid Encryption Algorithm*," International Journal of Innovative Research in Computer and Communication Engineering, vol. 4, pp. 13001-13007, 2016.

[20] N. Chintawar, S. Gajare, S. Fatak, S. Shinde, and G. Virkar, "*Enhancing cloud data security using elliptical curve cryptography*," Int. J. Adv. Res. Comput. Commun. Eng, vol. 5, pp. 1-4, 2016.

[21] D. R. Stinson, Cryptography: Theory and Practice: CRC Press, 1995.

[22] B. Qin, H. Wang, Q. Wu, J. Liu, and J. Domingo-Ferrer, "*Simultaneous authentication and secrecy in identity-based data upload to cloud*," Cluster Computing, vol. 16, pp. 845-859, 2013.

[23] H. Wang, Q. Wu, B. Qin, and J. Domingo-Ferrer, "*Identity-based remote data possession checking in public clouds*," Information Security Iet, vol. 8, pp. 114-121, 2014.

[24] Edney, Arbaugh, and A. William, "**Real 802.11 Security: Wi-Fi Protected Access and 802.11i**," 2003.

[25] G. Thomas, J. V. Prem, and P. Afsar, "*Cloud computing security using encryption technique*," Computer Science, 2013.

[26] J. Zhang, "*Data Security and Privacy in Cloud Computing*," vol. 10, pp. 1-9, 2014.

[27] A. Amazon, "*Amazon Web Services Overview of Security Processes*," ed, 2015.

[28] J. Thakur and N. Kumar, "*DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis*," International journal of emerging technology and advanced engineering, vol. 1, pp. 6-12, 2011.

[29] R. Kaur and S. Kinger, "*Analysis of security algorithms in cloud computing*," International Journal of Application or Innovation in Engineering and Management, vol. 3, pp. 171-6, 2014.

[30] P. Arora, A. Singh, and H. Tyagi, "*Evaluation and Comparison of Security Issues on Cloud Computing Environment*," World of Computer Science & Information Technology Journal, vol. 2, 2012.

[31] M. A. Hossain, M. B. Hossain, M. S. Uddin, and S. M. Imtiaz, "*Performance Analysis of Different Cryptography Algorithms*," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 6, 2016.

[32] T. Hardjono and L. R. Dondeti, *Security in wireless LANs and MANs: Artech House*, 2005.

[33] R. Nigoti, M. Jhuria, and S. Singh, "*A survey of cryptographic algorithms for cloud computing*," 2013.

[34] S. Gambhir, A. Rawat, and R. Sushil, "*Cloud Auditing: Privacy Preserving using Fully Homomorphic Encryption in TPA*," International Journal of Computer Applications, vol. 80, pp. 18-21, 2013.

[35] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "*Privacy-Preserving Public Auditing for Secure Cloud Storage*," IEEE Transactions on Computers, vol. 62, pp. 362-375, 2013.

[36] M. G. Kaosar, R. Paulet, and X. Yi, "*Fully homomorphic encryption based two-party association rule mining*," Data & Knowledge Engineering, vol. s 76–78, pp. 1-15, 2012.

[37] M. Tebaa, S. E. Hajji, and A. E. Ghazi, "*Homomorphic Encryption Applied to the Cloud Computing Security*," Lecture Notes in Engineering & Computer Science, vol. 2197, 2012.

[38] R. L. Rivest, A. Shamir, and L. Adleman, "*A method for obtaining digital signatures and public-key cryptosystems*," Communications of the Acm, vol. 26, pp. 96-99, 1978.

[39] M. Mani, K. Shah, and M. Gunda, "Enabling Secure Database as a Service using Fully Homomorphic Encryption: Challenges and Opportunities," Geološki Vjesnik, pp. 219-229, 2013.

[40] S. K. Abd, S. A. R. Al-Haddad, F. Hashim, and A. Abdullah, "*A review of cloud security based on cryptographic mechanisms*," in International Symposium on Biometrics and Security Technologies, 2015, pp. 106-111.

[41] A. Kaur and M. Bhardwaj, "*HYBRID ENCRYPTION FOR CLOUD DATABASE SECURITY*," 2012.

[42] M. Jain and A. Agrawal, "*Implementation of hybrid cryptography algorithm," International Journal Of Core Engineering & Management (IJCEM)*, vol. 1, pp. 126-142, 2014.

[43] N. Sengupta, "*Designing of Hybrid RSA Encryption Algorithm for Cloud Security*," vol. 3, 2015.

[44] P. Garg and V. Sharma, "*An efficient and secure data storage in Mobile Cloud Computing through RSA and Hash function*," in Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on, 2014, pp. 334-339.

[45] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, "*A comparative survey of symmetric and asymmetric key cryptography*," in Electronics, Communication and Computational Engineering (ICECCE), 2014 International Conference on, 2014, pp. 83-93.

[46] A. Bhardwaj, G. Subrahmanyam, V. Avasthi, and H. Sastry, "*Security algorithms for cloud computing*," Procedia Computer Science, vol. 85, pp. 535-542, 2016.

[47] P. N. Penchalaiah and D. R. Seshadri, "*Effective Comparison and Evaluation of DES and Rijndael Algorithm (AES)*," International Journal on Computer Science & Engineering, vol. 2, pp. 1641-1645, 2010.

[48] M. Mittal, "*Performance Evaluation of Cryptographic Algorithms*," International Journal of Computer Applications, vol. 41, pp. 1-6, 2012.

[49] D. S. A. Elminaam, H. M. A. Kader, and M. M. Hadhoud, "*Performance Evaluation of Symmetric Encryption Algorithms*," Communications of the Ibima, vol. 8, pp. 280-286, 2009.

[50] S. El-Etriby, E. M. Mohamed, and H. S. Abdul-Kader, "*Modern Encryption Techniques for Cloud Computing Randomness and Performance Testing*," in ICCIT 2012, 12-14 March 2012, Al-Madinah Al-Munawwarah, Saudi Arabia, 2012.

[51] N. Mishra, M. S. Husain, and J. P. Tripathi, "*A Compendium Over Cloud Computing Cryptographic Algorithms and Security Issues*," RIET-IJSET: International Journal of Science, Engineering and Technology, vol. 7, pp. 810-814, 2015.

[52] O. P. Verma, R. Agarwal, D. Dafouti, and S. Tyagi, "*Peformance analysis of data encryption algorithms*," in International Conference on Electronics Computer Technology, 2011, pp. 399-403.

[53] Z. Shen, L. Li, F. Yan, and X. Wu, "*Cloud computing system based on trusted computing platform," in Intelligent Computation Technology and Automation (ICICTA)*, 2010 International Conference on, 2010, pp. 942-945.

[54] W. Stallings, "*Cryptography and Network Security: International Edition 4th edition - paper*."

[55] D. C. a. T. J. W. R. C, "*The Data Encryption Standard (DES) and its strength against attacks*," IBM Journal of Research and Development, vol. 38, pp. 243 - 250, May 1994.

[56] J. Bo, "*DES integrated with RSA encryption methods," Microcomputer Information*, pp. pp. 52-54,, 2007.

[57] F. Dengguo, "*Domestic and abroad research status and development trend of cryptography*," Journal of communications, pp. pp. 18-26, 2002.

[58] R. Rivest, A. Shamir, and L. M. Adleman, "*A method for obtaining digital signatures and public-key cryptosystems*," Communications of the Acm, vol. 26, pp. 96-99, 1978.

[59] R. L. Rivest, "*The MD5 Message-digest Algorithm*," Rfc, vol. 473, pp. 492-492, 1992.

[60] G. C. Kessler, "*An Overview of Cryptography*," 28 November 2018.

[61] Y. Zheng, J. Pieprzyk, and J. Seberry, "*HAVAL — A one-way hashing algorithm with variable length of output (extended abstract)*," in International Workshop on the Theory and Application of Cryptographic Techniques, 1992, pp. 81-104.

[62] P. Gauravaram and L. R. Knudsen, *Cryptographic Hash Functions*, 2009.

[63] D. Eastlake and P. Jones, "*US Secure Hash Algorithm 1 (SHA1)*," Rfc, vol. 37, pp. 105-113, 2001.

[64] M. Ogburn, C. Turner, and P. Dahal, "*Homomorphic encryption*," Procedia Computer Science, vol. 20, pp. 502-509, 2013.

[65] S. Goldwasser and S. Micali, "*Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information*," in Fourteenth ACM Symposium on Theory of Computing, 1982, pp. 365-377.

[66] T. Elgamal, "*A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*," IEEE Trans.inf.theory, vol. 31, pp. 469-472, 1984.

[67] B. Dan, E. J. Goh, and K. Nissim, "*Evaluating 2-DNF Formulas on Ciphertexts*," in International Conference on Theory of Cryptography, 2005, pp. 325-341.

[68] C. Gentry, *A fully homomorphic encryption scheme: Stanford University*, 2009.

[69] M. S. K. G. VNKV Subba Rao, A.Yashwanth Reddy, K.Narayana, "*Data Security in Bioinformatics*," Journal of Advanced Research in Computer Science and Software Engineering pp. pp. 590 – 598, November - 2013.