


Encryption and Decryption Cloud Computing Data Based on XOR and Genetic Algorithm

Huthaifa A. Al Issa, Al-Balqa Applied University, Jordan

Mustafa Hamzeh Al-Jarah, Al-Balqa Applied University, Jordan

Ammar Almomani, IT Department, Al-Huson University College, AL-Balqa Applied University, Irbid, Jordan & Research and Innovation Department, Skyline University College, Sharjah, UAE*

 <https://orcid.org/0000-0002-8808-6114>

Ahmad Al-Nawasrah, British University of Bahrain, Bahrain

ABSTRACT

Cloud computing is a very large storage space that can be accessed via an internet connection. This concept has appeared to facilitate the preservation of personal and corporate data and the ease of sharing, and this data can also be accessed from anywhere in the world as long as it is on the internet. Large gaps have emerged around data theft and viewing. Accordingly, researchers have developed algorithms and methods to protect this data, but the attempts to penetrate the data did not stop. In this research, the authors developed a method that combines XOR and genetic algorithms to protect the data on the cloud through encryption operations and keep the key from being lost or stolen. The data that is uploaded to cloud computing may be important, and we should not allow any party to see it or steal it. Therefore, it became imperative to protect this data and encrypt it. The authors have developed an algorithm that uses XOR and genetic algorithms in the encryption process.

KEYWORDS

Cloud Computing, Decryption, Encrypting, Genetic Algorithm, XOR

INTRODUCTION

If a message has been altered or modified during transmission, the receiver must be capable of detecting it. No one should be able to exchange a false message for the actual message, or parts of it. (Delfs, Knebl, & Knebl, 2002; Gou, Yamaguchi, & Gupta, 2017). Fourthly, non-repudiation is the digital signature that provides the non-repudiation service to solve a problem that may happen when the sender does not pass the message.

The concept of cloud computing appeared around the year 2000, but the concept of computing appeared as a service around the year 1960 (“Zdnet,”), cloud computing is used to store and share data and it is a new form of data storage and retrieval. Examples include Google Drive, Dropbox, etc. A personal account is created with the username and password where a specific capacity is given to storage in the cloud, storage and access to data can be done at any time and from any place with the

DOI: 10.4018/IJACAC.297101

*Corresponding Author

internet, the cloud can be used by users, companies, and governments (Gupta, Yamaguchi, & Agrawal, 2018). In the cloud, you'll find everything from standard office apps to storage, networking, and the ability to handle natural language and artificial intelligence. (Al-Nawasrah, Almomani, Atawneh, Alauthman, & Computing, 2020; Almomani, Alauthman, Alweshah, Dorgham, & Albalas, 2019; Dorgham, Al-Rahamneh, Almomani, Khatatneh, & Computing, 2018; Manasrah, Smadi, ALmomani, & Sciences, 2017; "Zdnet,").

"Cloud computing" describes data centers that are accessible to multiple users via the Internet. (Bhushan, & Gupta, 2017; Mishra, Gupta, & Gupta 2020). The user can upload data on the cloud and share it with others; no one can take the data or know what the data is. In addition to that, cloud security consists of a set of procedures, controls, policies, and technologies that work together to protect systems, infrastructure, as well as cloud-based data. Storing data in the cloud rather than on local storage provides a number of advantages, but also raises questions about security and privacy. Store data in encrypted form to alleviate these issues. (Gupta, 2021).

Public, private, communal, and hybrid clouds are the four categories of clouds. The public cloud is a typical model and more popular, where users can use the cloud services by cloud service providers, such as Amazon, Google, etc. Private cloud use by a singular entity with high privacy, a private cloud used by organizations that required infrastructure for their applications, community cloud is used by a sociality of users, several organizations share the infrastructure, hybrid cloud is simply a combination of many clouds, it allows to users control in infrastructure.

The data on the cloud is hacked, due to poor protection and security. We specialize in data encryption operations (Stergiou, Psannis, Gupta, & Ishibashi, 2018; Gupta, & Agrawal, 2021), many encryption operations use a key to decryption and obtain data, in traditional encryption methods the key is stored with the user which leads to loss of the key and loss of information completely, we have developed a mechanism that stores the key with data and stores it in two clouds. When we apply our algorithm, we guarantee no data loss.

This research aims to develop a method that combines XOR and Genetic algorithm to protect the data on the cloud through encryption operations and keep the key from being lost or stolen. The benefits of this algorithm, we used a random key for encryption and decryption, so the hacker cannot determine the key. For this reason, our algorithm is more secure. The other parts of this study are illustrated through section No. 2, the related work encryption and decryption in cloud computing. Section 3 proposed a methodology for outlines the new encryption and decryption in cloud computing based on XOR and Genetic algorithm. Section 4 comprises the experiments and results, describes the data used in this paper. Finally, in Sect. 5 includes the conclusions and implications for future work.

RELATED WORK

Much of the personal data and information of companies and individuals are stored on the cloud, many hackers have access to all or part of the information, so researchers must find ways to protect this data.

In (Namasudra, Devi, Kadry, Sundarasekar, & Shanthini, 2020) proposed and explains a method that protects the data on the cloud with encryption and uses a long 1024-bit DNA based password generation technique based on a secret attribute of the user. Shivani Suggests developing the use of a genetic algorithm in the encryption process and storing the data encrypted in the cloud in a way that is difficult for hackers to access. Mall, S., & Saroj explains the mechanism of using the genetic algorithm in encrypting information and how it is stored in the cloud (Mall & Saroj, 2018). In (Kumari, Ekka, & Yadav, 2019) discusses some cryptographic algorithms such as Advanced Encryption Algorithm (AES), Data Encryption Standard (DES), IDEA, Blowfish Algorithm, Triple-DES (TDES), Rivest-Shamir-Adleman (RSA), and Diffie-Hellman Key Exchange. Wang, C., etc., (Wang, Wang, Ren, & Lou, 2010) propose a privacy-preserving public auditing system to protect the data on cloud computing, they use random masking and the homomorphic authenticator to prevent

the TPA from learning any knowledge about the data stored on the cloud server. In (Dhote, 2016) use homomorphic encryption, performed the multiplication and mod operations in encryption and decryption. (Jing, 2014) They are studying the cloud storage data protection model and executing encrypted storage of user data in the double-key form. They used asymmetric encryption algorithm to encrypt the user data and they used an asymmetric encryption algorithm to encrypt the secret key. They used AES Algorithm for encryption. The private key is managed and controlled by users, but the user may forget the key.

Riyaldhi & Kurniawan (Riyaldhi & Kurniawan, 2017) use AES, because of its slowness, they offer a novel way to speed up AES encryption using shift row and S. Box modification for mix column transformations.

Nie and Zhang (2009) study the two encryption algorithms DES and Blowfish. They analyzed the security for both algorithms and overviewed the base functions. Verma and Singh (2013) suggested a developed version of the Rivest Cypher 6 (RC6) Block Cipher Algorithm. These round-keys are used twice to encrypt the file in this produced version, which requires $2r+4$ additive rounds keys.

Goshwe and Security (2013) use precise message block sizes to construct encryption and decryption algorithms. Data can be transferred from one computer terminal to another via an unsecured network environment. Gupta and Sharma (2012) use asymmetric cryptography and they proposed a new method by combining the two algorithms RSA and Diffie-Hellman to achieve more security.

Qasem and Qataweh (2018) The use of MPI and MapReduce in parallel algorithms on a multi-core system helps speed up the Hill cipher algorithm.

Ramasamy, Prabakar, Devi, and Suguna (2009) present the implementation of Elliptic-Curve Cryptography (ECC). Firstly, they transformed the message into an affine point on the Elliptic-Curve (EC) and then used the knapsack algorithm on ECC encrypted message over the finite field $GF(p)$.

Arora, Khanna, Rastogi, & Agarwal (2017), an HCS that integrates both symmetric and asymmetric encryption to create an environment that is secure in cloud computing environments. To achieve this goal, they have developed a multi-factor authentication and encryption system that leverages many levels of cryptography.

PROPOSED METHODOLOGY

We enhancement new method to encryption and decryption data by using XOR and Genetic algorithm, then will upload or download data on/from a cloud. We will separate data after encryption into two files; each file is stored on a separate cloud. Our research is containing two parts. The two parts are encryption and decryption as shown in figure 1.

Data Features

The data used in the encoding and decoding processes are texts, and these texts may contain uppercase and lowercase letters. In addition to that, the text may contain numbers, symbols, or space.

Encryption Phase

For the clarification of the encryption process, we can realize this process in figure 2.

As we follow the steps in the flowchart, the steps are as following:

Step 1: Enter the data for encryption. For example (HI).

Step 2: We will convert data to ASCII code. The character (H) in ASCII code is equal (72) and the character (I) in ASCII code is equal (73).

Step 3: We will convert ASCII code to Binary. In our example, we have two numbers in ASCII code (72) and (73). When we convert (72) to binary is equal (01001000). Also, when convert (73) to binary is equal (01001001).

Figure 1. Our approach for cryptography

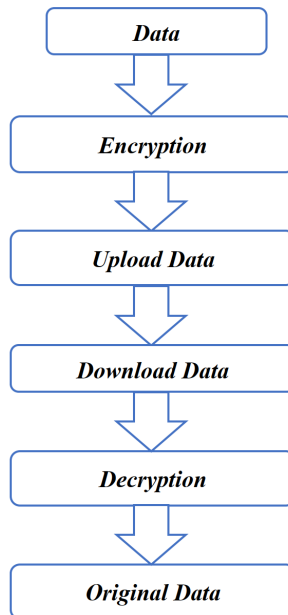
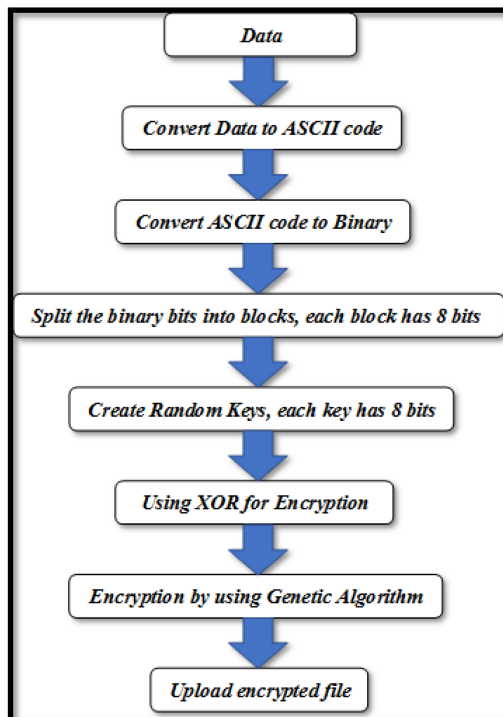


Figure 2. Encryption data approach



Step 4: We will split the binary into blocks, each block has 8 bits. In our example, the first block is (01001000) and the second block is (01001001).

Step 5: Create random keys, each key has 8 bits. The number of random keys is equal to the number of blocks. So, to complete our example, we let the first random key is (10001000) and the second random key is equal (11001100).

Step 6: Using XOR for encryption. In our example, when do XOR between the first block and the first random number (01001000 \oplus 10001000) the result is (11000000), and when do XOR between the second block (01001001) and the second random key (11001100) the result is (10000101).

Step 7: Encryption by using a Genetic algorithm. We will take the first 4 bits to start from the LSB of each block after doing XOR, then make a compliment for them. In our example, the first block is (11000000) and when we make a complement for the first 4 bits of the block the result is (11001111). Also, the second block is (10000101) and when we make a complement for the first 4 bits of the block the result is (10001010). The first block represents (İ) in ASCII code, and we know the random key for the first block represents (^) in ASCII code. The second block represents (Ş) in the ASCII code. Also, we know the random key for the second block represents (İ) in the ASCII code.

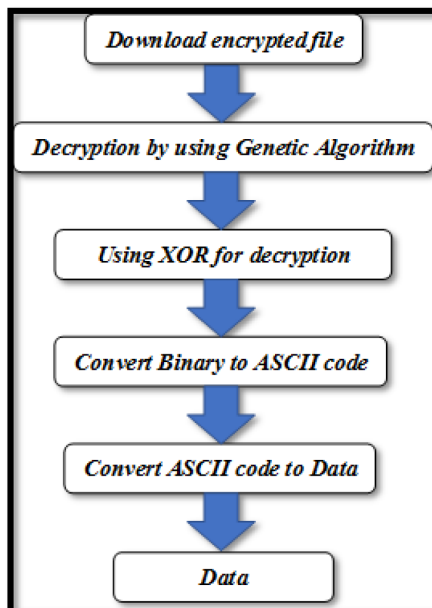
Step 8: Upload file encryption. Now when we encryption the data, we will upload the encrypted data on the cloud.

After finishing the encryption process, we separated the data into two files, and we arrangement each encrypted character and its random number into files. In which, the first character after encryption, we will store it in file 1 and its random number in file 2. Also, the second character after encryption, we will store in file 2 and its random number in file1. And so on, until the end data.

Decryption Phase

For the clarification of the decryption process, we can see this process in figure 3.

Figure 3. Decryption data approach



As we follow the steps in the flowchart, the steps are as following:

Step 1: Download the file from the cloud. We will download two files from the cloud.

Step 2: Decryption by using a Genetic algorithm. When we download two files, we take the first character from every file. We know the first character in file 1 represents the first encrypted character from data and the first character from file 2 represents the random key for the first encrypted character. In our example, file 1 contains (İİ) and file 2 contains (^Š). Now we convert each character to Binary, then we make a complement for the first 4 bits from the first encrypted character (İ in Binary is equal to 11001111) the result after making complement (11000000) and make complement for the first 4 bits from the second encrypted character (Š in Binary equal 10001010) the result after making complement(10000101).

Step 3: Using XOR for decryption, we make XOR between the result of the Genetic algorithm and its random key. In our example, when do XOR between the first character and its random number (11000000 \oplus 10001000) the result is (01001000), and when do XOR between the second character and its random number (10000101 \oplus 11001100) the result is (01001001).

Step 4: Convert Binary to ASCII code. We will convert the result of XOR for each character to ASCII code. In our example, the first character (01001000) is equal in ASCII code (72), and the second character (01001001) is equal in ASCII code (73).

Step 5: Convert ASCII code to Data. The first result (72) represents (H), and the second result (73) represents (I).

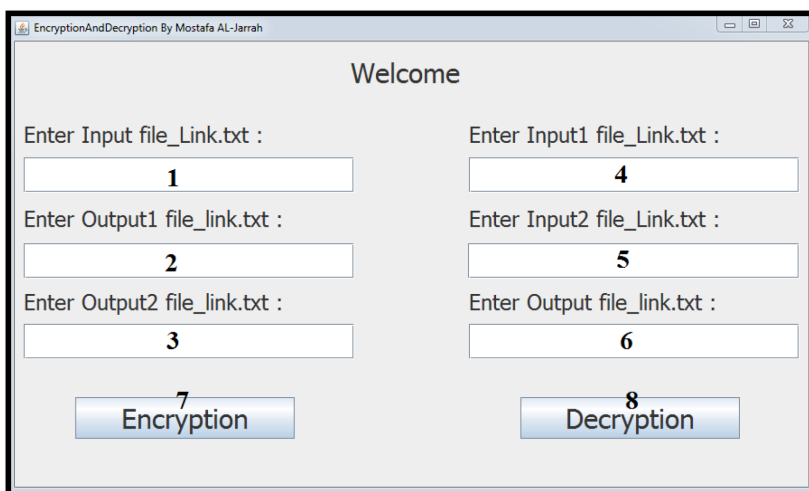
Step 6: We will get original data (HI).

TESTING AND RESULTS

We created a program to run our algorithm by using JAVA language. The specification of the laptop that runs the program is Windows 7 Ultimate 64-bit and CPU is Intel-COREi3 and 8GB-RAM, and we developed a desktop application (GUI). This GUI application can encrypt and decrypt any text regardless of its size.

The window of the application is containing some elements, as we see in figure 4.

Figure 4. Encryption and decryption application



To perform the encryption process, we put the data file link in 1 and we put the link of the files where the encrypted data is stored in 2 and 3, then we press the encryption button 7. To perform the decryption process, the links of the encrypted files are placed in 4 and 5 steps and the link of the file to store data after decryption in 6, then we press the decryption button 8.

As we can see in the example below, we encrypted and decrypted (HI). We can see it in figure 5. We followed the output of each step in the encryption process. As shown in figure 6.

Figure 5. Encryption and decryption example

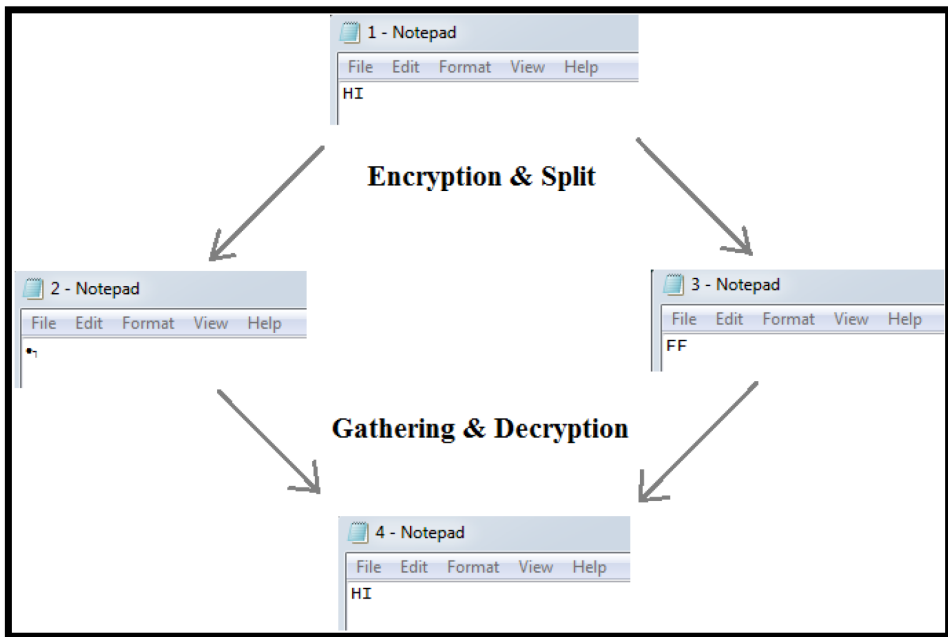


Figure 6. Output of each step at encryption process, (A) String to Ascii, (B) Ascii to Binary, (C) Encrypting, (D) Binary to Ascii, and (E) Ascii to String

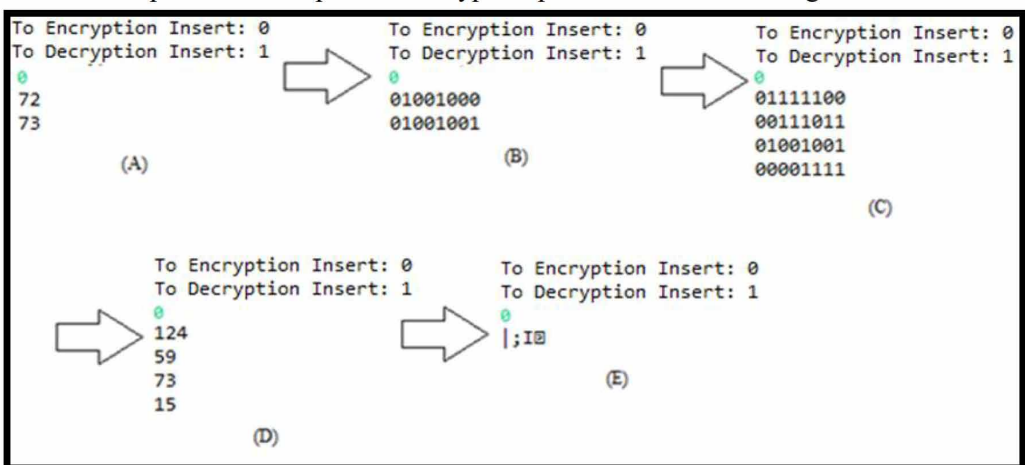
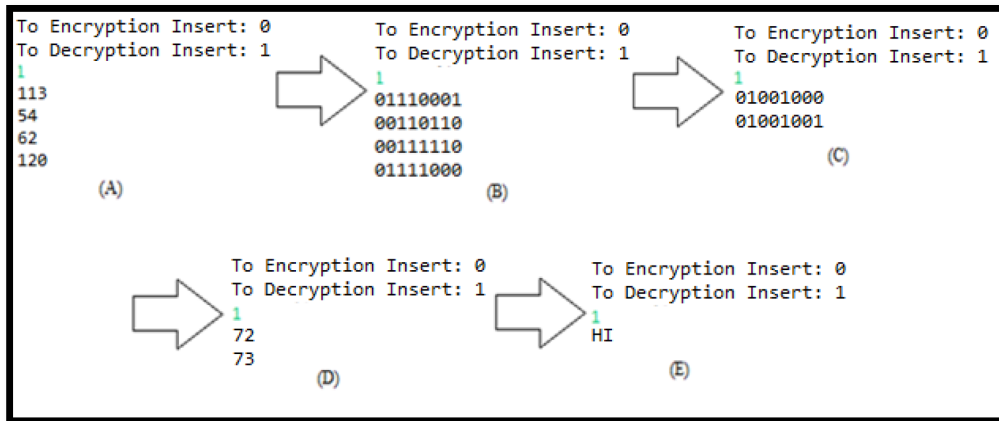


Figure 7. Output of each step at decryption process, (A) String to Ascii, (B) Ascii to Binary, (C) Decrypting, (D) Binary to Ascii, and (E) Ascii to String



In part (A), we converted from string to ASCII, in part (b) we converted from ASCII to binary, in part (c) we made encryption process, in part (d) we converted from binary to ASCII and in part (e) we converted from ASCII to string.

We followed the output of each step at the decryption process, as shown in figure 7.

In part (A), we converted from string to ASCII, in part (b) we converted from ASCII to binary, in part (c) we made decryption process, in part (d) we converted from binary to ASCII and in part (e) we converted from ASCII to string.

CONCLUSION AND FUTURE WORKS

The data that is uploaded to cloud computing may be important and we should not allow any party to see it or steal it. Therefore, it became imperative to protect this data and encrypt it. We have developed an algorithm that uses XOR and genetic algorithms in the encryption process. We divide data into two files that any file depends on each other, and we store each file on a cloud. Our method is much better than other methods.

In our method, However, encryption does not solve all of the problems associated with privacy, like the inability to perform a basic search and a restriction in flexibility when sharing data with other users, among others. To further ensure protection, we suggest using algorithms that rely on random storage or improving the storage method, and we also suggest using algorithms to compress files and reduce the size of files.

REFERENCES

- Al-Nawasrah, A., Almomani, A. A., Atawneh, S., & Alauthman, M. J. (2020). *A Survey of Fast Flux Botnet Detection With Fast Flux Cloud Computing*. Academic Press.
- Almomani, A., Alauthman, M., Alweshah, M., Dorgham, O., & Albalas, F. (2019). *A comparative study on spiking neural network encoding schema: implemented with cloud computing*. Academic Press.
- Arora, A., Khanna, A., Rastogi, A., & Agarwal, A. (2017, January). Cloud security ecosystem for data security and privacy. In *2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence* (pp. 288-292). IEEE. doi:10.1007/978-981-13-0277-0_31
- Bhushan, K., & Gupta, B. B. (2017). Security challenges in cloud computing: State-of-art. *International Journal of Big Data Intelligence*, 4(2), 81–107. doi:10.1504/IJBDI.2017.083116
- Delfs, H., Knebl, H., & Knebl, H. (2002). *Introduction to cryptography* (Vol. 2). Springer. doi:10.1007/978-3-642-87126-9
- Dhote, C. (2016). *Homomorphic encryption for the security of cloud data*. Academic Press.
- Dorgham, O., Al-Rahamneh, B., Almomani, A., & Khatatneh, K. F. (2018). *Enhancing the security of exchanging and storing DICOM medical images on the cloud*. Academic Press.
- Goshwe, N. (2013). *Data encryption and decryption using RSA algorithm in a network environment*. Academic Press.
- Gou, Z., Yamaguchi, S., & Gupta, B. B. (2017). Analysis of various security issues and challenges in cloud computing environment: a survey. In *Identity Theft: Breakthroughs in Research and Practice* (pp. 221-247). IGI Global. doi:10.4018/978-1-5225-0808-3.ch011
- Gupta, B. (2021). *Secure Searchable Encryption and Data Management*. CRC Press.
- Gupta, B. B., & Agrawal, D. P. (2021). *Security, privacy, and forensics in the enterprise information systems*. doi:10.1109/TENCON.2009.5396115
- Gupta, B. B., Yamaguchi, S., & Agrawal, D. P. (2018). Advances in security and privacy of multimedia big data in mobile and cloud computing. *Multimedia Tools and Applications*, 77(7), 9203–9208. doi:10.1007/s11042-017-5301-x
- Gupta, S., & Sharma, J. (2012). *A hybrid encryption algorithm based on RSA and Diffie-Hellman*. Paper presented at the 2012 IEEE International Conference on Computational Intelligence and Computing Research. doi:10.1109/ICCIC.2012.6510190
- Jing, P. (2014). *A new model of data protection on cloud storage*. Academic Press.
- Kumari, M., Ekka, D., & Yadav, N. (2019). An EHSA for RSA Cryptosystem. In *Advances in Data and Information Sciences* (pp. 375–385). Springer.
- Mall, S., & Saroj, S. K. (2018). *A new security framework for cloud data*. Academic Press.
- Manasrah, A. M., Smadi, T., & Almomani, A. (2017). *A variable service broker routing policy for data center selection in cloud analysts*. Academic Press.
- Mishra, A., Gupta, N., & Gupta, B. B. (2020). Security threats and recent countermeasures in cloud computing. In *Modern principles, practices, and algorithms for cloud security* (pp. 145–161). IGI Global. doi:10.4018/978-1-7998-1082-7.ch007
- Namasudra, S., Devi, D., Kadry, S., Sundarasekar, R., & Shanthini, A. (2020). *Towards DNA-based data security in the cloud computing environment*. Academic Press.
- Nie, T., & Zhang, T. (2009). A study of DES and Blowfish encryption algorithm. Paper presented at the Tencon 2009-2009 IEEE Region 10 Conference.
- Qasem, M. H., & Qatawneh, M. (2018). *Parallel Hill Cipher Encryption Algorithm*. Academic Press.

Ramasamy, R. R., Prabhakar, M. A., Devi, M. I., & Suguna, M. (2009). *Knapsack-based ECC encryption and decryption*. Academic Press.

Riyaldhi, R., & Kurniawan, A. (2017). *Improvement of advanced encryption standard algorithm with shift row and S. box modification mapping in mix column*. Academic Press.

Stergiou, C., Psannis, K. E., Gupta, B. B., & Ishibashi, Y. (2018). Security, privacy & efficiency of sustainable cloud computing for big data & IoT. *Sustainable Computing: Informatics and Systems*, 19, 174–184. doi:10.1016/j.suscom.2018.06.003

Verma, H. K., & Singh, R. K. (2013). *Enhancement of RC6 block cipher algorithm and comparison with RC5 & RC6*. Paper presented at the 2013 3rd IEEE International Advance Computing Conference (IACC). doi:10.1109/IAdCC.2013.6514287

Wang, C., Wang, Q., Ren, K., & Lou, W. (2010). Privacy-preserving public auditing for data storage security in cloud computing. *2010 Proceedings IEEE Infocom*. doi:10.1109/INFCOM.2010.5462173

Zdnet. (n.d.). Retrieved from <https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/>

Huthaifa A. Al Issa received his Bachelor's and Master's degrees in Electrical Engineering at the Near East University, Cyprus, in 2003 and 2005, respectively with high honors GPA. He received his Ph.D. degree in Electrical Engineering at the University of Dayton, Dayton, OH, USA, in 2012. Currently, he is an assistant professor in the Department of Electrical and Electronics Engineering at AL-Balqa Applied University. He has been a member of the Jordan Engineers Association (JEA) since 2003.

Mustafa Al-Jarah obtained his bachelor's degree in 2021 in the major of Telecommunication and Software Engineering from the Electrical and Electronic Engineering Department of Al-Balqa Applied University. He graduated with an excellent grade, he was first in the department and first in the class.

Ammar Almomani received his Ph.D. Degree from Universiti Sains Malaysia (USM) in 2013. He has published more than 75 research papers in International Journals and Conferences of high repute including IEEE, Elsevier, ACM, Springer, Inderscience, etc. with many international awards, He has visited several countries to present his research work, he is serving as a reviewer for 10s Journals of IEEE, Springer, Wiley, Taylor & Francis, etc. he has 16 years of experience with taught more than 40 different subjects in computer science, networks, and cybersecurity, and programming language, he has many international certificates and participation in dozens of projects and specialized scientific courses, His research interest includes cybersecurity, advanced Internet security and monitoring, currently, he is a senior lecturer at Al- Balqa Applied University and a professor with head of research and innovation department in SKYLINE university college-SHARJAH-UAE. link: https://scholar.google.com/citations?user=d_tRtPkAAAAJ&hl=en.

Ahmad Al Nawasrah received his PhD in Computer Science-Information security from the University of Salford, UK in 2018. Currently, Dr. Al Nawasrah is an assistant professor at ICT college, British University of Bahrain. He has published several research papers in International Journals and Conferences with high reputation, where some of these publications are tracked by Thomson Reuters (ISI) and Scopus. His research interests lie in information security, internet cyber-crimes.