Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.03
Pages: 259-271
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.3.008

Deniable Authentication Encryption for Privacy Protection using Blockchain

C. Vijesh Joe[1], Jennifer S. Raj[2]

[1]Assistant Professor, Department of Computer Science and Engineering, VV College of Engineering, Tirunelveli, India

[2]Professor, Department of ECE, Gnanamani College of Technology, Namakkal, India

E-mail: [1]vijesh.joe@gmail.com, [2]jennifer.raj@gmail.com

Abstract

Cloud applications that work on medical data using blockchain is used by managers and doctors in order to get the image data that is shared between various healthcare institutions. To ensure workability and privacy of the image data, it is important to verify the authenticity of the data, retrieve cypher data and encrypt plain image data. An effective methodology to encrypt the data is the use of a public key authenticated encryption methodology which ensures workability and privacy of the data. But, there are a number of such methodologies available that have been formulated previously. However, the drawback with those methodologies is their inadequacy in protecting the privacy of the data. In order to overcome these disadvantages, we propose a searchable encryption algorithm that can be used for sharing blockchain- based medical image data. This methodology provides traceability, unforgettable and non-tampered image data using blockhain technology, overcoming the drawbacks of blockchain such as computing power and storage. The proposed work will also sustain keyword guessing attacks apart from verification of authenticity and privacy protection of the image data. Taking these factors into consideration, it is determine that there is much work involved in providing stronger security and protecting privacy of data senders. The proposed methodology also meets the requirement of indistinguishability of trapdoor and ciphertext. The highlights of the proposed work are its capability in improving the performance of the system in terms of security and privacy protection.

ISSN: 2582-2012 (online)
Submitted: 11.07.2021
Revised: 14.08.2021
Accepted: 25.08.2021
Published: 03.09.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.03
Pages: 259-271
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.3.008

Keywords: Medical Imaging, Searchable encryption, privacy of identity, Deniable authentication encryption, Blockchain

1. Introduction

Treatment for patients who are suffering from a particular disease or infection is given by the doctors based on medical image data sharing [1]. Taking this into consideration, one of the most crucial component modules of medical is the medical image data that gives a better view of the image. Hence searching for this medical image is the vital part of smart medical. It will be easier for the doctors and physicians to search for specific medical image data relevant to the disease or condition associated with the symptoms shown by the patient [2]. However, there is also need for privacy protection to secure the image data. Hence it is important that dependability and authenticity of data is properly explained to the users, without enclosing data on the original medical image. In general, content based image retrieval methodology is used to extract details on semantic features, spatial relationship, shape, texture [3] and colour [4] of the image. According to these parameters, a similar data is searched from the database to identify the actual image. However, it is also necessary to encrypt the sensitive data before outsourcing it. The drawback however is that the use of ciphertext embedded with the image will decrease the efficiency of operation of the system [5].

To address this issue, the authors in [6] proposed a searchable encryption (SE). This methodology uses a symmetric cryptography environment. In [7], the authors have used a mechanism of key distribution which makes it easier to use public keys in the work. However, it results in poor security and low efficiency. This methodology is vulnerable to keyword guessing attack (KGA) as observed by authors in [8]. Therefore, further methodologies to improve the resistivity to these attacks were developed [9]. A novel scheme that describes the encrypted image is present by the authors in [10]. To overcome the drawbacks of the query mechanism, the authors in [11] introduced a query mechanism that encrypts the images to enhance security and improve the efficiency of the searching methodology. An outsourcing search scheme was developed in [12] to encrypt the images such that there is reduction in

ISSN: 2582-2012 (online)
Submitted: 11.07.2021
Revised: 14.08.2021
Accepted: 25.08.2021
Published: 03.09.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.03
Pages: 259-271
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.3.008

calculation complexity as well as cost of communication. These methodologies and algorithms are suitable for offline KGA and will be effective when the attack occurs from within. Hence these algorithms face the issue of certificate management and escrow. A certificateless searchable encryption scheme is proposed in [13] which address these drawbacks. Moreover this methodology is not applicable to the KGA offline. In [14] a new certificateless searchable encryption scheme that is susceptible to keyword guessing attacks from the inside is proposed along with a searchable encryption technique which uses public key authentication. This algorithm encrypts as well as authenticates the keyword against inside attacks.

The authors in [15] developed a certificate-based, channel free searchable encryption algorithm that incorporates the advantage of sustaining KGA, offering a more secure environment in comparison to the previously existing work. This was further developed to the use of identity-based encryption algorithms which used tester schemes to withstand attacks from the KGA using a specific server. However the drawback of key escrow still existed in this methodology [16]. In 2021, the authors in [17], medical internet of things with certificate-less encryption algorithm and designated tester is used to address the issues of certificate management and key escrow to enhance the security of the system. Despite the various research conducted and experiments done, these schemes and their parallel work could not completely protect the privacy of the data owner's identity. Hence in [18], the authors have addressed this shortcoming using a deniably authenticated encryption (DAE) using encryption scheme.

In [19], Application and Multimedia tools encryption and identity based authentication scheme is used which decreases the use of public key certification faced by the previous algorithm. Later, a certicateless DAE was introduced to address the issue of key escrow [20]. The methodologies surveyed so far are not easily compatible with blockchain environment. The design and protocol of Bitcoin's blockchain make it possible for users to have multiple private and public keys that are used for doing the transactions. Hence this type of working will not be apt for developing a medical blockchain. To address these drawbacks,

ISSN: 2582-2012 (online)
Submitted: 11.07.2021
Revised: 14.08.2021
Accepted: 25.08.2021
Published: 03.09.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.03
Pages: 259-271
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.3.008

a social network-based healthcare is proposed in [21]. Similarly in [22], the authors have used healthcare blockchain with attribute based signature to improve the security of the system, protecting the signer's identity. The disadvantage of this work is that keyword search function is not application in this methodology. This drawback is overcome in [23] using a symmetric encryption scheme using blockchain making it susceptible to KGA and establishing sender privacy.

In this work, we proposed a DAE methodology [24] that works on blockchain to share the image data. Here the information of data [25] extracted from the image is first encrypted by the sender and uploaded onto the server. This image as a ciphertext identifier is further signed and saved onto the blockchain [26]. The following are the contributions made by the proposed work:

1. A blockchain based Deniably Authenticated Encryption storage of image data is proposed. The signature is shared between the various terminals using blockchain technology so that secure transaction between the user and receiver takes place. The data that is sent in this manner will be traceable, unforgettable and non-tampered [27]. To further improve practicability of the proposed work, a storage mode that uses an off-chain server and blockchain together is used, thereby the limitations of computation and storage by the block.

2. The proposed DAE technology will enable higher privacy protection for the data sent. When compared with the other methodologies [28], there are some algorithm that prove to be of higher efficiency that the proposed methodology. However, the level of security offered by the proposed work remains the best.

3. Issues related to key escrow and certificate management is avoided when using the certificateless cryptosystem.

4. The proposed methodology is capable of resisting the attacks of KGA and also satisfies the incompatibility of trapdoor and ciphertext [29].

ISSN: 2582-2012 (online)
Submitted: 11.07.2021
Revised: 14.08.2021
Accepted: 25.08.2021
Published: 03.09.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.03
Pages: 259-271
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.3.008

2. Proposed Methodology

2.1 System Model

There are five major entities involved in this proposed work namely blockchain, cloud server, data user, data sender and key generation center. The system mode of the proposed blockchain-based DAE is depicted in Fig.1. As per the figure, the information from the image such as semantic features, spatial relationship, shape, texture and colour are extracted. This extracted data is further encrypted and the ciphertext identifier [30] is also signed. This data along with the signature is uploaded into the cloud server. Using blockchain, the signature is stored for broadcasting. On retrieved the ciphertext, the data user will be able to verify the received ciphertext with the help of the saved signature.

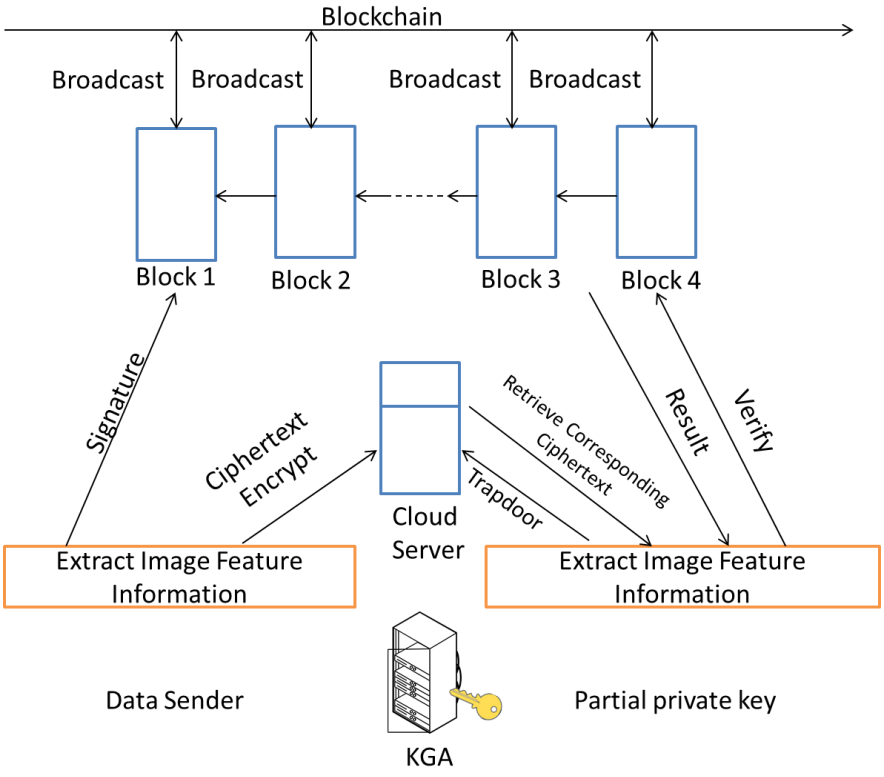

Figure 1. Blockchain-Based Deniably Authenticated Encryption Architecture

ISSN: 2582-2012 (online)
Submitted: 11.07.2021
Revised: 14.08.2021
Accepted: 25.08.2021
Published: 03.09.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.03
Pages: 259-271
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.3.008

Accordingly, the ciphertext can be accepted or rejected. The functions of the entities used in this process are as follows:

(1) Blockchain: When a request is received to determine the authenticity of a ciphertext, the signature that is stored is verified by Blockchain. A '0' or '1' is returned indicating 'False' and 'True' for the verification.

(2) Cloud Server: There are two major roles performed by the cloud server. One task is to search and return the ciphertext once the trapdoor is received from the Data user. The other task is to collect the large amount of medical data that is generated.

(3) Data User: Based on the medical image data, a keyword is chosen. Accordingly, a trapdoor is generated by the data users like the medical institution and the doctors. The generated trapdoor is sent to the cloud server to verify the signature and authenticate the ciphertext that is used.

(4) Data Sender: The extracted medical image data is encrypted using this entity (inclusive of patients). This data is further uploaded onto the cloud along with a signature for the ciphertext identifier. Using blockchain, the signature is stored for later authentication.

(5) Key Generation Center: The major role of this section is to generate partial private keys, system master keys and system parameters for data users and data senders.

2.2 Structure of Blockchain

In this proposed work, the blockain is categorized into two parts namely backup node and primary node. The role of the backup node is to build a new transaction, verify transaction signature and publish it. On the other hand, the role of the primary node is to collect the

ISSN: 2582-2012 (online)
Submitted: 11.07.2021
Revised: 14.08.2021
Accepted: 25.08.2021
Published: 03.09.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.03
Pages: 259-271
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.3.008

broadcasted transactions and build a new block. In the proposed blockchain-based DAE, the retrieved ciphertexts are received by the data user which is verified effectively to ensure the block's authenticity. A main block and a block header together constitute the block in the blockchain, similar to that of Bitcoin system. In particular, the ciphertext identifier and its signature are saved onto the main record. Timestamp, previous block hash as well as current block hash are available in the block header. To verify the authenticity of ciphertext, the main block will hold supporting documents as a collection of records. In this methodology, a practical byzantine fault tolerance is used as the consensus mechanism.

2.3 Correctness

The following correctness is followed by the proposed Blockchain-based DAE system:

a. The correctness to verify signature. The ciphertext identifier id is present in the signature 'sig' of the block chain.

b. If ω' is the keyword such that ω'= ω, I is the index holding keywork ω and $T_{\omega'}$ is the trapdoor, then the following equation is satisfied such that:

$$I_1 = e(H(a, B.c), rPK_{svr} \quad (1)$$

3. Results and Discussion

The changing trend of the running time of trapdoor algorithm is recorded in Fig.2. It is observed that as the number of ciphertext or keywords in every stage of the algorithm increases, there is a corresponding increase in the time taken. Similarly, the changing trend of the running time of the test algorithm is also observed and recorded in Fig. 2. Fig.5 shows the efficiency of the proposed and its comparison with the other algorithms. It is seen that the proposed blockchain-based DAE algorithms performs better than the other schemes and are found to overcome the negative drawbacks of the other methodologies. Moreover, DAE follows a storage model which uses both a cloud server as well as the blockchain. Though the efficiency

ISSN: 2582-2012 (online)
Submitted: 11.07.2021
Revised: 14.08.2021
Accepted: 25.08.2021
Published: 03.09.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.03
Pages: 259-271
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.3.008

of the proposed methodology is mildly lower than that of other methodologies, it still offers the best protection of user data.

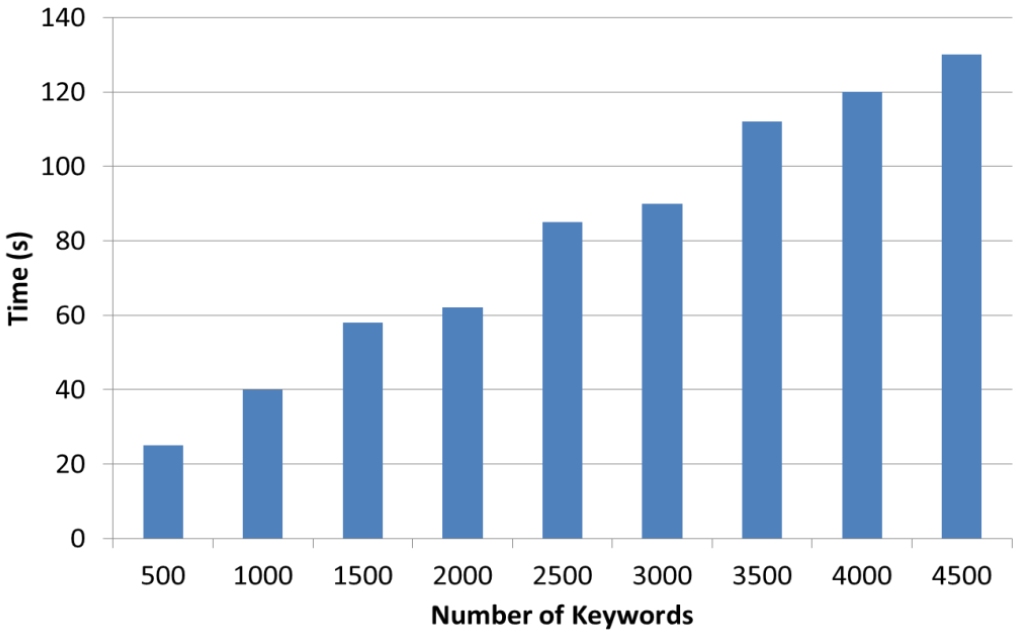

Figure 4. Trapdoor Algorithm

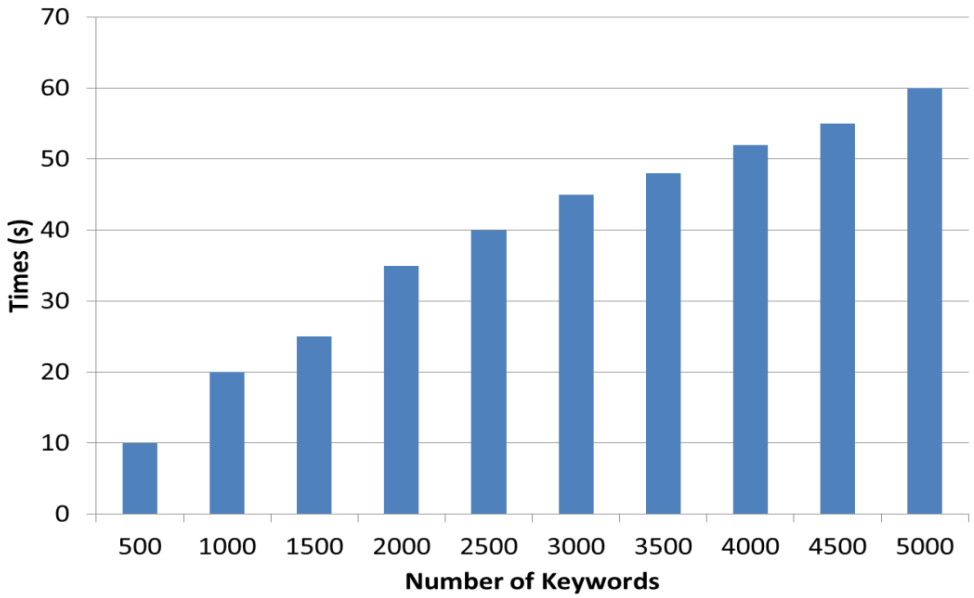

Figure 5. Test Algorithm

ISSN: 2582-2012 (online)
Submitted: 11.07.2021
Revised: 14.08.2021
Accepted: 25.08.2021
Published: 03.09.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.03
Pages: 259-271
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.3.008

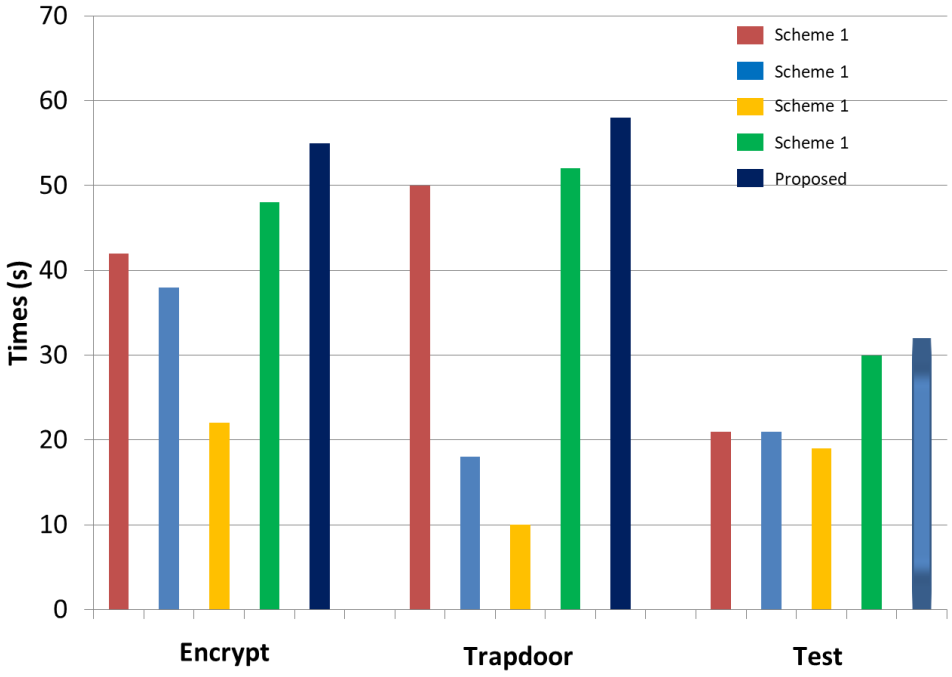

Figure 6. Time Comparison between Test, Encrypt and Trapdoor

4. Conclusion

In this paper, deniably authenticated encryption and blockchain are combined to develop an encryption algorithm that is suitable for medical image sharing, incorporating the advantages of both the algorithms positively. This model using a cloud server with blockcahin, so that the data that is shared remains traceable, unforgettable and non-tampered. Moreover, it also curbs the limitation of computing capabilities and storage of the2 blockchain. In this paper, we prove that the proposed blockchain based DAE will be able to resist KGA in certificateless cryptography. The proposed methodology is capable of resisting the attacks of KGA and also satisfies the incompatibility of trapdoor and ciphertext. 1. Issues related to key escrow and certificate management is avoided when using the certificateless cryptosystem. This algorithm will enable higher privacy protection for the data sent. When compared with the other methodologies, there are some algorithm that prove to be of higher efficiency that the proposed methodology. However, the level of security offered by the proposed work remains the best.

ISSN: 2582-2012 (online)
Submitted: 11.07.2021
Revised: 14.08.2021
Accepted: 25.08.2021
Published: 03.09.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.03
Pages: 259-271
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.3.008

Future work can involve improving the efficiency of the proposed work to meet the efficiency of trapdoor algorithm while maintaining its performance in privacy protection.

References

[1] Manoharan, Samuel, and Narain Ponraj. "Analysis of Complex Non-Linear Environment Exploration in Speech Recognition by Hybrid Learning Technique." Journal of Innovative Image Processing (JIIP) 2, no. 04 (2020): 202-209.

[2] Fu, B., Shu, Z., & Liu, X. (2018). Blockchain enhanced emission trading framework in fashion apparel manufacturing industry. Sustainability, 10(4), 1105.

[3] Madhuri, Chavan, Patil Deepali, and Shingane Priyanka. "Blockchain Technology in Healthcare Domain: Applications and Challenges." In International Conference on Innovative Data Communication Technologies and Application, pp. 543-550. Springer, Cham, 2019.

[4] Duraipandian, M. "Ranked k-NN Crowdsourced Model for Cloud Internet of Things (CIoT)." Journal of ISMAC 2, no. 03 (2020): 173-180.

[5] Shirley, D. R. A. (2014, July). Systematic diagnosis of power switches. In 2014 International Conference on Embedded Systems (ICES) (pp. 32-34). IEEE.

[6] Kruthik, J. T., K. Ramakrishnan, R. Sunitha, and B. Prasad Honnavalli. "Security Model for Internet of Things Based on Blockchain." In Innovative Data Communication Technologies and Application, pp. 543-557. Springer, Singapore, 2021.

[7] Parameswari, C. Devi, and Venkatesulu Mandadi. "Public Distribution System Based on Blockchain Using Solidity." In Innovative Data Communication Technologies and Application, pp. 175-183. Springer, Singapore, 2021.

[8] Chen, Joy Iong-Zong. "VANET-based Secure Information Exchange for Smart Charging." Journal of Electrical Engineering and Automation 2, no. 3 (2021): 141-145.

[9] Budhiraja, Sugandha, and Rinkle Rani. "TUDocChain-securing academic certificate digitally on blockchain." In International Conference on Inventive Computation Technologies, pp. 150-160. Springer, Cham, 2019.

ISSN: 2582-2012 (online)
Submitted: 11.07.2021
Revised: 14.08.2021
Accepted: 25.08.2021
Published: 03.09.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.03
Pages: 259-271
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.3.008

[10] Prakasam, V., and P. Sandeep. "Dual Edge-Fed Left Hand and Right Hand Circularly Polarized Rectangular Micro-Strip Patch Antenna for Wireless Communication Applications." IRO Journal on Sustainable Wireless Systems 2, no. 3: 107-117.

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

[12] Nirmal, D. "High Performance Flexible Nanoparticles Based Organic Electronics." Journal of Electronics and Informatics 1, no. 1, 2019 (2019): 99-106.

[13] Raj, Jennifer S. "Security Enhanced Blockchain based Unmanned Aerial Vehicle Health Monitoring System." Journal of ISMAC 3, no. 02 (2021): 121-131.

[14] Shajilin, J. B., & Shirley, D. R. A. (2021). Mitigation Measures for Power Quality Issues in Renewable Energy Integration and Impact of IoT in Grid Control. Integration of Renewable Energy Sources with Smart Grid, 305.

[15] Oham, Chuka, Regio A. Michelin, Raja Jurdak, Salil S. Kanhere, and Sanjay Jha. "B-FERL: Blockchain based framework for securing smart vehicles." Information Processing & Management 58, no. 1 (2021): 102426.

[16] Shirley, D., Sundari, V. K., Sheeba, T. B., & Rani, S. S. (2021). Analysis of IoT-Enabled Intelligent Detection and Prevention System for Drunken and Juvenile Drive Classification. In Automotive Embedded Systems (pp. 183-200). Springer, Cham.

[17] Feng, Shuo, Derong Shen, Tiezheng Nie, Yue Kou, and Ge Yu. "A generation probability based percolation network alignment method." World Wide Web (2021): 1-21.

[18] Sathesh, A. "Light Field Image Coding with Image Prediction in Redundancy." Journal of Soft Computing Paradigm 2, no. 3 (2020): 160-167.

[19] Dhaya, R., and R. Kanthavel. "Bus-Based VANET using ACO Multipath Routing Algorithm." Journal of trends in Computer Science and Smart technology (TCSST) 3, no. 01. (2021): 40-48.

[20] Chen, Joy Iong-Zong. "VANET-based Secure Information Exchange for Smart Charging." Journal of Electrical Engineering and Automation 2, no. 3 (2021): 141-145.

ISSN: 2582-2012 (online)
Submitted: 11.07.2021
Revised: 14.08.2021
Accepted: 25.08.2021
Published: 03.09.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.03
Pages: 259-271
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.3.008

[21] Valanarasu, Mr R. "Comparative Analysis for Personality Prediction by Digital Footprints in Social Media." Journal of Information Technology 3, no. 02 (2021): 77-91.

[22] Smys, Dr S., Dr Bashar, and Dr Wang. "SECURE AND SUSTAINABLE SMART GRID FRAMEWORK USING THE CLOUD COMPUTING." Journal of IoT in Social, Mobile, Analytics, and Cloud 1, no. 3: 137-146.

[23] Hamdan, Yasir Babiker. "Construction of Statistical SVM based Recognition Model for Handwritten Character Recognition." Journal of Information Technology 3, no. 02 (2021): 92-107.

[24] Thilaka, B., Janaki Sivasankaran, and S. Udayabaskaran. "Optimal Time for Withdrawal of Voluntary Retirement Scheme with a Probability of Acceptance of Retirement Request." Journal of Information Technology 2, no. 04 (2020): 201-206.

[25] Smys, S., and Jennifer S. Raj. "Analysis of Deep Learning Techniques for Early Detection of Depression on Social Media Network-A Comparative Study." Journal of trends in Computer Science and Smart technology (TCSST) 3, no. 01 (2021): 24-39.

[26] Tesfamikael, Hadish Habte, Adam Fray, Israel Mengsteab, Adonay Semere, and Zebib Amanuel. "Simulation of Eye Tracking Control based Electric Wheelchair Construction by Image Segmentation Algorithm." Journal of Innovative Image Processing (JIIP) 3, no. 01 (2021): 21-35.

[27] Valanarasu, Mr R. "Comparative Analysis for Personality Prediction by Digital Footprints in Social Media." Journal of Information Technology 3, no. 02 (2021): 77-91.

[28] Dickinson, Abigail, Manjari Daniel, Andrew Marin, Bilwaj Gaonkar, Mirella Dapretto, Nicole M. McDonald, and Shafali Jeste. "Multivariate neural connectivity patterns in early infancy predict later autism symptoms." Biological Psychiatry: Cognitive Neuroscience and Neuroimaging 6, no. 1 (2021): 59-69.

[29] Karuppusamy, P. "Building Detection using Two-Layered Novel Convolutional Neural Networks." Journal of Soft Computing Paradigm (JSCP) 3, no. 01 (2021): 29-37.

[30] Kumar, A. Dinesh. "Underwater Gripper using Distributed Network and Adaptive Control." Journal of Electrical Engineering and Automation 2, no. 1 (2020): 43-49.

ISSN: 2582-2012 (online)
Submitted: 11.07.2021
Revised: 14.08.2021
Accepted: 25.08.2021
Published: 03.09.2021

Journal of Artificial Intelligence and Capsule Networks (2021)
Vol.03/ No.03
Pages: 259-271
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2021.3.008

Author's biography

C. Vijesh Joe is presently working as an assistant professor in the Department of Computer Science and Engineering, at VV College of Engineering, Tirunelveli, India. His major area of research includes cloud computing, speech processing, wireless networks security, data science analytics, and computer graphics in multimedia.

Jennifer S. Raj received the Ph.D degree from Anna University and Master's Degree in communication System from SRM University, India. Currently she is working in the Department of ECE, Gnanamani College of Technology, Namakkal, India. She is a life member of ISTE, India. She has been serving as Organizing Chair and Program Chair of several International conferences, and in the Program Committees of several International conferences. She is book reviewer for Tata Mc Graw hill publication and publishes more than fifty research articles in the journals and IEEE conferences. Her interests are in wireless Health care informatics and body area sensor networks.

ISSN: 2582-2012 (online)
Submitted: 11.07.2021
Revised: 14.08.2021
Accepted: 25.08.2021
Published: 03.09.2021