

**How to Cite:**

Alghamdi, A. G., AlZain, M. A., & Masud, M. (2022). Cloud computing environments and management for big data security, and performance (CBDS) Model. *International Journal of Health Sciences*, 6(S1), 8860–8878. <https://doi.org/10.53730/ijhs.v6nS1.7030>

# Cloud computing environments and management for big data security, and performance (CBDS) Model

**Amal G. Alghamdi**  
**Mohammed A. AlZain**  
**Mehedi Masud**

**Abstract**---Big data is a technology that is growing at a tremendous speed in many sectors and fields, and this huge growth is also accompanied by the development of cloud computing, Cloud computing provides innovative organization in order to be able to meet the services you need to deal with big data in terms of infrastructure, where big data is processed and stored in the companies and establishments concerned, and unfortunately, still, It suffers from several problems and gaps that may threaten the security of this data In order to improve data security in cloud computing, provide secure access, and improve performance. This paper will discuss several concerns that may threaten data security, access, and cloud computing performance while managing big data, and that is by proposing a model(CBDS) Cloud for Big Data Security to develop performance in cloud management that meets several needs that will contribute to maintaining data integrity and confidentiality, providing secure access to data, and will greatly improve the performance of the cloud during data processing, storage, and recovery from the cloud at the user's desire and in complete security.

**Keywords**---big data, cloud computing, cloud computing performance, database, cloud security, data integrity, data security.

## Introduction

Cloud foundation scales on request to help fluctuating jobs which has brought about the versatility of information created and devoured by the big data applications. Cloud virtualization can make a virtual foundation of worker working frameworks and capacity gadgets to produce various machines simultaneously. This gives a cycle to share assets and disconnection of equipment to expand the entrance, the board, investigation, and calculation of the information [1,6]. By encrypting data by any strong encryption method or creating effective protection systems to improve performance and maintain data

confidentiality and integrity the importance arises of security and protection Information are one of the significant parts of big data in cloud computing, as information is facilitated as data is processed and hosted on the third-party services and framework, keeping up with protection and security is a major test [3]. The greater the volume, assortment, the veracity of enormous data the higher the danger related to its protection and security. In this paper, we will create a big data model to provide better performance and data safety and keep it in the cloud from unauthorized people, called (CBDS). The result of the proposed new model will be examined and implemented, in the appropriate manner to display the elements of big data security in cloud computing, for example, data confidentiality, data integrity, cloud computing performance, and service availability. The (CBDS) model allows users to make different forms of queries, for example, adding user data and querying authorized employees to query information about users and all this is done in a safe, fast, and excellent performance. In the cloud. Security risks such as data confidentiality, data integrity, security, and managed strategies from a cloud manager, all will be considered in the model.

### **Research Problem**

There are many research problems and gaps of big data in Cloud Computing environment related to data integrity, access control, and time performance. This thesis discusses the following problem statements:

1. How to provide secure access control to the big data in the environment of cloud computing?
2. How to provide integrity to the big data in the environment of cloud computing?
3. How to provide efficient performance for big data in the environment of cloud computing?

### **Aims and Objectives**

CBDS model ensures different aspects such as big data security Data integrity, big data Access control, Data performance, cloud performance, cloud management.

### **Research Methodology**

In the literature review, a theoretical analysis of different aspects of our proposed model such as big data in cloud security, big data in cloud performance. In addition, an experiment will be given at end of the theses to prove efficiency and performance for our proposed model. The stages of the methodology are defined as shown to conduct the research.

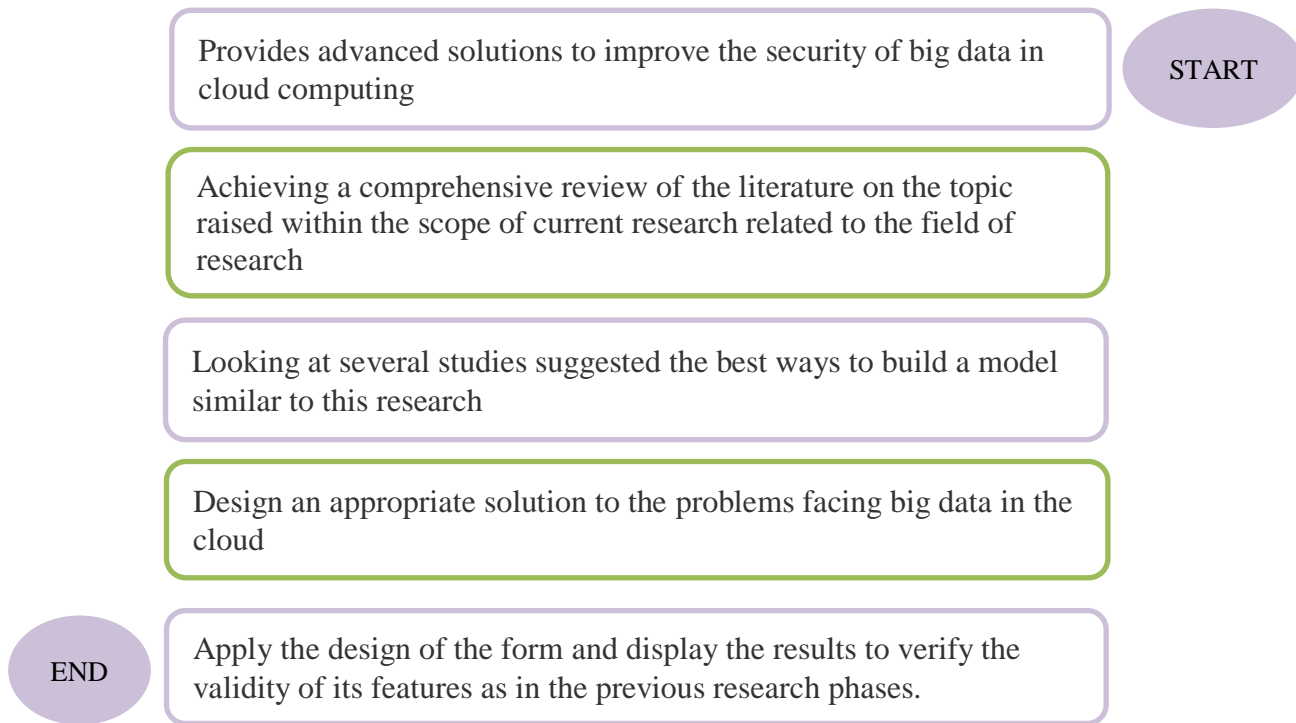


Figure 1. Big Data in Cloud Computing Model

Security of big data in the cloud is significant because data should be shielded from malevolent interlopers treats and how the cloud suppliers safely keep up with gigantic space of the. What Is Big Data's Relationship to The Cloud? How does the cloud processing climate relate to big data? The response to this inquiry mirrors the connection between them. This is done through the cloud processing highlights to deal with big data, the assets given by cloud registering, the asset administration to offer support to numerous clients where the different physical and virtual assets are consequently set and reset upon demand [2]. Figure:1. Shows an overview of the general cloud computing model. The user enters his data into the cloud, and the employee sends a query and receives information from the cloud, where he can direct data inquiries to the server for example in the social security system, the cloud is supposed to be confidential and secure, so the data source is stored on the cloud side, to ensure the reliability of Privacy and security of the query [7-13]. A problem may occur when the cloud service loses its reliability.

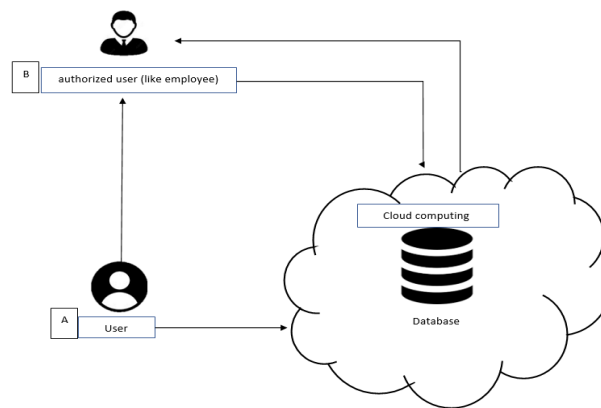


Figure 2. General cloud computing model.

### Proposed (CBDS) Model

Provides data weighting and classification CBDS model to show the data that is encrypted by the Advanced Encryption Standard AES symmetric service provider, after using the DED algorithm. This strategy is known as one of the best strategies used to improve cloud computing performance and maintain information security, and in this model we modified it To suit the requirements of the proposed system in order to increase performance and maintain data integrity and confidentiality, it has been divided into three stages, from the beginning of receiving user data before entering it until it is saved in the database in the cloud until it is recalled from the database, in order to further improve performance and maintain data confidentiality and safety from modification . Cloud computing for using the secure healthcare data security [14-22] and the use of 5G technologies with other cutting-edge technologies for the data transfer and data security including the blockchain, ransomware protection, etc. can enable further data security, and the same can be implemented for the educational data protection and security as well. In addition to that cloud security also essential for all applications.

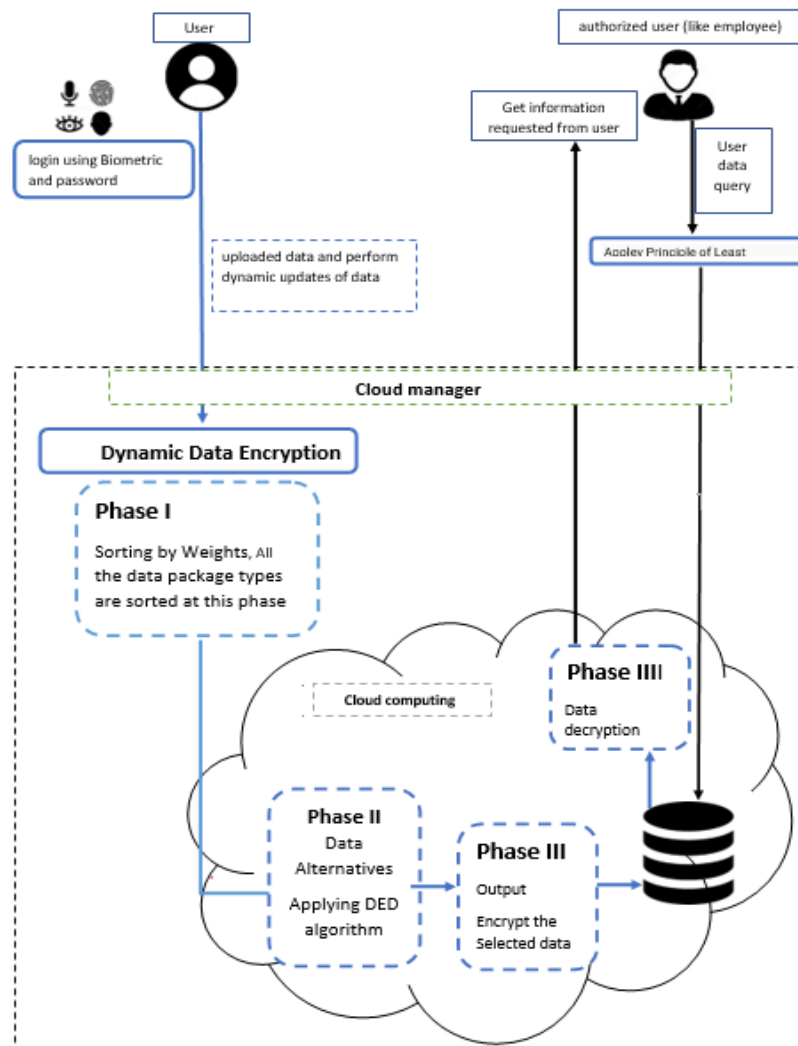


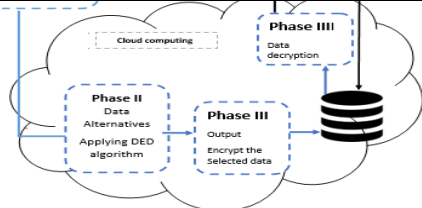



Figure: 3 (CBDS) model

### (CBDS) Component

It's clear from Table that (CBDS) model consists of several components such as the user who is supposed to enter his data after the password and fingerprint, also the cloud manager responsible for managing the data inside the server, also the DDE which is a strategy to improve cloud performance and maintain data integrity Starting from the first stage, which is to classify the data according to its weight and then apply the DED algorithm, then encrypt the selected data and save it in the database And when the authorized employee wants to search for user data, he must pass Appley Principle of Least Privilege in order to preserve the integrity of the data from modification, then pass the request to the data manager, who in turn decrypts the encrypted data and sends it to the authorized employee to receive the information.



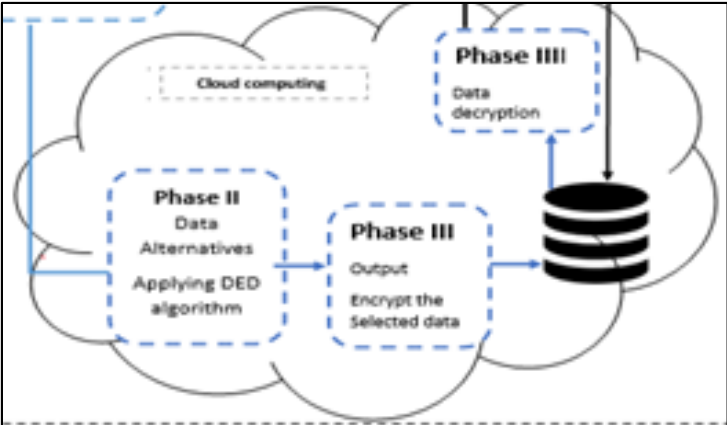
Table 1  
(CBDS) Component

CBDS Component	Description
	The user who logs in to add and update data
<div>login using Biometric and password</div> 	The end point at which the user proves that he is authorized to enter, by entering the password and choosing one of the biometric methods
<div>Cloud manager</div>	Cloud manager specializes in managing cloud computing services, including transferring data from one stage to another and even recovering data from the database and sending it to the employee
<div>Dynamic Data Encryption</div>	This strategy specifically encrypts data to protection at the most elevated level, consists of several phases
	Cloud computing, where it implements two phases of strategy Dynamic Data Encryption Strategy, and in which data is stored in an encrypted form.
	Query employee who logs into the server to send an unencrypted query to the cloud about the user
<div>Appley Principle of Least</div>	Reducing the powers given to the employee to limit access to unauthorized data

### CBDS Layers

The CBDS model has three layers. The table shows the three layers, namely, the application layer, the presentation layer, and the management layer. In the presentation layer, it includes the user's browser. In the management layer, it includes the data cloud computing management system where the cloud service provider receives. It receives user data and then applies steps Dynamic Data Encryption Strategy to it to encrypt and store it in the database and decrypt it also when the employee makes a query.

Table 2  
CBDS Layers

Layers	CBDS Component	
Presentation Layer	 <div>User</div>	 <div>authorized user (like employee)</div>
Application Layer	<div>login using Biometric and password</div>	<div>Apply Principle of Least</div>
Management Layer	<div>Cloud manager</div> 	

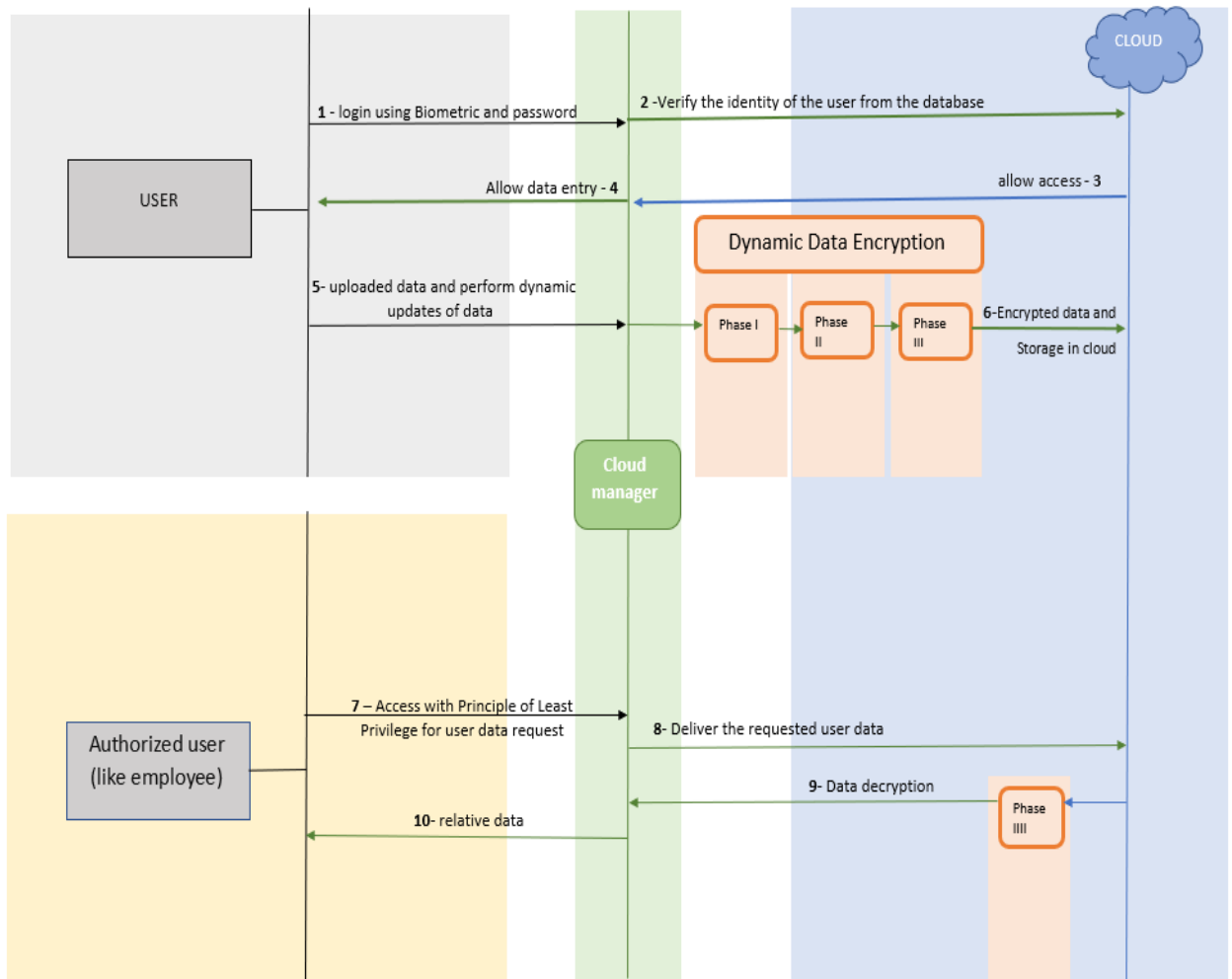


Figure: 3 model data flow (CBDS)

### Model data flow (CBDS)

- This part explains the flow of data in the CBDS Form and shows the process of sending data to cloud computing, then it shows how the user performs data entry and the employee performs the query through the CBDS form in a special way. Moreover, it describes how to move forward in improving the performance of cloud management and big data encryption by using Dynamic Data Encryption strategy which consists of 4 phases and is more secure than traditional techniques.
- Perform data retrieval this section describes the flow of data from the database to the fourth stage. The employee query reaches the cloud manager in a secure connection, and then the employee query of the user data is sent unencrypted from the database to the fourth stage of the Dynamic Data Encryption strategy



### Dynamic Data Encryption Strategy

This strategy specifically encrypts data to boost the volume of encoded data under the necessary planning Constraints, which is intended to secure information proprietors' protection at the most elevated level when utilizing the relevant gadgets and systems administration offices. The significant methods utilized:

- (1) Classifying data packages as per protection level.
- (2) decide if data packages can be encrypted under timing constraints.

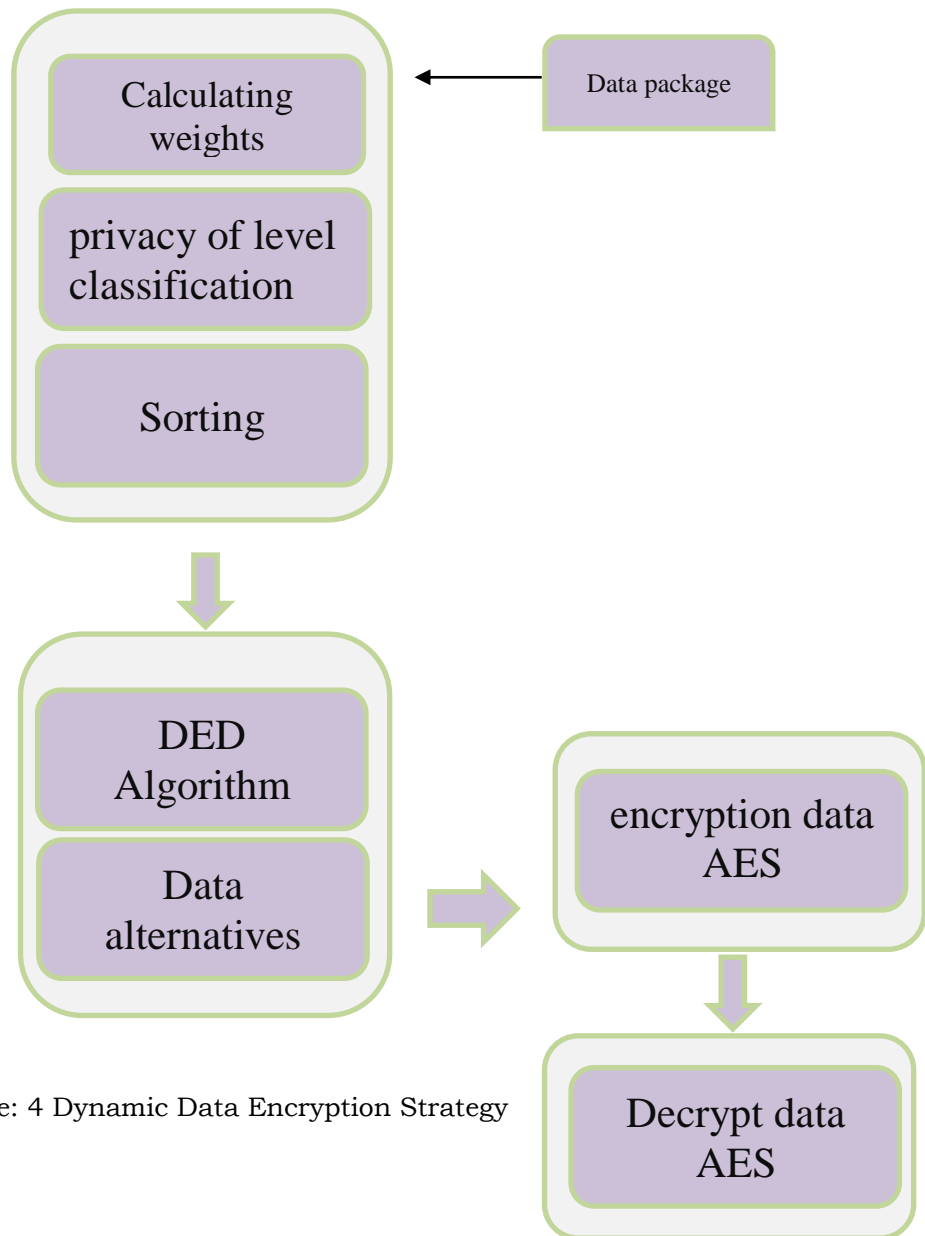


Figure: 4 Dynamic Data Encryption Strategy

**Phase I: Sorting by Weights**

The main stage: arranging by weight

This is the main phase of the proposed model. A wide range of information bundles are arranged now. Screening processes are two vital elements. Both execution time (performance) and security insurance (Security), and it happens after the client signs in, checks his personality, and afterward permits him to enter the server and add information

**Phase II: data surrogates**

This stage inside distributed computing, we pick information parcels for encryption activities. We propose the DED calculation to achieve this stage. The S Table will be utilized to give a reference to assurance abilities. A basic working rule is that an information parcel with a higher SDi esteem has a more elevated level of substitute need than information bundles with lower esteems than SDI (What does SDI mean? Sequential Digital Interface (SDI) is a norm for computerized video correspondence utilizing a coaxial link While information rates of up to 3 gigabits each second (Gbps) are conceivable with SDI, the most widely recognized speed is a large portion of the speed at 270 Mbps are some sub-steps to choosing data packets

First, the timing range must be determined.

Second, the data substitutions are implemented.

**Phase III: the output**

This stage produces as the output of a coding strategy derived from the correct results of the second stage. Those data with a higher level of encryption priority will be selected for encryption under certain restrictions and then entered the database.

**Phase IIII: decryption**

After the employee requests the user's data, the process of decrypting the data from the database takes place.

**The algorithm DED**

This algorithm is used to dynamically select data packages that can be encrypted under certain conditions when considering both timing constraints and resources capacities Dynamic Encryption Determination Algorithm (DED) algorithm. This algorithm is designed to dynamically select data packages that can be encrypted under certain conditions, which considers both timing constraints and facilities' capacities.

**The Advanced Encryption Standard (AES)**

To offer secure communication through the organization, encryption calculation assumes a significant part. It is an important and principal component for the data protection. Encryption calculation changes over the information into the mixed structure with the utilization of "a key" and just the client have the way to decode the information. Concerning investigates that have been made, a significant encryption method is the Symmetric key Encryption.

At the end of this chapter, and after we have presented the proposed model and explained the currency mechanism, we will start applying it and presenting the

results of the analysis experimental in the fourth chapter to prove its effectiveness.

### **Analysis and Experimentation**

This chapter introduces the CBDS model in a hands-on way, The goal of this experiment is to address cloud big data security, cloud performance, and cloud management. First, this section explains the CBDS scenario with the workings of its components. Second, regarding cloud security, this section examines the CBDS model and compares the performance of the cloud for data storage before and after using the strategy Dynamic Data Encryption Strategy, and can also be used to compare data confidentiality, data integrity and service availability. Third, regarding cloud performance, this section summarizes the experience of our proposed new model. Experiment with studying the security, integrity and performance of the CBDS model and demonstrating data storage and retrieval procedures.

### **CBDS Scenario**

As described in the proposed model section (3.2 Suggested Model (CBDS)), our goal is to protect big data in the cloud and improve performance. Where the user enters the server after he proves that he is authorized with the password and the biometric methods and then enters the data to be stored in the cloud, it goes through a strategy to improve the performance of the cloud consisting of 3 steps managed by the cloud manager, and finally we store the data in the cloud after encrypting it with AES technology. Encryption is implemented to maintain the security and integrity of the data.

For queries, the authorized employee enters the server after proving that he is authorized to do so, applying the principle of least privilege to the employee, then sends the request in unencrypted form to be delivered by the cloud manager to the database in the cloud, uploads the request and passes it to the decryption algorithm and then delivers the data In unencrypted form to the employee. We argue that our CBDS model is more secure than the traditional model.

### **Data Security Analysis**

#### **Data security**

Data confidentiality is one of the security risks that big data can occur with cloud computing, for example, accessing and viewing user data without permission, whether a hacker or an employee.

The (CBDS) model depends on encrypting data in the cloud and also securing access to the server for the user using the password and Biometric technique. As for the employee, the system limits his access to the data and the data is in a state of encryption, to offer secure correspondence through the organization, encryption calculation assumes a significant part. It is an important and principal component for the assurance of information. Encryption calculation changes over the information into a mixed structure with the utilization of "a key" way to

decode the information. Concerning investigates that have been made, a significant encryption method is Symmetric key Encryption. algorithm encrypts the data blocks of 128 bits in 10, 12, and 14 rounds. Additionally, AES has been tested with attention for a huge number of security applications. AES algorithm considered better than others as we mentioned in the Literature Review (2.1.3 Big data security).

### **Data integrity**

Data integrity is a factor associated with the critical issues of data security threats in the cloud. Stored data can expose damage during transfers to or from a cloud storage provider, the risks of attack from within and outside of the cloud provider must be considered.

Therefore, the main approach to the data cannot be modified by any other users or intruders. As we explained before, AES was used for encryption. Moreover, the user can only login after entering the password and verifying his identity with the Biometric technique, as for maintaining data integrity on the part of the employee, the employee must apply the Principle of Least Privilege to it to limit the infringement of user data.

### **Service performance**

Server performance and data processing speed depend on the performance of the cloud. Cloud performance metrics take advantage of this by monitoring your cloud resources well, ensuring that all components are connected smoothly. Cloud performance metrics measure file system performance, often I/O operations per second, automatic scaling as well as caching.

In the CBDS model, we contributed to improving the performance of the server by applying the Dynamic Data Encryption Strategy, and we designed it in 4 steps, managed by the cloud manager, from receiving the data until saving it in the database in an encrypted.

The weight of the data is calculated and classified accordingly, to facilitate and speed up the encryption process, as we mentioned in (3.7 Dynamic Data Encryption Strategy) This strategy is known as one of the best strategies used to improve cloud computing performance and maintain information security , In this model, we have modified it to suit the requirements of the proposed system in order to increase performance and maintain data integrity and confidentiality, from the beginning of receiving the user data before entering it until it is saved in the database in the cloud and until it is recalled from the database.

### **Experiment and Evaluation**

We set up the experimental dependent on our research facility setting. We chose Advanced Encryption Standard (AES) as the encryption technique in our examinations. Then, cloud conditions were set up in our lab too. The equipment setup was processor (Intel(R) Core (TM) i7-750 CPU @8M Cache, 2.66 GHz), 16 GB actual memory. The cloud computing side was introduced on an Oracle VM

Virtual Box workstation with running an Ubuntu 16.4.04 LTS Server. Besides, we assessed our DDES model's exhibitions according to two points of view, which included both security assurance level and processing effectiveness. The exploratory settings were in accordance with these two perspectives, which comprised of a progression of settings for arriving at the normal assessment objectives. We recreated diverse responsibility sizes of the data transmission by designing measures of information bundles and the execution season of data encryption for every data packages. To assess the security insurance ability, we esteemed various data packages with various protection loads.

### Data storing procedure

Storing data in a CBDS model involves the delivery of data to cloud computing. Our model requires encryption before the data is stored. The difference between the traditional method and CBDS is at the time of data storage and the weight of the data before encryption. CBDS stages contribute to improving the performance of the cloud as it calculates and classifies the data before it reaches the cloud and contributes to ensuring the privacy and integrity of the employee's query through the data retrieval process. We perform experimentation to perform data storage in a CBDS model using an amount of input data. Figures 5, 6, and show the expected execution time of the CBDS model and the total time is taken for operations without using the DED algorithm. Figures 7 and 8 shows the comparison of data weights using the steps of CBDS and calculating the weights in the traditional way. In figures:5 big data go through the steps of CBDS model and store it in the cloud and we observe convergence in the results in all four rounds

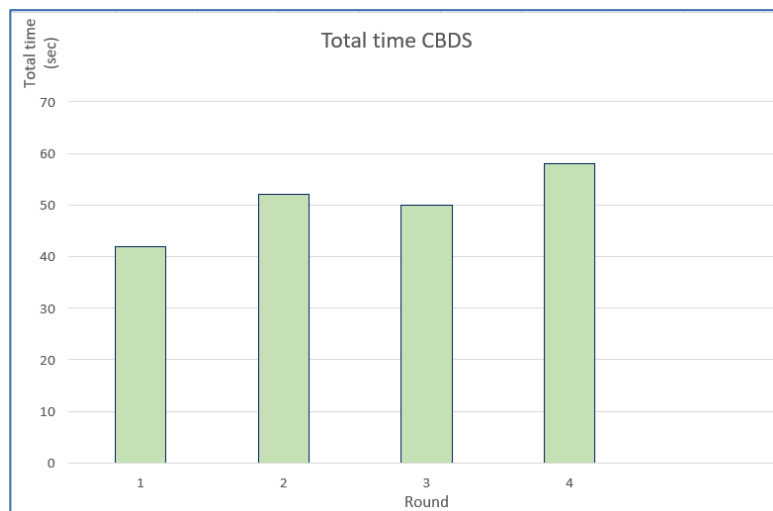


Figure: 5, Total time after applying CBDS

In figures 6 The Big Data goes through the traditional steps and then you store it in the cloud, The similarity in the results in all four rounds is also clear

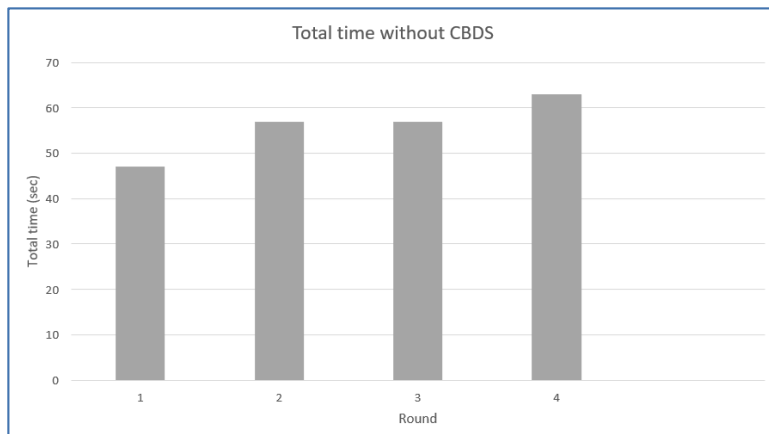


Figure: 6, Total time without applying CBDS

Figure: 7 In the case of measuring the weight of big data, we notice that the results are similar and nearly constant.

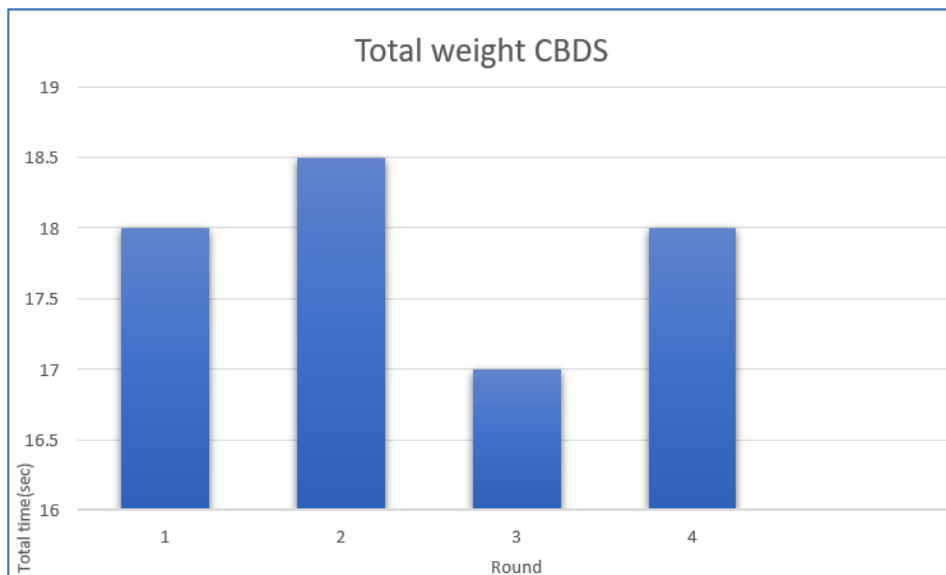


Figure: 7, Total weight after applying CBDS

Figure: 8 shows the Total weight of the data after passes through the first stages of the CBDS model, we notice a change in the size of the data before it is encrypted, and the drawing shown in all the four rounds gave clos.

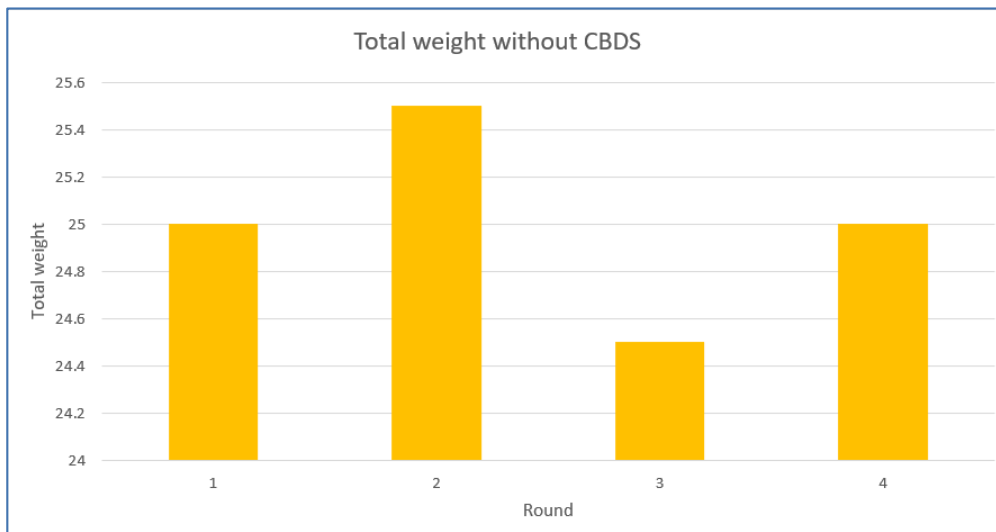


Figure: 8, Total weight without CBDS

We made a comprehensive comparison shown in the figure:9, in all the four rounds the apparent result says that the direct relationship that accompanies the sum of time when the weight of the data decreases.

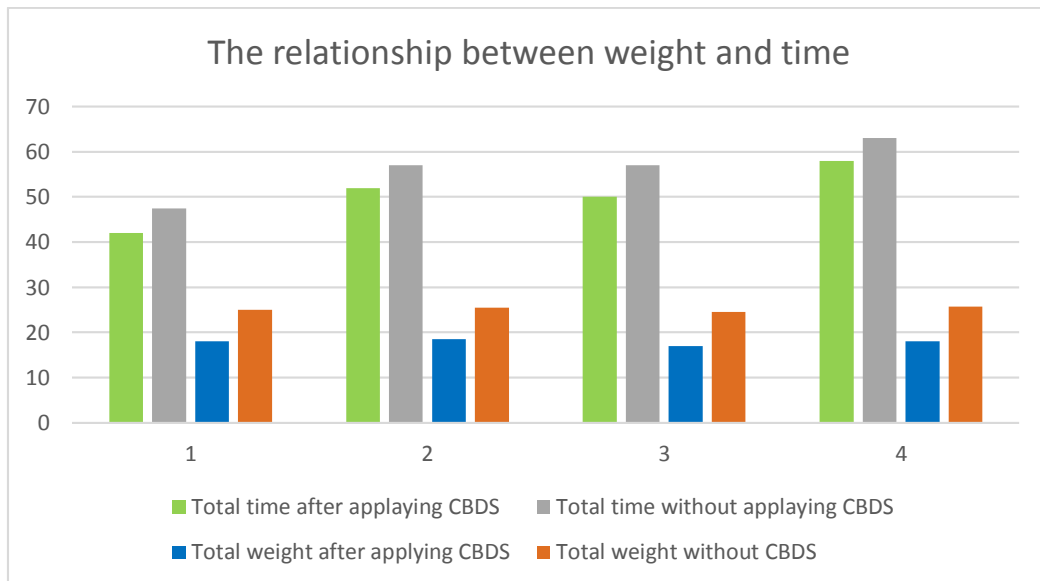


Figure: 9, Comparison of total time and total weight

Figure: 10 shows the clear time discrepancy between the traditional method and our model in the performance of the system when dealing with big data, encrypting, and storing it in the database.

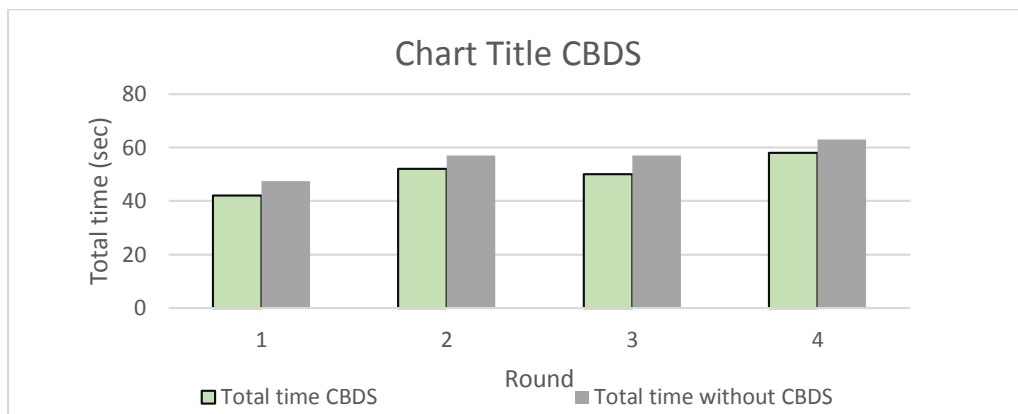


Figure 10, Total time of the traditional method and CBDS model

Figure: 11 shows the clear disparity in the weight of the data between the traditional method and our model in the performance of the system when dealing with big data, as it was classified according to its weight using the steps of the Dynamic Data Encryption Strategy which contributed to accelerating the encryption process before storing it in the database and thus significantly improving the performance of the cloud

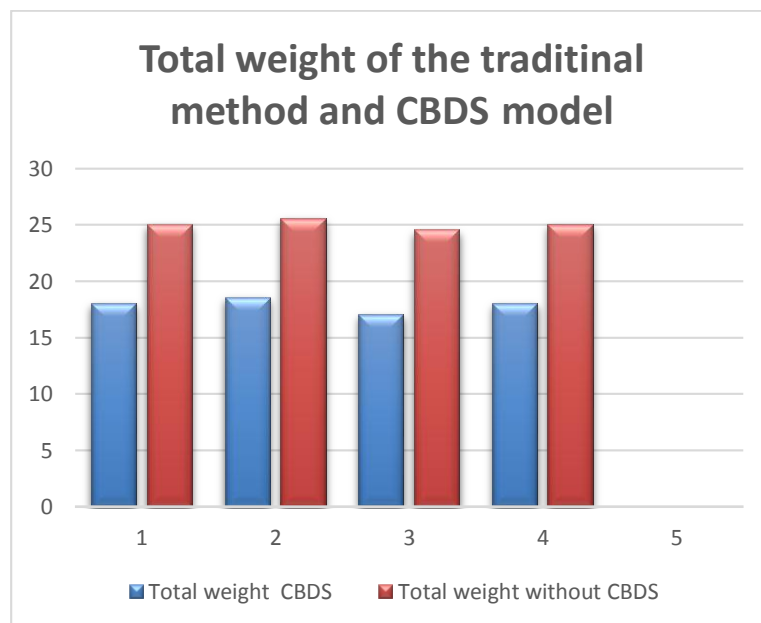


Figure:11, Total weight of the traditional method and CBDS mode

## Conclusion

Cloud computing offers incredible potential to further develop usefulness, decrease expenses, and store BD. As users and large companies enjoy the services and benefits of cloud computing, keeping big data secure in the cloud is a major challenge. Since there are numerous security vulnerabilities in the cloud



computing system that numerous may overlook, hackers continue to exploit these vulnerabilities. The thing of this exploration is a proposed new model, which is the CBDS model, which uses the AES encryption algorithm. Also, the cloud performance is improved before the encryption process by applying the Dynamic Data Encryption Strategy. Also, the bandied armature and factors of the CBDS model are examined. The thing of the CBDS model is to reduce the security pitfalls that do in cloud computing and ameliorate its performance during the processing of big data.

At this point, we've compared our performance features in our proposed model with traditional data storehouse styles like the traditional authentication cloud model. And some trials to store big data. Incoming work, we plan and suggest comparing our proposed model with other models, systems, and cryptographic algorithms to foster our evaluation so that we can grow more and develop our model. Thus, we will give sweats to screen big data security dangers in the cloud and countermeasures for cloud security breaks.

## References

- [1] SCLPV: Secure Certificateless Public Verification for Cloud-Based Cyber-Physical-Social Systems Against Malicious Auditors Yuan Zhang, Student Member, IEEE, Chunxiang Xu, Member, IEEE, Shui Yu, Senior Member, IEEE, Hongwei Li, Member, IEEE, and Xiaojun Zhang.
- [2] Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing Environment Sumit Vikram Tripathi<sup>1</sup>, Ritukar<sup>2</sup>, Prof. Murthy B<sup>3</sup>, Dr. K. S. Jagadeesh Gowda<sup>4</sup>.
- [3] Intelligent cryptography approach for secure distributed big data storage in cloud computing Yibin Lia, Keke Gaib,<sup>\*</sup>, Longfei Qiuc, Meikang Qiub,<sup>1</sup>, Hui Zhaod a School of Computer Science and Technology, Shandong University, China b Department of Computer Science, Pace University, New York City, NY 10038, USA c Nanjing Foreign Language School, Jiangsu, China d Software School, Henan University, Kaifeng, Henan, 475000, China
- [4] C. Mulliner, W. Robertson, and E. Kirda. Hidden GEMs: Automated discovery of access control vulnerabilities in graphical user interfaces. In IEEE Symposium on Security and Privacy, pages 149–162, San Jose, CA, USA, 2014. IEEE.
- [5] S. Sen, S. Guha, A. Datta, S. Rajamani, J. Tsai, and J. Wing. Bootstrapping privacy compliance in big data systems. In IEEE Symposium on Security and Privacy, pages 327–342, San Jose, CA, USA, 2014. IEEE.
- [6] Protection of Big Data Privacy ABID MEHMOOD<sup>1</sup>, IYNKARAN NATGUNANATHAN<sup>1</sup>, YONG XIANG<sup>1</sup>, GUANG HUA<sup>2</sup>, AND SONG GUO<sup>3</sup>. <sup>1</sup>School of Information Technology, Deakin University, Victoria 3125, Australia <sup>2</sup>School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798 <sup>3</sup>Department of Computer Science and Engineering, The University of Aizu, Fukushima 965-8580, Japan.
- [7] T Singh, B Kaur, GS Gaba, M Masud, M Baz, A Metaheuristic Approach to Secure Multimedia Big Data for IoT-Based Smart City Applications HS Gill, Wireless Communications and Mobile Computing 2021

- [8] P Singh, M Masud, MS Hossain, A Kaur, Cross-domain secure data sharing using blockchain for industrial IoT, *Journal of Parallel and Distributed Computing* 156, 176-184
- [9] M Masud, GS Gaba, K Choudhary, R Alroobaea, MS Hossain, A robust and lightweight secure access scheme for cloud based E-healthcare services, *Peer-to-peer Networking and Applications* 14 (5), 3043-3057
- [10] MI Khalil, NZ Jhanjhi, M Humayun, SK Sivanesan, M Masud, MS Hossain, Hybrid smart grid with sustainable energy efficient resources for smart cities, *Sustainable Energy Technologies and Assessments* 46, 101211
- [11] P Singh, M Masud, MS Hossain, A Kaur, Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid, *Computers & Electrical Engineering* 93, 107209
- [12] M Masud, M Alazab, K Choudhary, GS Gaba, 3P-SAKE: privacy-preserving and physically secured authenticated key establishment protocol for wireless industrial networks, *Computer Communications* 175, 82-90
- [13] FR Khan, M Muhabullah, R Islam, M Monirujjaman Khan, M Masud, A Cost-Efficient Autonomous Air Defense System for National Security, *Security and Communication Networks* 2021
- [14] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun and N. Jhanjhi, "Secure Healthcare Data Aggregation and Transmission in IoT—A Survey," in *IEEE Access*, vol. 9, pp. 16849-16865, 2021, doi: 10.1109/ACCESS.2021.3052850.
- [15] M. Humayun, N. Jhanjhi, M. Alruwaili, S. S. Amalathas, V. Balasubramanian and B. Selvaraj, "Privacy Protection and Energy Optimization for 5G-Aided Industrial Internet of Things," in *IEEE Access*, vol. 8, pp. 183665-183677, 2020, doi: 10.1109/ACCESS.2020.3028764.
- [16] Khan, N. A., Brohi, S. N., & Jhanjhi, N. Z. (2020). UAV's applications, architecture, security issues and attack scenarios: a survey. In *Intelligent computing and innovation on data science* (pp. 753-760). Springer, Singapore.
- [17] N. A. Khan, N. Z. Jhanjhi, S. N. Brohi, A. A. Almazroi and A. A. Almazroi, "A secure communication protocol for unmanned aerial vehicles," *Computers, Materials & Continua*, vol. 70, no.1, pp. 601-618, 2022.
- [18] M. Satheesh Kumar, S. Vimal, N.Z. Jhanjhi, Shanmuga Sundar Dhanabalan, Hesham A. Alhumyani, Blockchain based peer to peer communication in autonomous drone operation, *Energy Reports*, Volume 7, 2021, Pages 7925-7939, ISSN 2352-4847, <https://doi.org/10.1016/j.egyr.2021.08.073>.
- [19] S. Saeed, N. Z. Jhanjhi, M. Naqvi, M. Humayun and S. Ahmed, "Ransomware: A Framework for Security Challenges in Internet of Things," 2020 2nd International Conference on Computer and Information Sciences (ICCIS), 2020, pp. 1-6, doi: 10.1109/ICCIS49240.2020.9257660.
- [20] N. A. Khan, N. Z. Jhanjhi, S. N. Brohi, A. A. Almazroi and A. A. Almazroi, "A secure communication protocol for unmanned aerial vehicles," *Computers, Materials & Continua*, vol. 70, no.1, pp. 601-618, 2022.
- [21] M. Satheesh Kumar, S. Vimal, N.Z. Jhanjhi, Shanmuga Sundar Dhanabalan, Hesham A. Alhumyani, Blockchain based peer to peer communication in autonomous drone operation, *Energy Reports*, Volume 7, 2021, Pages 7925-7939, ISSN 2352-4847, <https://doi.org/10.1016/j.egyr.2021.08.073>.

- [22] S. Saeed, N. Z. Jhanjhi, M. Naqvi, M. Humayun and S. Ahmed, "Ransomware: A Framework for Security Challenges in Internet of Things," 2020 2nd International Conference on Computer and Information Sciences (ICCIS), 2020, pp. 1-6, doi: 10.1109/ICCIS49240.2020.9257660.