Journal of Trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 02
Pages: 147-160
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.2.006

SDN Controller and Blockchain to Secure Information Transaction in a Cluster Structure

Suma V
Professor, Department of Information Science and Engineering, Dayananda Sagar College of Engineering, Bangalore, India
E-mail id: suma-ise@dayanandasagar.edu

Abstract

The Internet of Things [IoT] is one of the most recent technologies that has influenced the way people communicate. With its growth, IoT encounters a number of challenges, including device heterogeneity, energy construction, comparability, and security. Energy and security are important considerations when transmitting data via edge networks and IoT. Interference with data in an IoT network might occur unintentionally or on purpose by malicious attackers, and it will have a significant impact in real time. To address the security problems, the suggested solution incorporates software defined networking (SDN) and blockchain. In particular, this research work has introduced an energy efficient and secure blockchain-enabled architecture using SDN controllers that are operating on a novel routing methodology in IoT. To establish communication between the IoT devices, private and public blockchain are used for eliminating Proof of Work (POW). This enables blockchain to be a suitable resource-constrained protocol for establishing an efficient communication. Experimental observation indicates that, an algorithm based on routing protocol will have low energy consumption, lower delay and higher throughput, when compared with other classic routing algorithms.

Keywords: SDN, Proof-of-Work, block chain, energy efficiency, internet of things, security

ISSN: 2582-4104
Submitted: 29.05.2021
Revised: 01.07.2021
Accepted: 22.07.2021
Published: 27.07.2021

Journal of Trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 02
Pages: 147-160
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.2.006

1. Introduction

As the internet evolves, so do technological elements of introducing instruments to the community [1]. This includes Internet of Things (IoT) devices, automobiles, appliances, and so on. The combination of blockchain with the internet of things has resulted in the development of smart cities and, eventually, smart nations [2]. Informational services such as e-service marketing, e-business governance and e-learning have also changed the way of life and everyday happenings with the inclusion of modern day technologies [3]. With this rapid growth and expansion, it is only predictable that by 2030 IoT will have a tremendous influence in our everyday lives [4-5]. However, a number of challenges are associated with the use of IoT such as compatibility, multiple attacks, heterogeneity of devices and lack of central control [6]. Energy consumption and security are some of the most crucial challenges in the IoT industry. Because of their heterogeneous nature, the desired devices have a number of constraints in terms of processing and energy resources [7]. This results in the possible implementation of security and challenges in communication.

In recent years, edge computing has been proven to be a positive architecture to tackle some of the challenges faced due to IoT resource constraints. However, there are some issues that are yet to be addressed inclusive of IoT specific issues. Security, availability and confidentiality are some of the new solutions that have been made available to improve the efficiency of IoT devices during communication process [8, 9]. It is necessary to consider energy consumption in order to ensure that it doesn't affect the security or performance of the system. Availability is enforced so that the data service is always available at any point of time by considering that IoT devices consume low amount of energy. Similarly, the confidentiality is implemented so that only the authorised people can be given access to important messages [10]. Finally, binding relevant parties and integrity make sure that the information about source and destination [11] along with modification, if any, it is easily detected. This indicates that, a new architecture is required to establish a proper communication in the IoT network [13, 14].

ISSN: 2582-4104
Submitted: 29.05.2021
Revised: 01.07.2021
Accepted: 22.07.2021
Published: 27.07.2021

Journal of Trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 02
Pages: 147-160
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.2.006

The architecture should be built to properly manage the minimum energy consumption and security in the network layers such as physical layers as well as applications [15]. Hence, we have used blockchain [16] and software defined networking (SDN) [17] to incorporate this architecture. SDN can be used to hold two elements namely switch and control that operates the control plane and data plane. The controller will be used to incorporate management policies and specific network programmability, [18] while the switch [19] is used for packet forwarding. This will leverage programmability, high flexibility, intelligent management, communication and remote control, as well as full control over the network. It also enables the ability to incorporate secure [20] and centralized network services such as bandwidth management, energy consumption, routing and security apart from unauthorised access prevention. However, the biggest concerns while using SDN is its insecurity. It is possible to use blockchain to securely transfer a file in a SDN.

Blockchain not only protects the privacy but also reserves resource availability in the event of intruders. In fact, Bitcoins transaction verification is built on blockchain technology [21]. Distributed cloud storage e-governance, medical information collection and intelligent counting officers are some of the places, where blockchain is being incorporated beyond financial transactions [22]. It is mainly built up of blocks that hold information and instead of centralised management it incorporates peer-to-peer network management which is distributed and flexible. On using blockchain capability, it is possible to tackle numerous limitations and challenges of IoT and using SDN controller a more energy efficient and secure architecture is built [23]. However, it has been observed that blockchain tend to complicate the calculator aspects such as delay and bandwidth overhead and hence on suitable for IoT devices. To address this drawback, we have introduced and IoT-friendly blockchain that proves to be efficient using SDN controller in every cluster through a distributed trust manner [24]. The make use of a private distribution ledger which can be altered, in every cluster, and is controlled centrally by a SDN [25]. To further enhance proof-of-work a proper routing protocol is incorporated along with prevention of selfish nodes entry. A cluster structure has been used in this architecture to enhance security and optimise energy consumption [26, 27]. The major

ISSN: 2582-4104
Submitted: 29.05.2021
Revised: 01.07.2021
Accepted: 22.07.2021
Published: 27.07.2021

Journal of Trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 02
Pages: 147-160
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.2.006

focus of this work deals with building a blockchain-enabled architecture for SDN controllers. Following is the outline of the objectives of this work [28].

- Provide an energy-efficient and secure file transfer facility between the devices in under a SDN controller, using appropriate routing protocols based on the cluster stricter, taking into consideration the constraints on IoT devices [29].
- Develop IoT compatible private and public blockchain, which use peer-to-peer communication and secure access control to data and IoT devices.
- Build a blockchain-based SDN Controller, operating in clusters with distributed network management.

2. Proposed Methodology

This research work has designed a blockchain-based SDN Controller and clustering operations with distributed network management. The SDN controller initiates communication between the possible IoT devices by connecting it to a single blockchain [30]. As observed in Bitcoin, a distributed peer-to-peer network is created by the SDN controllers. There are two crucial goals: One is to ensure that the file transfer between SDN and blockchain takes place in a secure manner. Another is to decrease the energy consumption of the devices. Without a properly organized structure, it is not possible for large networks to operate in a smooth manner and the cluster structure serves this purpose. Here every cluster in the architecture is known as a SDN domain. Every SDN controller behaved as a cluster head to decrease the overhead and network delay. A cluster head is appointed for each SDN domain to coordinate the functions of the clusters to activate the IoT devices. A number of objects such as the heterogeneous devices were connected to the SDN controller which served as a coordinator. As the coordinator, the SDN will be able to monitor the IoT devices, enforce policies and also respond to the needs in every cluster. A crucial part of this architecture is cloud storage which is used to store the information on the cloud. In general, cybercrime attacks and illegal exploitation are

ISSN: 2582-4104
Submitted: 29.05.2021
Revised: 01.07.2021
Accepted: 22.07.2021
Published: 27.07.2021

Journal of Trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 02
Pages: 147-160
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.2.006

common attack on centrally managed system. The use of peer-to-peer communication will enhance the data integrity, security and remove unwanted interferences.

2.1 Transfer of File

In this work, every IoT device has a private key and a public key, which was used to secure the transaction process by following the SDN controller policies. Every packet that is transmitted by the IoT device is signed with a private key and published with a public key. By considering the sender's public key, the pack is verified based on the authenticity of the key and later it is transmitted in a block format. When a file is shared by the IoT device, authentication is done by the other members present in the cluster. This block will be kept in the private blockchain, while the information is delivered to the destination. When an IoT device has to send information to a receiver located outside the cluster, the SDN controller will first establish relationship by requesting access to the cluster head of the destination cluster after publishing the public key. Ultimately when the IoT device is transferred, the corresponding file will also be sent to its destination.

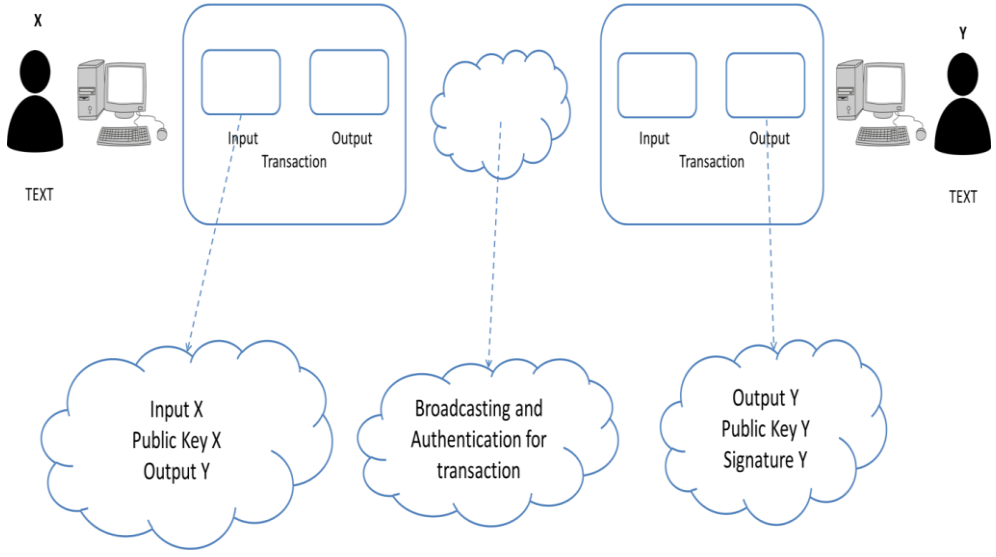

Figure 1. Architecture of Proposed Blockchain

ISSN: 2582-4104
Submitted: 29.05.2021
Revised: 01.07.2021
Accepted: 22.07.2021
Published: 27.07.2021

Journal of Trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 02
Pages: 147-160
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.2.006

Consider the figure 1, where a blockchain is present such that it holds all the IoT devices within a cluster. The process of file transfer will take place in the following manner.

- Step 1: A file has to be transferred with A1 as the source and A4 as the destination.
- Step 2: A1 signs the transaction. A private key is used to sign and a public key is used to publish.
- Step 3: Using the public key, the block is broadcasted to be viewed by the entire network. If the cluster does not have an appropriate IoT, the IoT device will be sent to another SDN controller.
- Step 4: Based on the public key, the IoT devices will authenticate the transaction similar to the way the sender authenticates the file.
- Step 5: To enable transactional transparency, a block is added to the chain of transactions.
- Step 6: The transferred file can only be opened by the receiver, who holds the private key to the file.

2.2 Enhancement of energy efficiency and security

In public blockchain, Proof of work (POW) is used as a consensus mechanism to allocate blocks. However the incorporation of POW has made the use of blockchain with IoT impractical due to its requirement of large amount of processing resources and energy resources. To overcome these obstacles, indication method distributed trust and a cluster structure by SDN controller is used. It addresses the POW based blockchain problems such as reducing energy consumption and time overheads. In the private and public blockchain, communication between two cluster heads and communication within the clusters are considered as transactions. Taking these facts into consideration, POW is excluded from blocks

ISSN: 2582-4104
Submitted: 29.05.2021
Revised: 01.07.2021
Accepted: 22.07.2021
Published: 27.07.2021

Journal of Trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 02
Pages: 147-160
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.2.006

in the blockchain. This is enforced in such a way that overhead due to POW is reduced significantly. To verify the received blocks and decrease their overhead a distributed trust is used by the SDN controller for authentication. The SDN controller generates the hash for every block. The hash value changes as the data changes, through computation. Use of hash value in the block enhances the security of the system. Using this proposed architecture it is possible to consider features using smart contracts, carry out transactions and share data. For proper maintenance of the numerous energy resources, the heterogeneous devices need to follow an appropriate routing protocol under every SDN domain. This will improve the energy consumption and energy efficiency of the IoT devices.

The proposed protocol is capable of preventing the selfish and malicious nodes from accessing the SDN domain, which will result in decreased energy consumption and improved security. Reduction in energy consumption is highly favoured as it plays a crucial role in data transfer. The algorithm followed for energy efficiency and secure mechanism is as follows:

- The IoT devices must initially register the controller.
- A unique address is allocated to every IoT in every SDN domain followed by private and public key.
- Under the SDN domain, every private blockchain will hold a data set that retains the information about energy remaining and energy sources of the connected IoT devices. Depending on the energy amount transmitted to the other devices and the controller for communication, the size of the IoT device packets will also vary.
- In the event of crossing the energy threshold, the device uses neighbouring nodes to transfer the packets. Selfish or malicious nodes that have penetrated the controller will make use of the neighbouring blocks and its energy resources for overcoming the threshold. Moreover, they are also registered in the public blockchain and will not able to associate with any other cluster.

ISSN: 2582-4104
Submitted: 29.05.2021
Revised: 01.07.2021
Accepted: 22.07.2021
Published: 27.07.2021

Journal of Trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 02
Pages: 147-160
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.2.006

3. Results and Discussion

Experimental results of the proposed work is observed and recorded. Fig.2 shows the energy consumed by the cloud storage, IoT device and SDN controller. It is seen that, the amount of energy consumed by the proposed methodology is considerably less, when compared with the previous BCF algorithm.

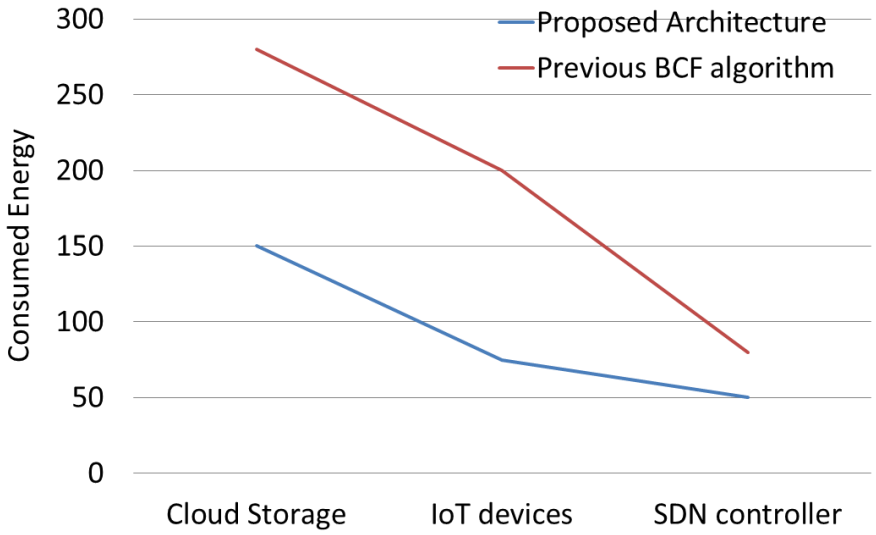

Figure 2. Energy Consumption Measures for Proposed Vs. Existing Method

Fig. 4 shows the time overhead calculated for the proposed and existing methodology, while Fig.5 indicates a comparison on the efficient usage of the bandwidth by using the number of packets transmitter along the way.

ISSN: 2582-4104
Submitted: 29.05.2021
Revised: 01.07.2021
Accepted: 22.07.2021
Published: 27.07.2021

Journal of Trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 02
Pages: 147-160
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.2.006

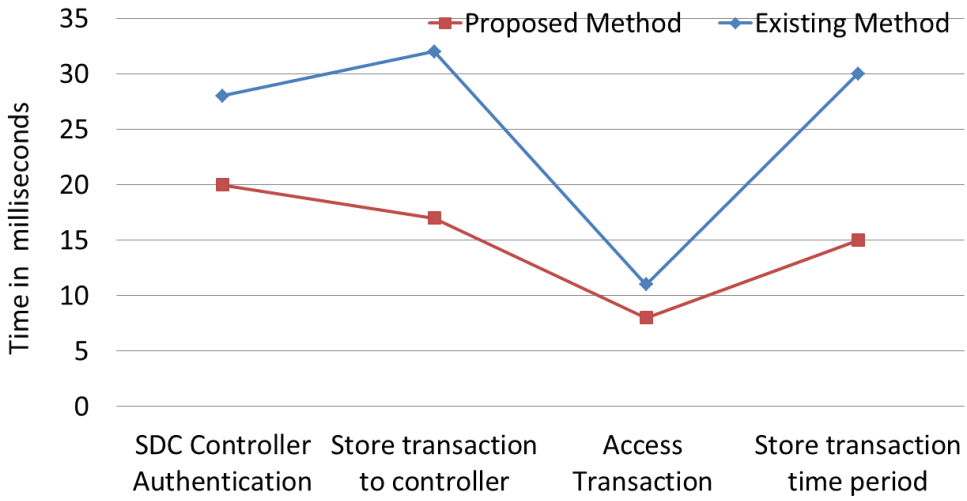

Figure 3. Time Overhead for Proposed Vs. Existing Method

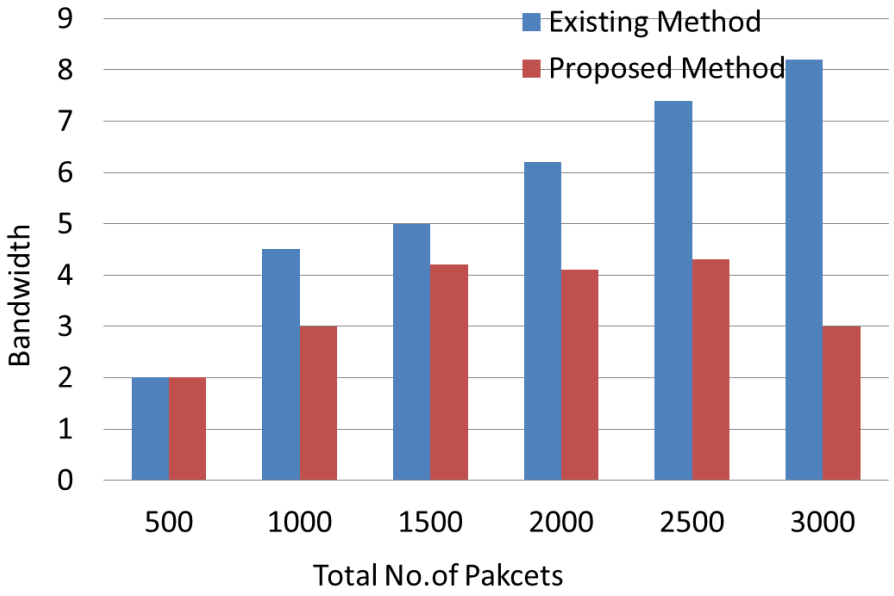

Figure 4. Bandwidth vs. No. of Packets

ISSN: 2582-4104
Submitted: 29.05.2021
Revised: 01.07.2021
Accepted: 22.07.2021
Published: 27.07.2021

Journal of Trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 02
Pages: 147-160
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.2.006

4. Conclusion

As the Internet of Things (IoT) expands and develops technologically, demonstrating its power in many fields, it is being employed in a variety of applications. It does, however, confront a number of limitations and challenges in terms of processing power, privacy, and security. With the aid of blockchain and SDN, the proposed work addresses some of the challenges imposed by this architecture. Both public and private blockchains are incorporated into the IoT network by using the clustered structure. On eliminating POW and with the proposed routing protocol design, an improved security of communication and reduced energy consumption has been observed. Based on experimental observation, it is seen that the energy efficiency, performance and throughput of the proposed work is better than the existing BCF algorithm.

References

[1] Bhalaji, N. "Reliable Data Transmission with Heightened Confidentiality and Integrity in IOT Empowered Mobile Networks." Journal of ISMAC 2, no. 02 (2020): 106-117.

[2] Ramaguru, R., Sindhu, M., & Sethumadhavan, M. (2019, April). Blockchain for the Internet of Vehicles. In International Conference on Advances in Computing and Data Sciences (pp. 412-423). Springer, Singapore.

[3] Shakya, Subarna. "Process mining error detection for securing the IoT system." Journal of ISMAC 2, no. 03 (2020): 147-153.

[4] Saranti, P. G., Chondrogianni, D., & Karatzas, S. (2018, May). Autonomous vehicles and blockchain technology are shaping the future of transportation. In The 4th conference on sustainable urban mobility (pp. 797-803). Springer, Cham.

[5] 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.

ISSN: 2582-4104
Submitted: 29.05.2021
Revised: 01.07.2021
Accepted: 22.07.2021
Published: 27.07.2021

Journal of Trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 02
Pages: 147-160
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.2.006

[6] Shirley, D. Ruth Anita. "Systematic diagnosis of power switches." In 2014 International Conference on Embedded Systems (ICES), pp. 32-34. IEEE, 2014.

[7] Smys, S. "A Survey on Internet of Things (IoT) based Smart Systems." Journal of ISMAC 2, no. 04 (2020): 181-189.

[8] Erdem, A., Yildirim, S. Ö., & Angin, P. (2019). Blockchain for ensuring security, privacy, and trust in IoT environments: the state of the art. Security, Privacy and Trust in the IoT Environment, 97-122.

[9] Suma, V. "Community Based Network Reconstruction for an Evolutionary Algorithm Framework." Journal of Artificial Intelligence 3, no. 01 (2021): 53-61.

[10] Madaan, G., Bhushan, B., & Kumar, R. (2021). Blockchain-based cyberthreat mitigation systems for smart vehicles and industrial automation. In Multimedia Technologies in the Internet of Things Environment (pp. 13-32). Springer, Singapore.

[11] Haoxiang, Wang, and S. Smys. "Big Data Analysis and Perturbation using Data Mining Algorithm." Journal of Soft Computing Paradigm (JSCP) 3, no. 01 (2021): 19-28.

[12] Haro-Olmo, F. J., Alvarez-Bermejo, J. A., Varela-Vaca, A. J., & López-Ramos, J. A. (2021). Blockchain-based federation of wireless sensor nodes. The Journal of Supercomputing, 77(7), 7879-7891.

[13] 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.

[14] Banotra, A., Sharma, J. S., Gupta, S., Gupta, S. K., & Rashid, M. (2021). Use of blockchain and internet of things for securing data in healthcare systems. In Multimedia Security (pp. 255-267). Springer, Singapore.

[15] Bagde, Sejal, Pratiksha Ambade, Manasvi Batho, Piyush Duragkar, Prathmesh Dahikar, and Avinash Ikhar. "Internet of Things (IOT) Based Smart Switch." Journal of IoT in Social, Mobile, Analytics, and Cloud 3, no. 2 (2021): 149-162.

[16] Senthilkumar, M., Kavitha, V. R., Kumar, M. S., Raj, P. A. C., & Shirley, D. R. A. (2021, March). Routing in a Wireless Sensor Network using a Hybrid Algorithm to Improve the

ISSN: 2582-4104
Submitted: 29.05.2021
Revised: 01.07.2021
Accepted: 22.07.2021
Published: 27.07.2021

Journal of Trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 02
Pages: 147-160
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.2.006

Lifetime of the Nodes. In IOP Conference Series: Materials Science and Engineering (Vol. 1084, No. 1, p. 012051). IOP Publishing.

[17] Shakya, Subarna. "IoT based F-RAN Architecture using Cloud and Edge Detection System." Journal of ISMAC 3, no. 01 (2021): 31-39.

[18] Angin, P., Mert, M. B., Mete, O., Ramazanli, A., Sarica, K., & Gungoren, B. (2018, June). A blockchain-based decentralized security architecture for IoT. In International Conference on Internet of Things (pp. 3-18). Springer, Cham.

[19] Karthikeyan, M., S. Sathiamoorthy, and M. Vasudevan. "Lane Keep Assist System for an Autonomous Vehicle Using Support Vector Machine Learning Algorithm." In International Conference on Innovative Data Communication Technologies and Application, pp. 101-108. Springer, Cham, 2019.

[20] Kaiser, C., Steger, M., Dorri, A., Festl, A., Stocker, A., Fellmann, M., & Kanhere, S. (2018, September). Towards a Privacy-Preserving Way of Vehicle Data Sharing–A Case for Blockchain Technology?. In International Forum on Advanced Microsystems for Automotive Applications (pp. 111-122). Springer, Cham.

[21] Aishwariya, K. K., Sanil K. Daniel, and K. V. Sujeesh. "Zone Safe Traffic Assist System and Automated Vehicle with Real-Time Tracking and Collision Notification." In International Conference on Innovative Data Communication Technologies and Application, pp. 663-669. Springer, Cham, 2019.

[22] Shirley, D. R. A., Sundari, V. K., Sheeba, T. B., & Rani, S. S. Analysis of IoT-Enabled Intelligent Detection and Prevention System for Drunken and Juvenile Drive Classification. Automotive Embedded Systems: Key Technologies, Innovations, and Applications, 183.

[23] Manickavasagam, L., N. Krishanth, B. Atul Shrinath, G. Subash, S. R. Mohanrajan, and R. Ranjith. "Instrument Cluster Design for an Electric Vehicle Based on CAN Communication." In Inventive Computation and Information Technologies, pp. 271-284. Springer, Singapore, 2021.

ISSN: 2582-4104
Submitted: 29.05.2021
Revised: 01.07.2021
Accepted: 22.07.2021
Published: 27.07.2021

Journal of Trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 02
Pages: 147-160
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.2.006

[24] Ekramifard, A., Amintoosi, H., & Seno, A. H. (2019, March). A systematic literature review on blockchain-based solutions for iot security. In The 7th International Conference on Contemporary Issues in Data Science (pp. 311-321). Springer, Cham.

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

[26] Reebadiya, D., Rathod, T., Gupta, R., Tanwar, S., & Kumar, N. (2021). Blockchain-based Secure and Intelligent Sensing Scheme for Autonomous Vehicles Activity Tracking Beyond 5G Networks. Peer-to-Peer Networking and Applications, 1-18.

[27] Srinivas, Kethavath, and Mohit Dua. "Fog Computing and Deep CNN Based Efficient Approach to Early Forest Fire Detection with Unmanned Aerial Vehicles." In International Conference on Inventive Computation Technologies, pp. 646-652. Springer, Cham, 2019.

[28] Rakovic, V., Karamachoski, J., Atanasovski, V., & Gavrilovska, L. (2019). Blockchain paradigm and Internet of Things. Wireless Personal Communications, 106(1), 219-235.

[29] Kumar, S. Satheesh, S. Karthik, J. S. Sujin, N. Lingaraj, and M. D. Saranya. "Smart On-board Vehicle-to-Vehicle Interaction Using Visible Light Communication for Enhancing Safety Driving." In Inventive Computation and Information Technologies, pp. 247-257. Springer, Singapore, 2021.

[30] Abubaker, Z., Gurmani, M. U., Sultana, T., Rizwan, S., Azeem, M., Iftikhar, M. Z., & Javaid, N. (2019, November). Decentralized mechanism for hiring the smart autonomous vehicles using blockchain. In International Conference on Broadband and Wireless Computing, Communication and Applications (pp. 733-746). Springer, Cham.

Author's biography

Suma V holds a B.E. in Information Science and Technology, M.S. in Software Systems and Ph.D. in Computer Science and Engineering. Currently, she is working as Dean of the Research and Industry Incubation Centre, and a Professor at the Department of Information Science and Engineering, Dayananda Sagar College of Engineering, Bangalore, India. She has more than

ISSN: 2582-4104
Submitted: 29.05.2021
Revised: 01.07.2021
Accepted: 22.07.2021
Published: 27.07.2021

Journal of Trends in Computer Science and Smart technology (TCSST) (2021)
Vol.03/ No. 02
Pages: 147-160
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2021.2.006

17 years of teaching experience and has published over 180 papers, including research articles published in leading international journals, such as ACM, ASQ, Crosstalk, IET Software, and journals published by MIT and Dartmouth College in the USA. Her research has also been published on NASA, UNI Trier, Microsoft, CERN, IEEE, ACM and Springer portals.

ISSN: 2582-4104
Submitted: 29.05.2021
Revised: 01.07.2021
Accepted: 22.07.2021
Published: 27.07.2021