Proceedings of the Sixth International Conference on Research in Intelligent and Computing pp. 57–63
DOI: 10.15439/2021R7
ISSN 2300-5963 ACSIS, Vol. 27

Authentication and Encryption algorithms for data security in Cloud computing: A comprehensive review

Thanh Ngoc Nguyen
Department of Computer Networks
and Data Communications
Eastern International University
Binh Duong, Vietnam
thanh.nguyenngoc.set16@eiu.edu.vn

Thien T. T. Le
Faculty of Electronics
and Telecommunication
Saigon University
Ho Chi Minh City, Vietnam
thanhthien2003@gmail.com

***Abstract*—With the growth of data stored in cloud, data may become the target of attackers in the Internet. Therefore, the end users require high confidentiality, integrity and authentication in order to protect their data in cloud. In this paper, we aim at a comprehensive studying about the data security in cloud computing. The paper will discuss the details of cloud computing data security challenges and find out which are the most important challenges as well as the efficient solutions. The existing authentication and encryption algorithms are compared in terms of users' scenarios, outstanding features and the limitation. We also review the advantages and drawbacks of the algorithms for data security in terms of cloud computing services.**

***Index Terms*—cloud computing, data security, encryption, authentication.**

I. Introduction

CLOUD computing is one of the most popular technologies which allow many users using the resource without hardware implementation. Cloud computing is employed widely by both organizations and individuals because of its flexibility and mobility [1]. Cloud computing is a network model which is on-demand, efficient and users can access to shared resources, such as: storage, networks, ser-vice. The concept of cloud computing is X-as-a-Service or shortly called XaaS in which "X" represented to three major cloud service models as follows: (1) "S" for software which represented as Software-as-a-Service (SaaS); (2) "I" for infrastructure which represented as Infrastructure-as-a-Service (IaaS); (3) "P" for platform which represented as Platform-as-a-Service (PaaS). This concept allows many system components such as: databases, IT infrastructure can be distributed as a service. In IaaS, the cloud service provider provides users virtual machines and storage for higher business capabilities. In PaaS, the service provider delivers an environment to deploy, test and run applications. SaaS is the most used service, which allows user to use applications deployed by service provider. The Internet provides environment or platform for cloud computing through which many services are delivered to users. An important aspect of cloud computing is Utility-oriented which its strategy is "pay-per-use" to charge users.

Cloud computing has many advantages such as money saving, no up-front commitments, efficient resource allocation, and on-demand accessibility. However, there are some challenges for cloud computing which need to be taken into account such as data security, technical issues related to infrastructure management, legal issues due to different policies in distinct nations [1-3]. Security is the most important issue in cloud computing and it is growing dramatically every year. The main cause of security in cloud is its service models [4]. According to [5], each kind of cloud service models have its own security issues, which are listed as follows: (1) Security issues of SaaS: data theft by malicious attacks, unable to monitor data transfer amongst cloud users, etc.; (2) Cloud security issues experienced IaaS: unable to completely control the access to sensitive data, attackers can host a data theft attack in cloud infrastructure, security staff shortage, etc.; (3) PaaS's security issues: require a higher cost and bigger effort to implement and maintain the infrastructure, new types of cyber attacks. Therefore, the protection of data stored in cloud is urgently necessary; it can be achieved by employing authentication, virtualization and encryption, which help prevent unauthorized access [6]. It is necessary to develop the data security method in order to ensure the confidentiality, integrity, and availability of data in any circumstances [7]. There are many methods such as authentication, encryption, third-party auditing, identity and access management techniques which can be deployed in different cloud computing types [3, 8]. For example, in private cloud, the cloud owners use the form of Active Directory to store all of the credentials in the server and the authentication process are done via virtual private network. In public cloud, users can connect to service providers through Internet simultaneously and they can use any devices to access to cloud resources anywhere. This is the reason why public cloud exposes to be more vulnerable than private cloud, so the cloud providers have to include highly secured authentication methods.

In this paper, we will focus on the data security challenge, which is the hottest issues in cloud computing. We also explore distinct security challenges and also study about the methods used to remedy those issues. The data encryption and decryption will be described in terms of data security in cloud. The authentication method is also investigated in details.

This paper is divided into six sections. In the next section, we explain some threats to data in cloud computing. In section III, we will discuss some countermeasures to protect the data and provide some comparisons between

different solutions. We describe other existing algorithms for data security from relevant literature surveys in Section IV. In section V, the comparisons among distinctive algorithms are discussed in terms of encryption and authentication. Finally, the conclusion and the further challenges are given in Section VI.

II. THREATS IN CLOUD COMPUTING

Although cloud computing provides customers a great deal of benefits, it still has some drawbacks which cause the loss of data. Therefore, the customers cannot access the data stored in cloud or the data has been changed. These drawbacks include data breach, data loss, and insecure APIs. The threats in cloud computing are explained in Table I as follows.

TABLE I. MAIN DATA THREATS IN CLOUD COMPUTING

Types of threats	Causes	Consequences	Countermeasures
Data breach	Outside attacks, low-secured encryption and encryption key loss, malicious insider	Data can be viewed, stolen or destroyed	Strong encryption mechanisms, strong firewall, multifactor authentication methods
Data loss	Natural disaster or incidents caused by human, outside hackers	The loss of your data of the entire cloud system	Backup data frequently, strong encryption mechanisms, strong firewall, multifactor authentication methods
Insecure APIs	Interact with the programmes using the APIs in the wrong way or not safely; use or install insecure third-party programmes or unauthorized programmes	Data can be viewed, stolen or destroyed	Use only programmes from trusted sources

III. DATA SECURITY COUNTERMEASURES IN CLOUD COMPUTING

To prohibit and reduce the impacts of threats mentioned in previous section, some solutions have been employed by companies and cloud service providers. In this section, we will discuss about some popular countermeasures such as authentication and data encryption.

A. *Authentication*

Authentication is the process of determining the identity of users who want to access to the resources in cloud [3]. Four methods of authentication can be listed as follows: (1) something the individual knows, for example, a password; (2) something the individual possesses such as electronic or physical keys, which are commonly called token; (3) something the individual is, for instance, the finger-print, face or retina; (4) something the individual does, such as voice and hand-writing and so on. Authentication also provides access control service to compare the credentials of users with credentials stored in server. Some most popular types of authentication method are discussed as follow.

1) Biometric authentication.

In [9], biometric authentication is employed in the aspect of identification and authentication in cloud data security. Biometric refers to the biological sciences which can be listed in two main classes:

(1) Physiological and behavioral. Physiological is variable because it is different between people and it is relevant to human's physical body parts such as: fingerprints, facial recognition and so on.

(2) Behavioral is about the behavior of people such as signature and voice.

Details of biometric authentication technologies may consist of one or many features such as: finger print, face recognition, IRIS technology, hand geometry technology, retina geometry technology, speaker recognition, signature verification technique.

2) Multifactor authentication

Multifactor authentication employs not only one but also more than one factor to verify the users [10,11]. In the two-factor authentication, username and password are used to determine the user while accessing the cloud. In order to secure the authentication method, more than one factor is used such as voice recognition, facial recognition, or mobile identity number.

Beside credentials, some other techniques can be used as a secondary factor such as captchas, one-time password (OTP). Because of using more than one au-thentication factor, the security level of multifactor authentication is enhanced. OTP is often used in online transaction which can be explained as follows: the server creates an OTP which can be used only one time, and this OTP is sent to the users via two main means, mobile phone text or email [11]. Another mechanism can be used as secondary factor is captcha, this technique is quite popular and we can see it quite often when surfing the Internet. Captcha is employed to prevent web applications from attacks of malwares, there are a few types of captcha such as numbers, alphabet letters, images or a combination of numbers and letters [9,11].

In multifactor authentication, the more factors employed, the more secure the system is and to prove this, we make a comparison between two-factor authentication, which used handwriting recognition in addition to normal password, and five-factor authentication, which include password, voice recognition, facial recognition, Mobile identity number (IMEI) and International Mobile Subscriber Identity (IMSI) [8]. The detail comparison can be found in Table II below.

B. *Encryption*

Encryption is employed a lot these days to secure the information sent over the Internet and the secured information can only be seen by the intended recipient [12]. The overall process of encryption is described as follow: (1) encrypting plain text into cipher, (2) receivers who have a secret key can decrypt the cipher text into readable text; in both stages, a unique key is used by senders and receivers to

encrypt or decrypt. Depend on the number of keys used, we can separate encryption into two different types, symmetric and asymmetric [11-13].

1) Symmetric encryption

Symmetric encryption is also known as single-key encryption, which uses only one key for encryption and decryption. The use of symmetric must meet two requirements: (1) strong encryption algorithm; (2) the secret key transfer must be in a secure fashion. There are some popular symmetric algorithms such as DES, 3DES, Advanced Encryption Standard (AES). AES is a symmetric encryption algorithm which has a higher security level than DES and 3DES. Because there is not any successful attack against AES, it becomes one of the most popular encryption algorithms which is employed by major organizations such as banks, governments [15]. The AES Encryption algorithm is shown in Fig. 1.

In Fig. 1, the AES allows the key lengths of 16 bytes and 10 rounds in the en-cryption process. AES takes a 16-byte block as an input for encryption and de-cryption algorithm, this input block is used to make a 4x4-byte matrix, which was referred to as a State array. Most of the rounds, except the last round, consist of four distinct steps as follow: (1) SubBytes, where each byte is substituted based on a S-box; (2) ShiftRows, in which each row is shifted cyclically; (3) MixCol-umns, where each four bytes of each column is combined; (4) AddRoundKey is the step of combination of each byte of the state with the round key. The last round comprises only three stages, which are the same as in previous rounds, except the MixColumns step.

TABLE II. COMPARISON BETWEEN TWO-FACTOR AND FIVE-FACTOR AUTHENTICATION

Types of Authentications	**Two-factor authentication**	**Multi-factor Authentication**
Techniques	Handwriting recognition. Username and password	Username and password, voice recognition, facial recognition, Mobile identity number (IMEI), International Mobile Subscriber Identity (IMSI)
Strengths	The process of signing in is simple. Processing the handwriting figure on the cloud help reduces time consumption	All of the factors are processed in cloud, so the speed, time and efficiency are improved. The communication is secured by using transport security layer or secure socket layer. IMEI and IMSI are used to protect the system against the devices' loss.
Weaknesses	Some errors can occur because the change in users' writing style. There is no mutual authentication between the parties and also no protection against attacks.	It is too complicated for end users because too many factors are employed and there is also no mutual authentication.

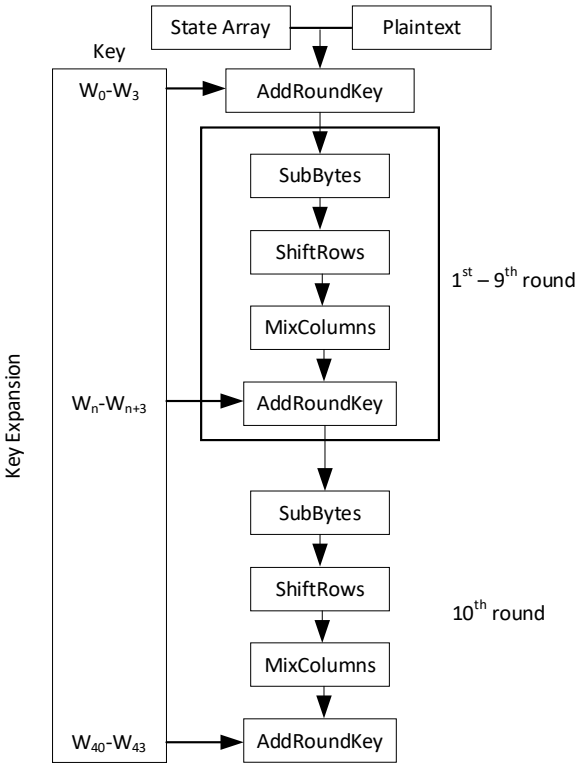

Fig. 1. AES Encryption [12, 15]

2) Asymmetric encryption

Asymmetric encryption or also called public-key encryption which uses two separated keys, named as public key and secret key [12, 15]. RSA is an acronym of its inventors' names, Rivest, Shamir and Adleman, it is used worldwide in encryption and digital signature [11]. The security level of this algorithm depends on the difficulty of the disintegration of large numbers and the public and private key are made from two large prime numbers. There are three main steps in RSA algorithm and all of them are listed as below: (1) key generation; (2) encryption; (3) decryption [16]. The key generation is shown Fig. 2.

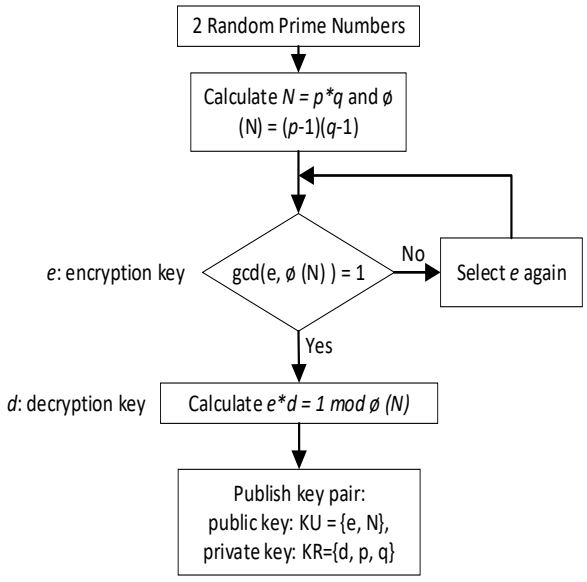

Fig. 2. RSA key generation [12,16]

The details of these three steps are described as below:

(1) Key generation: first, select two random prime numbers p and q. Then, compute the system modulus $N = p \times q$ and $\varnothing(N) = (p\text{-}1) \times (q\text{-}1)$. Afterwards, select a random encryption key e, where $1 < e \varnothing (N)$, $gcd(e, \varnothing (N)) = 1$. In the next step, compute decryption key d by solving the equation: $e \times d = 1 \bmod \varnothing (N)$ and $0 \leq d \leq N$. Finally, the public key $KU = \{e, N\}$ is published while the private key $KR = \{d, p, q\}$ is still kept.

(2) Data encryption: after acquiring the public key $KU = \{e, N\}$ from the first stage, we compute $C = M^e \bmod N$, where $0 \leq M < N$.

(3) Data decryption: we use the private key $KR = \{d, p, q\}$ to decrypt, we compute $M = C^d \bmod N$.

IV. EXISTING ALGORITHMS FOR DATA SECURITY IN CLOUD COMPUTING

A. *Data security in cloud computing using three-factor authentication*

In [17], the data security in cloud computing is protected by the three-factor authentications which consists of login phase, authentication phase, and biometric phase. The three factors are user credentials, fingerprints and passwords. In the initialization phase, the server chooses the private key and public key by using elliptical cryptography. Then, the user verifies himself with the server using these factors: identity, password, and the biometric imprints.

B. *Scrambling and descrambling of document image for data security in cloud computing*

In [18], the users may store their document image on cloud which requires high confidentiality, identity and authentication. The Arnold transform scrambling and descrambling is used to protect users' data. Before the users store their image in the cloud, the document images are applied by the Arnold Transformation. This process ensures that any unauthorized persons cannot be able to read the document image information. The users must apply the descrambling process to retrieve the original image.

C. *Towards DNA based data security in the cloud computing environment*

According to [19], many cryptography methods have been applied to protect data of the users in cloud. The DNA Based Data Security (DNABDS) encryption scheme is applied to calculate the secret key or the public key. The data is encrypted by the DNA based public key, then the users decrypt data by applying the DO's private key. The 1024-bit secret key is generated based on DNA computing, user's attributes and Media Access Control (MAC) address of the user, and decimal encoding rule, American Standard Code for Information Interchange (ASCII) value. The server and the users exchange data and keys by using the secure communication medium such as secure socket layer.

D. *Cognitive cryptography for data security in cloud computing*

In order to protect data of users, the advanced multilevel user authentication protocol is applied by using hybrid CAPTCHA codes. This type of authentication only is distributed for providing data access amongst the experts or trusted users of specific areas. These codes will define a new class of cognitive CAPTCHAs, which based on the recognition or interpretation of noisy pattern [20].

E. *Public-key encryption secure against related randomness attacks (RRA) for improved end-to-end security of cloud/edge computing*

In [21], the data security is provided by secure communication channel which requires the public key and private key at both users and the server. The author focuses on constructing secure public key encryption scheme against related randomness attacks. The RRA security under chosen plaintext attack (RRA-CPA) secure public key encryption scheme is derived from any publicly deniable encryption; and the RRA security under Chosen Ciphertext Attack (RRA-CCA) secure public key encryption scheme is derived from standard Indistinguishability under Chosen Ciphertext Attack (IND-CCA) public key encryption scheme with a hardcore function for arbitrarily correlated input [21].

F. *Cyber security risks in robotics*

In modern era, robotics is developing at a rapid pace and appears in every aspect of people around the world, this also leads to some new security challenges in this area. Therefore, some solutions were recommended to remedy the security issues, which include: Communication Robustness, Data Distribution Service in ROS, Authentication Mechanism in YARP, Securing the Cloud, Communication Buses. Robotics is expected to be one of the most important area in the future, and with the implementation of suggested solutions, the security risks in robotics can be reduced to the minimum [22].

G. *Internet memes: A novel approach to distinguish humans and bots for authentication*

In [23], bots have been overwhelmed the Internet and they have also evolved themselves to bypass some types of CAPTCHA authentication, making it difficult to distinguish human and bots. In order to eliminate automatic activities of bots, Internet Memes, a new type of authentication is employed. This type of authentication cannot be learnt by bots because Memes are dynamic and changed frequently, so it can identify which are human activities and which are bots' activities.

H. *Some cyberpsychology techniques to distinguish humans and bots for authentication*

These days, with the growth of Artificial Intelligence (AI), bots can imitate humans' behaviors to bypass traditional types of authentication and break into computer systems. Therefore, a psychology-based method is implemented to distinguish between humans and bots, which is called cyber-

psychological authentication. The deployment of cyber-psychological authentication includes lots of means, such as: pronunciation and translation checking, event classification and so on, and it has successfully differentiated between humans' behaviours and bots' behaviours [24].

I. Secure cloud computing authentication

In [25], the elliptic curve cryptography algorithm is applied to secure data transmission from a user to a server. In the system consists of two users and one server, the sender encrypts the plain text using the receiver's public key before sending the cipher text to the server. Then, the receiver uses its private key to decrypt data. The elliptic curve cryptography (EEC) is the public encryption which requires public key and private key. The EEC is less complexity than the RSA [12] but it provides the same security. However, the EEC requires higher in terms of size and computation requirements.

J. The elliptic curve cryptography- (ECC-) based three-factor authentication scheme

In [26], the cloud computing server combines IoT technologies which provide a huge amount of data from the IoT devices sending to the server of the cloud. The cloud server can be accessed by some authenticated users. The user's IoT devices are already registered by applying the ECC encryption. The user requests the registration phase by using the identity, password, and biometric information. The user logins the server and processes authentication steps through the public channel.

K. Secure authentication protocol for remote healthcare system

In [27], the secured authentication protocol is developed for remote healthcare systems where the server is connected to the IoT bio-devices monitor the patient. The IoT bio-devices will collect the data of patients then send to the server; the doctor can access the information of patient at the server through Internet. In [27], the authentication consists of five phases which are (1) system setup phase; (2) new sensor registration phase; (3) user registration phase; (4) login and authentication phase; (5) password changing phase.

L. Fingerprint-based authentication using single user credential in IoT

In [28], the user can access the cloud computing server's services by using the concept of Single Sign-On. The first step is registration and verification which uses the users' fingerprint scan, hash password and registration details. This information is encrypted by using the encryption key. The cloud server checks the registration and verification of the user; then setup a secure channel to the user. In the second step, the user can login by using his register's biometric registration.

V. COMPARISON AND DISCUSSION

A. Comparison

In this section, the comparison of current existing works on data security is summarized as in Table III. We compare the existing algorithms in terms of data encryption and authentication methods. The outstanding features and the limitations of these algorithms are also discussed and presented in Table III.

B. Discussion

The existing works focus on the authentication process which requires many parameters. The most common parameter is the biometric information such as DNA, fingerprint because they are unique. Therefore, the authentication and verification process will provide secure channel between the sender and the receiver or the user to the server. However, the public encryption scheme is widely used to protect the data because high security. It uses public key for encryption and private key for decryption.

TABLE III. COMPARISON BETWEEN CURRENT EXISTING WORKS ON DATA SECURITY

Current existing works	**Scenarios**	**Methods**		**Outstanding features**	**Limitation**
		Data encryption	**Authentication**		
Three-Factor Authentication [17]	Providing security for data in cloud	none	Credentials, fingerprints and passwords	Using elliptical cryptography	Simple process
Scrambling and Descrambling of Document Image [18]	Provide authentication process for users' document images	Arnold transform scrambling and descrambling	none	high confidentiality, identity for document image	Not mention other types of document
DNA based data security [19]	Protecting data of the users in cloud	DNA Based Data Security DNABDS) encryption scheme	none	The secret key is generated based on DNA computing and user's attributes results in high confidential of data	Slow performance
Multilevel user authentication protocol [20]	Providing data access amongst the experts	none	Hybrid CAPTCHA codes is based on the noisy pattern	Secures the confidential data	Limited applications which are only used for scientific data or experts
Public-key encryption secure against related randomness attacks (RRA) [21]	Improving end-to-end security of cloud computing	Secure public key encryption scheme	none	Avoid randomness attacks	Lack of authentication of the users

Internet memes [22]	Distinguish humans and bots for authentication	none	Internet Memes-based authentication, Memes are dynamic and changed frequently	Bots cannot learn to authenticate any service	Lack of datasets, extracting data from images may not be simple because the lack of tools
Cyberpsychology techniques to distinguish humans and bots for authentication [23]	Bots can imitate humans' behaviors to bypass traditional types of authentication	none	cyber-psychological authentication	Employ the psychological characteristics such as: pronunciation and translation checking, event classification	Reduce the users' experience because it takes time for users to answer the questions
Secure cloud computing authentication [25]	Data transmission from a user to a server	elliptic curve cryptography	none	Provide high secure channel	High complexity and calculation
The elliptic curve cryptography- (ECC-) based three-factor authentication scheme [26]	Data transmission from the IoT devices to the server of the cloud	elliptic curve cryptography	identity, password, and biometric information	Establish high secure channel between IoT devices and the server	High complexity and calculation of EEC crypto may require high memory and power at the IoT devices
Secure authentication protocol for remote healthcare system [27]	IoT and healthcare system	none	Identification of the sensor	Prevent replay attack and insider attack	The healthcare data should be encrypted because only the doctor can access the data
Fingerprint-based authentication using single user credential in IoT [28]	Single user in IoT – server transmission	none	fingerprint scan, hash password and registration details	The single account for multiple server may remove the fake user account	Data may require encryption at the receiver

VI. CURRENT ISSUES AND CHALLENGES

A. *Current issues*

In the view of users, cycle of data consists of six stages: create, store, use, share, archive and destroy. If the user store data in the cloud, it is needed to authenticate the users before carrying out any activities such as using, sharing, or deleting. Data should be protected to ensure the CIA triad which includes confidentiality, integrity, and availability. The cryptography algorithm is used to secure communication channel in which it needs having the key management mechanism. In RSA, two keys are used for establishing the secure channel between two end users require the mechanism to secretly distribute keys to the users.

B. *Challenges*

The users may be a mobile device, a laptop or any internet-connecting device which has limitation resources. Therefore, authentication mechanisms should be developed taken the resource of user into account which requires less computing, memory, and storage requirements. In addition, we also need to consider the devices of Internet-of-Things that are placed in the house, garden, or cars to collect the environment data. The sensing data may be stored in the cloud, then, only the authenticated users can access and modify data. The cryptographic and authentication method can be deployed together in order to prevent any attackers modifying data.

Even though encryption algorithm can secure data during transmission, the key management should be considered. In addition, the time complexity and computation of encryption should be low because of high energy consumption and high memory calculation. The elliptic curve cryptography is widely used to establish high data security during transmission.

In the recent years, a number of IoT devices increase which lead to a massive amount of data stored in cloud's server. It is necessary to provide a secure-direct communication from IoT devices to server in cloud [29]. The group users in cloud will be the new challenges because many applications require more than one user to access the same data in the cloud server. The authentication steps must collect biometric of different users then setup a secure channel. In the future, fog computing architecture and cloud computing will require the machine learning approach to manage the users, communication, and data of users [30-32].

VII. CONCLUSIONS

In this paper, we have gone through some concepts in Cloud computing which introduce the Cloud computing platform and different types of cloud. Some advantages and disadvantages of Cloud computing have been discussed. Therefore, we can help everyone make a choice easily if they are considering implementing a Cloud platform. We have done a research about a specific type of challenges that many Cloud computing platforms are facing these days, which are Data security threats.

We have made a study about how to prevent hackers to approach sensitive data of users in which the Cloud service providers are using Authentication. This solution requires the user to identify themselves when they want to log in the accounts. However, this method has some drawbacks, such

as the careless users can accidentally give their identifications for the hackers. Therefore, we have chosen to study about another solution with higher security level, Encryption. We have provided some information about encryption methods and the algorithms, which represent for those methods. In the future, we will develop and implement an authentication mechanism to evaluate the performance of different authentication methods.

REFERENCES

[1]. R. Buyya, C. Vecchiola, and S. T. Selvi, "Mastering cloud computing: foundations and applications programming". Elsevier, 2013.

[2]. P. R Kumar, P. H. Raj, and P. Jelciana, "Exploring data security issues and solutions in cloud computing" in Procedia Computer Science, vol. 125, pp. 691-697, January 2018.

[3]. Yunchuan Sun, Junsheng Zhang, Yongping Xiong and Guangyu Zhu, "Data security and privacy in cloud computing" in International Journal of Distributed Sensor Networks, July 2014.

[4]. 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" in IEEE Access, vol. 9, pp. 57792-57807, April 2021.

[5]. M. K. Sasubilli and V. R, "Cloud computing security challenges, threats and vulnerabilities", 2021 6th International Conference on Inventive Computation Technologies (ICICT), pp. 476-480, 2021.

[6]. Isma Zulifqar, Sadia Anayat, Imtiaz Kharal, "A review of data security challenges and their solutions in cloud computing" in I.J. Information Engineering and Electronic Business, March 2021.

[7]. M. De Donno, A. Giaretta, N. Dragoni, A. Bucchiarone and M. Mazzara, "Cyber-storms come from clouds: Security of cloud computing in the IoT era", May 2019.

[8]. T. S. Chou, "Security threats on cloud computing vulnerabilities" in International Journal of Computer Science & Information Technology, vol. 5, no. 3, June 2013.

[9]. D. Bhattacharyya, R. Ranjan, F. Alisherov and M. Choi, "Biometric authentication: A review" in International Journal of u-and e-Service, Science and Technology, vol. 2, no. 3, pp. 13-28, September 2009.

[10]. I. Indu, P. R. Anand, and V. Bhaskar, "Identity and access management in cloud envi-ronment: Mechanisms and challenges" in Engineering science and technology, an interna-tional journal, vol. 21, no. 4, pp. 574-588, May 2018.

[11]. J. K. Mohsin, L. Han, M. Hammoudeh, and R. Hegarty, "Two factor vs multi-factor, an authentication battle in mobile cloud computing environments" in Proceedings of the International Conference on Future Networks and Distributed Systems, pp. 1-10, July 2017.

[12]. W. Stallings, "Cryptography and network security principles and practice". 7th ed., Pearson, England, 2017.

[13]. R. Bhanot, R. Hans, "A review and comparative analysis of various encryption algorithms" in International Journal of Security and Its Applications, vol. 9, no. 4, pp. 289-306, April 2015.

[14]. N. Khanezaei and Z. M. Hanapi, "A framework based on RSA and AES encryption algorithms for cloud computing services" in 2014 IEEE Conference on Systems, Process and Control, pp. 58-62, Kuala Lumpur, Malaysia, December, 2014.

[15]. A. Sachdev and M. Bhansali, "Enhancing cloud computing security using AES algorithm" in International Journal of Computer Applications, vol. 67, no. 9, April 2013.

[16]. X. Zhou and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption" in IEEE Proceedings of 2011 6th international forum on strategic technology, vol. 2, pp. 1118-1121, August 2011.

[17]. S. Nalajala, B. Moukthika, M. Kaivalya, K. Samyuktha and N. L. Pratap, "Data security in cloud computing using three-factor authentication" in International Conference on Communication, Computing and Electronics Systems, pp. 343-354, Springer, Singapore, 2020.

[18]. N. Salimath, S. Mallappa, N. Padhy and J. Sheetlani, "Scrambling and descrambling of document image for data security in cloud computing" in Smart Intelligent Computing and Applications, pp. 283-290, Springer, Singapore, 2020.

[19]. S. Namasudra, D. Devi, S. Kadry, R. Sundarasekar and A. Shanthini, "Towards DNA based data security in the cloud computing environment" in Computer Communications, vol. 151, pp. 539-547, February 2020.

[20]. U. Ogiela, "Cognitive cryptography for data security in cloud computing" in Concurrency and Computation: Practice and Experience, vol. 32, no. 18, September 2020.

[21]. P. Liu, "Public-key encryption secure against related randomness attacks for improved end-to-end security of cloud/edge computing" IEEE Access, vol. 8, pp. 16750-16759, January 2020.

[22]. I. Priyadarshini, "Cyber security risks in robotics" in Cyber security and threats: concepts, methodologies, tools, and applications, pp. 1235-1250, IGI Global, May 2018.

[23]. I. Priyadarshini and C. Cotton, "Internet memes: A novel approach to distinguish hu-mans and bots for authentication" in Proceedings of the future technologies conference, pp. 204-222, Springer, Cham, October 2019.

[24]. I. Priyadarshini, H. Wang and C. Cotton, "Some cyberpsychology techniques to distinguish humans and bots for authentication" in Proceedings of the Future Technologies Conference, pp. 306-323, Springer, Cham, October 2019.

[25]. M. Chakraborty, B. Jana and T. Mandal, "A Secure Cloud Computing Authentication Using Cryptography," in Proceedings of International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR), 2018, pp. 1-4, doi: 10.1109/ICETIETR.2018.8529100..

[26]. H. Lee, D. Kang, Y. Lee, and D. Won, "Secure three-factor anonymous user authentication scheme for cloud computing environment". Wireless 2021Communications and Mobile Computing, vol. 2021, July 2021.

[27]. M. Azrour, J. Mabrouki and R. Chaganti, "New Efficient and Secured Authentication Protocol for Remote Healthcare Systems in Cloud-IoT", Security and Communication Networks, 2021.

[28]. B. Alemu, R. Kumar, D. Sinwar, G. Raghuwanshi, "Fingerprint Based Authentication Architecture for Accessing Multiple Cloud Computing Services using Single User Credential in IOT Environments", In Journal of Physics: Conference Series, Vol. 1714, No. 1, p. 012016.

[29]. P. Hajder, M. Hajder, M. Liput, M. Nycz, S. Agarwal, D. N. Barrell, & V. K. Solanki, "Direct communication of edge elements in the Industrial Internet of Things". In FedCSIS (Communication Paper) ACSIS, Vol. 23, pages 35–42 (2020).

[30]. C. Mechalikh, H. Taktak, F. Moussa, "PureEdgeSim: A Simulation Framework for Performance Evaluation of Cloud, Edge and Mist Computing Environments" Computer Science and Information Systems, Vol. 18, No. 1, 43–66. (2021).

[31]. B. N. Barreto, A. R. de Sa, & A. D. R. L. Ribeiro, "A Fog Computing Architecture for Security and Quality of Service". In FedCSIS (Position Papers), ACSIS, Vol. 19, pages 69–73, 2019.

[32]. M. Saleem, M. R. , Warsi, S. Islam, A. Anjum, & N. Siddiquii, "Trust Management in the World of Cloud Computing. Past Trends and Some New Directions", Scalable Computing: Practice and Experience, 22(4), 425-444, 2021.