Implementation of a Security System in IaaS Cloud Server through an Encrypted Blockchain

B. Vivekanandam[1], Midhunchakkaravarthy[2]

[1,2]Associate Professor, Faculty of computer science and Multimedia, Lincoln University College, Malaysia

E-mail: [1]vivekresearch2014@gmail.com, [2]midhun.research@gmail.com

Abstract

Infrastructure as a Service (IaaS) is a kind of cloud sharing service allocated to different category of application at the same time. The shared cloud services are provided through internet for computing, networking, and data storage applications. The utilization of IaaS reduces the maintenance and installation cost of physical hardware modules at the base station. The cloud service providers configure their available cloud components with respect to the suitability of the user requirements. The security protocol available in the IaaS servers are usually better than the traditional local servers. However, the IaaS servers are also open to attacks when the modules encounter misconfiguration and vulnerabilities. The work enforces an encrypted blockchain model for enhancing the quality of service in the IaaS systems on handling image data.

Keywords: Cloud server, server security, data encryption, cloud blockchain, data computing, serverless storage

1. Introduction

Cloud server provides a virtual infrastructure to the base station where the physical storage area is insufficient to handle the observed data. The Internet of Things (IoT) application is a good example for a system employed with cloud server. In most cases, the IoT devices are connected to a light-weight microcontroller device for handling the sensor connections. Therefore, there is no additional memory storage unit available in such cases rather than the small memory space present inside the microcontroller [1]. The recent year microcontroller

DOI: https://doi.org/10.36548/jscp.2021.4.008

Received: 07.12.2021, received in revised form: 02.01.2022, accepted: 13.01.2022, published: 24.01.2022

units are constructed with an IoT shield for transferring the observed data to the base station from its source point. However, the base station modules available in the IoT systems have the ability to project the observed/processed data as a display device [2].

Cloud computing is the architecture of processing the collected information from a remote sensor unit. The algorithm which is made for the computing process is installed over the cloud server with a reliable firewall unit for securing the information [3]. The collected data are processed virtually in the cloud server with respect to the algorithmic flow instructed by a user. This reduces the memory and computational space requirement at the base station. The IaaS is a shared cloud infrastructure, where the available space is split into different sections for enabling multiple users to use the same module [4]. Figure 1 denotes the features of a generalized cloud server.

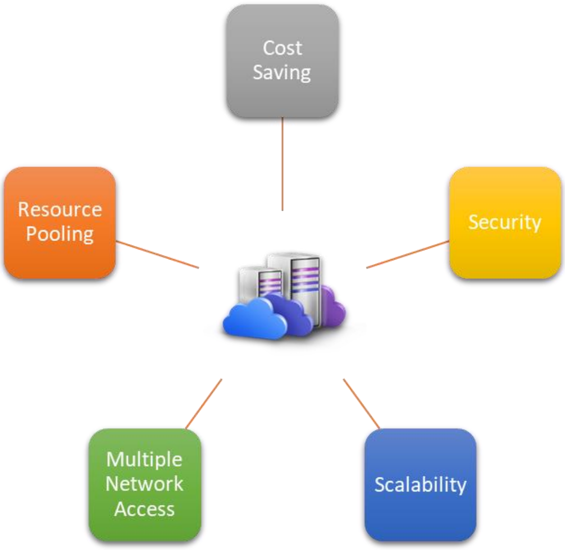

Figure 1. Features of a cloud server

The cloud servers are scalable in nature which allows the user to improve and reduce the size allocated for their computational process in the shared server. This reduces the limitations while enhancing the business model to next level. The multiple network access feature lets the cloud server to be processed from different locations in the world. In certain applications, the cloud servers are connected to space stations for enabling reliable and fast processing of data. The resource pooling feature improves the data sharing process, up to a certain extent by retaining few important source file information at the base station unit [5, 6].

Such important data are allowed to be accessed by the cloud server only at necessary conditions.

Misconfiguration of cloud firewall module is a primary cause of security failure in the cloud server. This extends the data stored in the cloud server to be shared with known or unknown sources and in some cases, it allows the unauthorized users to access the precious information available in the memory unit [7]. Account hijack is yet a common issue in utilizing the cloud server with weak and shared password on systems. Additionally, the user lacks visibility of particular data due to the misconfiguration of cloud server. All such issues are tackled in recent days by implementing focused cloud security tool that reduces the denial-of-service attacks and data loss [8].

In recent applications, the data to be stored in the cloud server are encrypted from original data to save their valuable information at the time of data leakage, since the attackers decrypt the data when the algorithm is not secure enough [9]. The blockchain based models are enforced in recent days to overcome the limitations of the encryption models. The blockchain model generates a ledger and maintains the information which are to be kept secure in the cloud platform. This allows the important data to be stored at multiple places in the cloud server as different pieces of data [10]. The following section explores the limitations and achievements of the recent year algorithms on cloud data securing process.

2. Literature Review

The privacy issues involved in the cloud environment was addressed with a genetic algorithm model [11]. The algorithm created separate keys for encrypting the data to be stored in the cloud architecture. The combination of cryptographic algorithm employed with the genetic algorithm produced a better throughput and execution time. The experimental analysis explored betterment over the DES, AES and Blowfish algorithm. A medical data cloud application was employed with a blockchain network for ensuring its privacy [12]. The image data information was encrypted in the work before keeping it over the blockchain module. The developed model avoided the keyword guessing attack in an efficient way over the existing approaches. A biological concept-based encryption algorithm was employed to the cloud network as DNA computing technique [13]. A secret key of 1024 bit was prepared with the DNA computing algorithm along with a media access control and given attributes.

A public key encryption model based on keyword search and ciphertext policy was developed to overcome the issues of the attribute-based encryption models [14]. A secure proxy decryption model was also included in the work at the destination module for reducing the energy consumptions. A secured data sharing architecture was designed with a cloud edge-based approach [15] to analyze the cyber threat data available in the networks. The developed approach was incorporated with a multi-level of operation that can be controlled by the user based on his needs. A blockchain based framework was proposed to address the third-party access on smart vehicles [16]. This ensured an authentic communication between the users of smart vehicles.

A blockchain based integrity protection approach was framed to make a reliable cloud computing module [17]. The approach was enforced with a virtual machine agent which allows multiple user to access the data at a same time in an efficient way. The secure communication was ensured by creating a separate hash value for each user data access. The blockchain system was also included in the IoT systems for securing its data communication [18]. A spatial domain poison distribution model was utilized in the work for estimating the transaction rate of the connected nodes. An edge-based auditing technique was structured to provide a secure communication at IoT models [19]. The computational load in the edge auditing process was minimized at the preprocessing stage by having a correlation approach with binary tree.

An IoT based big data computing approach was developed by incorporating the artificial intelligence algorithms along with a blockchain network [20]. The intelligent algorithm employed in the work classified the data to be accessed and operated by the blockchain network. The experimental analysis indicated a better accuracy and latency rate on the techniques employed with blockchain setup. A decentralized security model was included in the blockchain setup for enabling data security in the IoT communications [21]. An unspent transaction output verification algorithm was employed in the work in combination with RSA accumulator for reducing the computational cost at the light nodes. A multi keyword fuzzy search model was developed for encrypting the data on cloud computing [22]. This was achieved by generating an index and query vectors through bloom filters and locality sensitive hashing function. The generated vectors were balanced with a binary tree set and the data search was triggered with a top k-search algorithm.

A steganography approach was employed in a cloud environment for ensuring a secure transmission on image data [23]. The steganography algorithm was merged with a quantum algorithm to make a universal computation system. A multi-model biometric authentication system was designed to generate feature fusions on cloud environment for providing a satisfied security environment [24]. The feature points collected from the iris, palm and finger points were fused in the work for analysis. The images which are to be utilized in the cloud network for authentication process were preprocessed in the work before extracting its features. Therefore, the key generated in the approach was more secure and replicated the information gathered from the biometric data. The convergent encryption algorithms were widely employed in the deduplication of data in blockchain [25]. However, the traditional convergent encryption models were utilizing a third-party verifiers for ensuring the data integrity. Implementation of third-party verifier system was avoided in the convergent model to stop making changes in the blockchain hashes by having a tamper proofing ledger.

The literature work finding indicates that the blockchain models are very efficient in proving a secure environment in the cloud spaces. Similarly, the finding also shows a slight improvement in the securing process when the blockchain model is merged with an encryption or artificial intelligence technique.

3. Methodologies

3.1 Cryptographic Algorithm

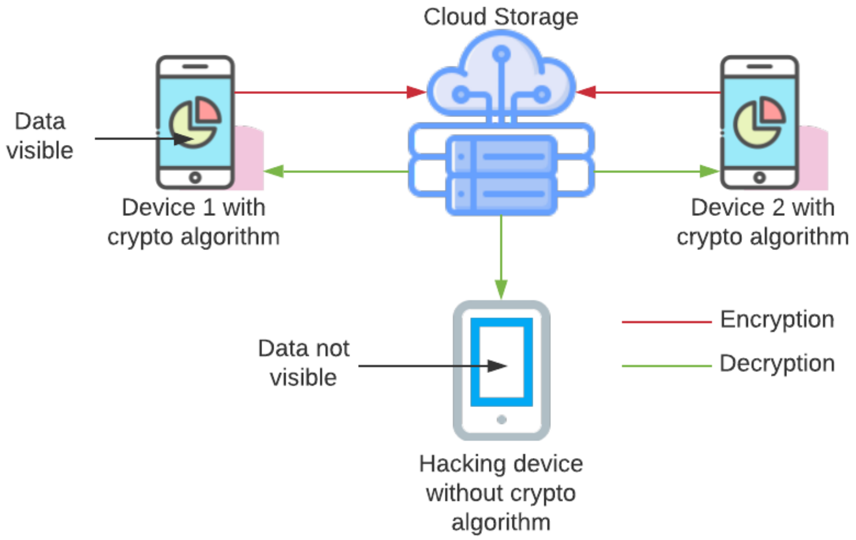
Cloud Storage
Data visible
Device 1 with crypto algorithm
Device 2 with crypto algorithm
Data not visible
Encryption
Decryption
Hacking device without crypto algorithm

Figure 2. Architecture of the cryptographic cloud storage

The traditional cryptographic algorithms perform at their source place. The information which needs to be stored in the cloud surfaces are encrypted with the algorithm stored in the device. The cloud storage receives the encrypted information from the transmitting devices. This provides the users to install their own kind of cryptographic algorithms. Therefore, the attackers will not be able to steal or read all the data available in the cloud environment. The architecture model of cryptographic technique is shown in Figure 2, where an attacker without the appropriate decryption algorithm attempts to download information from the cloud storage. However, this technique prohibits the attacker from viewing the precious information stored in the cloud space. The hacking of information from the cloud environment is possible when the cloud module is configured with wrong data or attributes. Therefore, in such cases the attacker may crash the cloud system through a distributed DoS (Denial of Service) attack, which makes the cloud system busy and inoperable for the actual users.

3.2 Blockchain Model

The blockchain systems are developed to secure the cloud space with an encryption model. The encryption model receives the files to be stored in the cloud environment without any encryption procedure. An individual key is generated randomly in such cases, for creating a mathematical function of the received file data and its location. A hash value is generated with respect to the mathematical calculation and it represents the place where the file will be stored in the cloud space. From this, a new block is created in the cloud space for storing the location of the file in the network with an encrypted index. Figure 3 represents the architecture of the blockchain network.

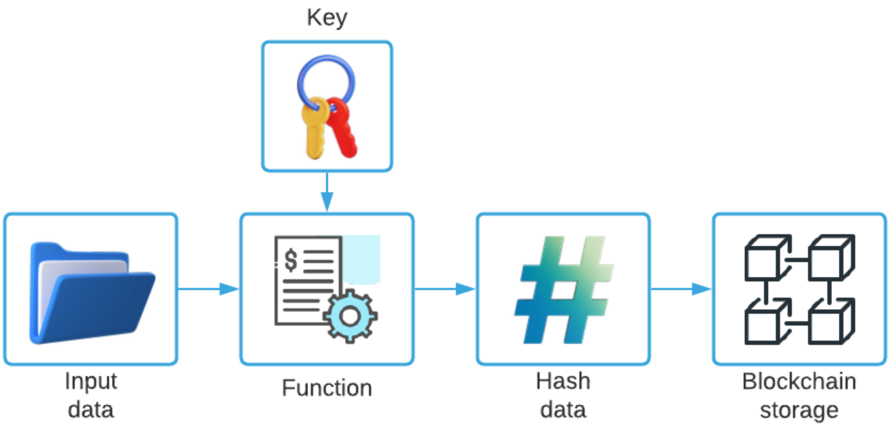

Figure 3. Architecture of the Blockchain model

The encryption of data location in the cloud environment does not let the hackers reach the specific location in the cloud. This improves the reliability of the cloud environment to a certain extent. However, the computational speed of the blockchain network is comparatively slower than the regular encryption model. Therefore, it requires more energy for its operation. Moreover, blockchain is a decentralized network that produces individual keys for all the users separately. Hence the user responsibility also plays a major role in the blockchain security.

3.3 Proposed Method

The motive of the proposed work is to address the limitations of the cryptographic and the traditional blockchain models. Figure 4 explores the workflow of the proposed model. Here the cryptographic model is combined with the block system for improving its safety and security. The proposed model is designed for the image securing process in cloud network, where the input data are enclosed with a cover image.

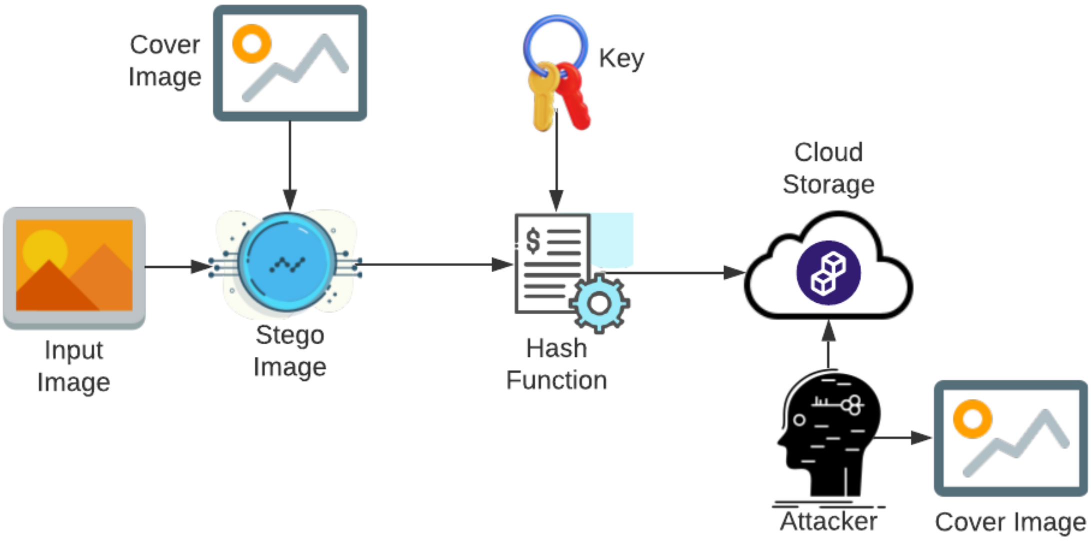

Figure 4. Architecture of the proposed method

The generated stego image is forwarded to the blockchain network, where an individual key is given to the user data for making a hash function. The hash function generated for the respective image is stored in the blocks generated in the cloud storage. The proposed work is comparatively stronger than the traditional encryption and blockchain models. If a blockchain fails due to misconfiguration or any other technical flaw, the attacker may get the key access to download the hash information from the cloud environment. However, the data downloaded from a cryptographic key can read only the cover image data. The computational speed and energy drawbacks available in the blockchain models are verified in the work by implementing different kinds of steganography and hash function models.

4. Experimental Work

The performance of the proposed work is verified with a chest Xray dataset [26] that is covered with a breast cancer dataset [27] downloaded from kaggle.com. The Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) are employed in the work for a comparative analysis. The LSB technique is a spatial domain technique with reduced computational complexity. The LSB technique is an independent model which is suitable for all kind of images in different formats and textures. Similarly, DCT is one of the simplest transform domain algorithms that has less computational parameters for the steganography process. The detectability of DCT is found to be comparatively better than the LSB.

The performance of the steganography process of LSB and DCT are shown in Table 1 and 2 on PSNR (Peak Signal to Noise Ratio), SSIM (Structural Similarity Index Metric), NCC (Normalized Cross Correlation) and UIQ (Universal Image Quality).

Table 1. Performance of the LSB technique

Image Count	PSNR	SSIM	NCC	UIQ
1	45.2312	0.9456	0.9997	0.8314
2	44.8546	0.9412	0.9945	0.8345
3	45.6325	0.9458	0.9994	0.8432
4	45.9845	0.9384	0.9978	0.8425
5	44.2351	0.9421	0.9998	0.8397
6	44.9321	0.9489	0.9987	0.8298
7	45.8794	0.9501	0.9993	0.8461
8	45.1239	0.9378	0.9991	0.8432
9	44.5872	0.9495	0.9975	0.8512
10	45.4981	0.9412	0.9993	0.8497

Table 2. Performance of the DCT technique

Image Count	PSNR	SSIM	NCC	UIQ
1	47.2498	0.9912	0.9912	0.9065
2	46.1274	0.9951	0.9997	0.9047
3	46.0197	0.9945	0.9995	0.9089
4	46.9846	0.9978	0.9998	0.9124
5	46.3458	0.9967	0.9959	0.9045
6	47.1497	0.9971	0.9946	0.9012
7	47.5479	0.9969	0.9995	0.9197
8	46.2564	0.9948	0.9996	0.9136
9	46.8714	0.9927	0.9963	0.9078
10	47.1148	0.9983	0.9941	0.9146

Figure 5 and 6 indicate the encryption and decryption time of the verified models for 10 images on cloud systems with and without blockchain. The experimental work performed with DCT shows a better PSNR value when compared to the LSB technique. Similarly, the NCC value of DCT has a huge difference from that of the LSB technique. Furthermore, the UIQ and SSIM also shows a better improvement when the images are encrypted with DCT algorithm.

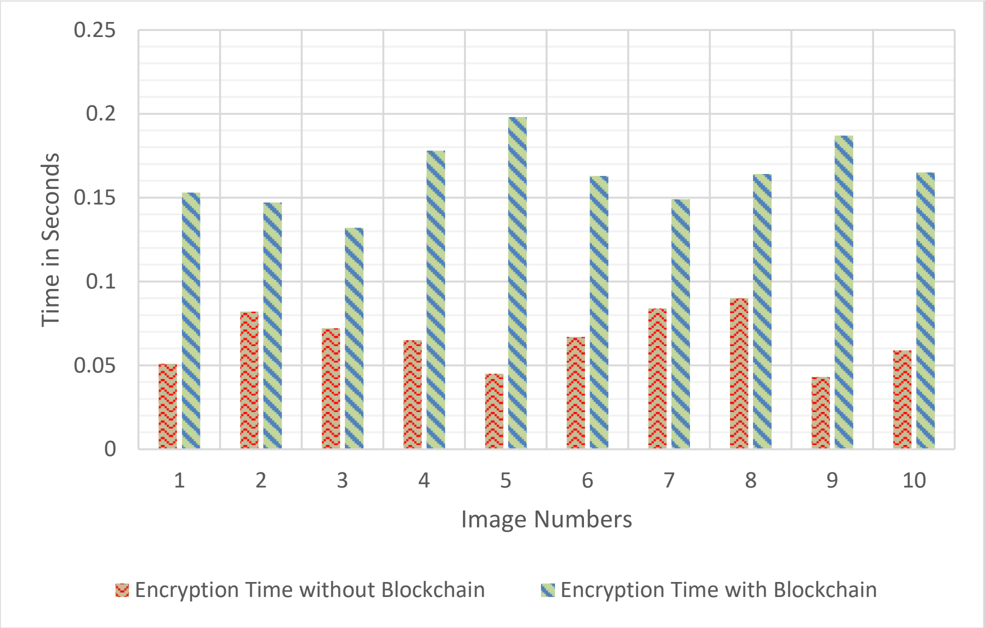

Figure 5. Comparison of encryption time with and without blockchain model

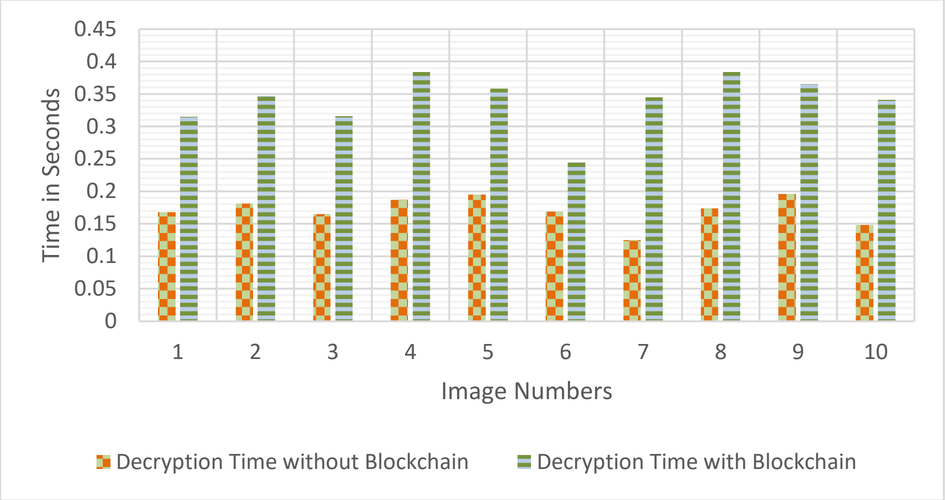

Figure 6. Comparison of decryption time with and without blockchain model

The encryption and decryption time taken on storing data in cloud environment with and without blockchain model are analyzed. The model without blockchain network has an average time of encryption as 0.0658 seconds per image and decryption time as 0.1708 seconds per image. The average encryption and decryption time with blockchain network are 0.1636 and 0.34 seconds respectively.

5. Conclusion

IaaS is a shared model of cloud space among different clients. Data security is one of the primary concerns in such architectures. Misconfiguration of cloud algorithm may authorize accessing other client's data for certain minutes. Therefore, the traditional algorithmic models facilitated the clients to encrypt their data. Similarly, the cloud environment providers also came up with a blockchain solution of providing individual key generated on hash algorithm to their clients. The proposed work suggests an encrypted blockchain model for ensuring the safety during blockchain crack or hacking process. The performance of the proposed model is verified with a LSB and DCT steganography algorithm on health care image data and found satisfied with the DCT algorithm. The computational time difference of the suggested steganography model is also verified on cloud environment with and without blockchain and found a time difference of 0.0978 seconds in average for an image to be encrypted. Likewise, a time of 0.1692 seconds difference is observed on decryption process. However, this time difference is acceptable when a client requires a reliable security system.

References

[1] Manoharan, J. Samuel. "A Novel User Layer Cloud Security Model based on Chaotic Arnold Transformation using Fingerprint Biometric Traits." Journal of Innovative Image Processing (JIIP) 3, no. 01 (2021): 36-51.

[2] Pimple, Kshitij U., and Nilima M. Dongre. "Biometric Authentication in Cloud." In International Conference on Intelligent Data Communication Technologies and Internet of Things, pp. 245-254. Springer, Cham, 2019.

[3] Kumar, Dinesh, and Dr S. Smys. "Enhancing Security Mechanisms for Healthcare Informatics Using Ubiquitous Cloud." Journal of Ubiquitous Computing and Communication Technologies 2, no. 1: 19-28.

[4] Reddy, Midde Ranjit, D. Raghava Raju, and T. Venkata Naga Jayudu. "Improved Scheduling Algorithm for Load Balancing in Cloud Computing." In Computer Networks and Inventive Communication Technologies, pp. 793-800. Springer, Singapore, 2021.

[5] Andi, Hari Krishnan. "Analysis of Serverless Computing Techniques in Cloud Software Framework." Journal of IoT in Social, Mobile, Analytics, and Cloud 3, no. 3 (2021): 221-234.

[6] Mishra, Piyush, Shubham Bhatnagar, and Avita Katal. "Cloud Container Placement Policies: A Study and Comparison." In International Conference on Computer Networks and Inventive Communication Technologies, pp. 513-524. Springer, Cham, 2019.

[7] Fathima, KM Majidha. "A Survey of the Exemplary Practices in Network Operations and Management." In *Data Intelligence and Cognitive Informatics*, pp. 181-194. Springer, Singapore, 2021.

[8] Sivaganesan, D. "Performance Estimation of Sustainable Smart Farming with Blockchain Technology." IRO Journal on Sustainable Wireless Systems 3, no. 2 (2021): 97-106.

[9] Rajathi, N., and Meghna Praveen. "Practical Implementation and Analysis of TLS Client Certificate Authentication." In *Proceedings of International Conference on Intelligent Computing, Information and Control Systems*, pp. 695-703. Springer, Singapore, 2021.

[10] Tahir, Muhammad, Muhammad Sardaraz, Zahid Mehmood, and Shakoor Muhammad. "CryptoGA: a cryptosystem based on genetic algorithm for cloud data security." *Cluster Computing* 24, no. 2 (2021): 739-752.

[11] Shakya, Subarana. "An efficient security framework for data migration in a cloud computing environment." Journal of Artificial Intelligence 1, no. 01 (2019): 45-53.

[12] Joe, C. Vijesh, and Jennifer S. Raj. "Deniable Authentication Encryption for Privacy Protection using Blockchain." Journal of Artificial Intelligence and Capsule Networks 3, no. 3 (2021): 259-271.

[13] Namasudra, Suyel, Debashree Devi, Seifedine Kadry, Revathi Sundarasekar, and A. Shanthini. "Towards DNA based data security in the cloud computing environment." *Computer Communications* 151 (2020): 539-547.

[14] Raj, Jennifer S. "Secure Data Sharing Platform for Portable Social Networks with Power Saving Operation." Journal of IoT in Social, Mobile, Analytics, and Cloud 3, no. 3 (2021): 250-262.

[15] Chadwick, David W., Wenjun Fan, Gianpiero Costantino, Rogério De Lemos, Francesco Di Cerbo, Ian Herwono, Mirko Manea, Paolo Mori, Ali Sajjad, and Xiao-Si Wang. "A cloud-edge based data security architecture for sharing and analysing cyber threat information." *Future Generation Computer Systems* 102 (2020): 710-722.

[16] Smys, S., and Haoxiang Wang. "Security Enhancement in Smart Vehicle Using Blockchain-based Architectural Framework." Journal of Artificial Intelligence 3, no. 02 (2021): 90-100.

[17] Wei, PengCheng, Dahu Wang, Yu Zhao, Sumarga Kumar Sah Tyagi, and Neeraj Kumar. "Blockchain data-based cloud data integrity protection mechanism." *Future Generation Computer Systems* 102 (2020): 902-911.

[18] Kamel, D. K. "Wireless IoT with blockchain-enabled technology amidst attacks." IRO Journal on Sustainable Wireless Systems 2, no. 3 (2021): 133-137.

[19] Wang, Tian, Yaxin Mei, Xuxun Liu, Jin Wang, Hong-Ning Dai, and Zhijian Wang. "Edge-based auditing method for data security in resource-constrained internet of things." *Journal of Systems Architecture* 114 (2021): 101971.

[20] Sivaganesan, D. "A Hybrid Architecture combining Artificial intelligence and Blockchain for IoT Applications." *IRO Journal on Sustainable Wireless Systems* 2, no. 3 (2021): 138-142.

[21] Ge, Chunpeng, Zhe Liu, and Liming Fang. "A blockchain based decentralized data security mechanism for the Internet of Things." *Journal of Parallel and Distributed Computing* 141 (2020): 1-9.

[22] Zhong, Hong, Zhanfei Li, Jie Cui, Yue Sun, and Lu Liu. "Efficient dynamic multi-keyword fuzzy search over encrypted cloud data." *Journal of Network and Computer Applications* 149 (2020): 102469.

[23] Abd El-Latif, Ahmed A., Bassem Abd-El-Atty, Sherif Elseuofi, Hany S. Khalifa, Ahmed S. Alghamdi, Kemal Polat, and Mohamed Amin. "Secret images transfer in cloud system based on investigating quantum walks in steganography approaches." *Physica A: Statistical Mechanics and its Applications* 541 (2020): 123687.

[24] Joseph, Teena, S. A. Kalaiselvan, S. U. Aswathy, R. Radhakrishnan, and A. R. Shamna. "A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment." *Journal of Ambient Intelligence and Humanized Computing* 12, no. 6 (2021): 6141-6149.

[25] Zhang, Guipeng, Zhenguo Yang, Haoran Xie, and Wenyin Liu. "A secure authorized deduplication scheme for cloud data based on blockchain." *Information Processing & Management* 58, no. 3 (2021): 102510.

[26] Mooney, Paul. “Chest X-Ray Images (Pneumonia).” Kaggle,. https://www.kaggle.com/paultimothymooney/chest-xray-pneumonia.

[27] *Breast Cancer Wisconsin (Diagnostic) Data Set*. (2016, September 25). Kaggle. https://www.kaggle.com /uciml/breast-cancer-wisconsin-data.

Author's biography

B. Vivekanadam is an Associate Professor in the Department of Computer Science and Multimedia at Lincoln University College in Malaysia. His major area of research are machine learning, neural network algorithms, image processing, video and signal processing, cloud computing, deep learning, artificial intelligence, object recognition, complex feature extraction and vision graphics.

Midhunchakkaravarthy is currently an Associate Professor from the Department of Computer Science and Multimedia at Lincoln University College in Malaysia. His area of research includes machine learning, big data, bockchain network, artifical intelligence in automation and computation in cloud systems.