International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5744
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

Secure Communication Model for Dynamic Task Offloading in Multi-Cloud Environment

[a]**Chava Usharani**, [b]**P. Venkata Krishna**, [c]**Praveena Akki**, [d]**V. Saritha**, [e]**Dr. Gitanjali J**

[a] Department of Computer Science, Sri Padmavati Mahila University, Tirupati, India
ranic225@gmail.com
[b]Department of Computer Science, Sri Padmavati Mahila University, Tirupati, India
pvk@spmvv.ac.in
[c]School of Computing, SRM Institute of Science and Technology,
Kattankulathur, Chennai, 603203, Tamil Nādu, India
Email: praveena2@srmist.edu.in
[d]Department of Computer Science and Engineering,
Sri Padmavati Mahila University, Tirupati, India
vsaritha@spmvv.ac.in
[e]Dept of Information Technology and Engineering
Vellore Institute of Technology, Tamil Nādu, India
Gitanjalij@vit.ac.in

Abstract— As the data is increasing day-by-day, the mobile device storage space is not sufficient to store the complete information and also the computation capacity also is a limited resource which is not sufficient for performing all the required computations. Hence, cloud computing technology is used to overcome these limitations of the mobile device. But security is the main concern in the cloud server. Hence, secure communication model for dynamic task offloading in multi-cloud environment is proposed in this paper. Cloudlet also is used in this model. Triple DES with 2 keys is used during the communication process between the mobile device and cloudlet. Triple DES with 3 keys is used by the cloudlet while offloading the data to cloud server. AES is used by the mobile device while offloading the data to the cloud server. Computation time, communication time, average running time, and energy consumed by the mobile device are the parameters which are used to evaluate the performance of the proposed system, SCM_DTO. The performance of the proposed system, SCM_DTO is compared with ECDH-SAHE and is proved to be performing better.

Keywords- Multi-Cloud Computing,Secure Communicate, mobile cloud computing

I. INTRODUCTION

The systematic use of the cloud platform to connect smaller mobile devices and other machines to the network for data exchange, different mobile operating systems, processing power, apps, storage, etc. is called mobile cloud computing (MCC). Millions of interconnected mobile users can quickly and easily access a variety of homogenous and heterogeneous resources at their locations throughout the world. Applications that are running on a distant server with powerful computing power are accessed by MCC. Different formats are required for the massive storage and mobile devices to service mobile customers. A cloud operating system, mobile devices, network devices, various resource-rich servers, as well as local and remote applications, comprise MCC. These are kept in a certain structured manner and connected. The resources must be effectively managed, kept up, and distributed among the cloud devices. Today, the world is moving toward MCC because of the cloud's many advantages.

Processor speed, battery life, encrypted copying, and distributing various mobile programmes from the cloud to MCC users are some of the primary research areas for the company. efficient task submission and processing enabling fault tolerance, resource sharing, reusing computing resources across numerous devices, or even the same computing device, to enable internet-based applications like games, online simulation approaches, etc. t, are the problems with mobile devices nowadays with MCC. By shifting some resources and computationally demanding tasks to the mobile cloud, MCC enables mobile devices to conserve power and processing time. The research observed that task precedence needs and the ability to break down large tasks into smaller ones. The task level offloading's precise granularity can result in time and energy savings. Additionally, MCC optimises task scheduling by offloading it from a mobile device to the MCC VM. Offloading all computations to the computational cloud for processing and returning the results to the mobile cloud service is one of the more effective deployment techniques for MCC. In order to decrease the energy and time consumption of mobile devices, several existing methodologies are introduced, including smart batteries, power scheduling, efficient operating systems, energy-aware communication protocols, and apps. Offloading of tasks is thus introduced to minimise the demands of these mobile device tasks. The handling of mobile device energy and time optimisation is improved and the battery life of the devices is decreased.

II. RELATED WORK

A novel Adaptive Task Offloading (ATO) auction mechanism is presented in [1] to select the MEC server to offload with access capability and security constraints, and how to schedule tasks with various deadline constraints, which incentivizes the third party of MEC providers to share their computing resources with the maximum profit. The efficiency, truthfulness, and individual rationality of the suggested auction system are its features. ATO auction performance has been extensively simulated, and the experimental studies indicate that the method maximises the utility of the MEC server more effectively than the traditional greedy methods.

The resource-constrained edge devices are made feasible for task offloading by a task offloading approach with a centralised low-latency, secure, and reliable decision-making algorithm with strong emergency handling capacity (LSRDM-EH) is proposed in [2]. Additionally, a thorough blockchain-based two-layer and multidimensional security plan is suggested to properly assure the security of the entire network. Furthermore, a blockchain sharing method to minimize system time latency in order to address the fundamental time-inefficiency issue of blockchain is proposed. Numerous simulations have been performed in order to validate the effectiveness of the suggested measures, and the results show that our solutions are superior in terms of time-latency, dependability, and security.

An algorithm for module placement based on classification and regression trees (MPCA) is proposed in [3]. By MPCA, we choose the top FDs for modules. First, it is determined whether the power consumption of MDs exceeds that of Wi-Fi; if so, offloading will take place. Authentication, privacy, integrity, availability, capacity, speed, and cost are among of the criteria used by the MPCA to determine which FD is best. We examine and use the likelihood of network resource utilisation in module offloading in order to optimise MPCA. This function is invoked by (MPMCP).

A blockchain network based on mobile edge computing (MEC) is presented in [4] in which several mobile users (MUs) serve as miners by wirelessly offloading their data processing and mining activities to a nearby MEC server. Our goal is to minimise the long-term system offloading utility and to maximise the privacy levels for all blockchain users. Specifically, we formulate task offloading, user privacy preservation, and mining profit as a combined optimization issue that is treated as a Markov decision process.

A Customized List Scheduling based Offloading (CLSO) algorithm is proposed in [5] that aims to reduce overall completion time while taking the end devices' energy constraints into account. The outcomes of the experiment demonstrate that our approximation technique greatly exceeds the current state-of-the-art offloading strategy and can successfully lower the overall completion time.

A bargaining-based approach's is proposed in [6] that main benefit is that it offers an axiom-based strategic solution for the task offloading problem while adapting quickly to the current network settings. In-depth simulation studies are carried out to show how successful the suggested plan is, and it is found that it performs better than existing schemes.

To choose the best task offloading method in the IoT, a novel energy-conscious task offloading methodology is proposed in [7]. The architecture of mobile edge computing (MEC) in the Internet of Things is first examined. The difficulties of task offloading in MEC for IoT are introduced in the second section. Third, the ideal task offloading approach for computing tasks is accomplished using the framework for MEC. Finally, simulation findings demonstrate that, when compared to the traditional method, the suggested approach can significantly increase task offloading efficiency.

A promising network paradigm has been put forth: vehicle edge computing networks (VECNs) is proposed in [8], which combine MEC and vehicular networks. MEC offloading allows for a significant reduction in the computational strain on ICVs by placing MEC servers at the network's edge. However, given the rapid changes in communications, computing resources, and other areas, prior task offloading techniques did not adequately account for quickly changing ICVs and frequent handover.

Nimbus, a task placement and offloading solution for a multi-tier edge-cloud infrastructure is proposed in [9] that allows deep learning tasks to be taken out of the pipeline for AR applications and sent to nearby GPU-powered edge devices[10] . Our goal is to reduce energy consumption on mobile devices and end-user latency. Comprehensive analysis, which is based on benchmarked

DOI: https://doi.org/10.17762/ijritcc.v10i10.5744
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

performance of AR jobs, demonstrates the effectiveness of our solution. For real-time object detection in AR applications, Nimbus lowers task latency by a factor of four and energy usage by a factor of seventy-seven percent[11].

To separate the original issue into two problems: a task offloading (TO) problem that improves the optimal-value function corresponding to the RA problem, and a resource allocation (RA)[12] problem with fixed task offloading decision is proposed in [13]. Convex and quasi-convex optimization methods are used to tackle the RA problem, and an unique heuristic algorithm for the TO problem that yields a suboptimal result in polynomial time is provided[14]. Simulation findings demonstrate that our algorithm performs nearly as well as the ideal solution and greatly outperforms more conventional methods in terms of the utility of offloading for consumers[15].

III. PROPOSED METHODOLOGY

3.1 Secure Communication Model for Dynamic Task Offloading in Multi-Cloud Environment (SCM_DTO)

Task offloading process is required in order to send the task to be executed in the environment like cloud, cloudlet, etc which is external to the mobile device as the resources like computation capacity, power, etc are limited in the case of mobile device. In this paper, three different environments are considered for performing computations. They are device environment, multi-cloudlet and multi-cloud environment. The system model is shown in Fig. 3.1

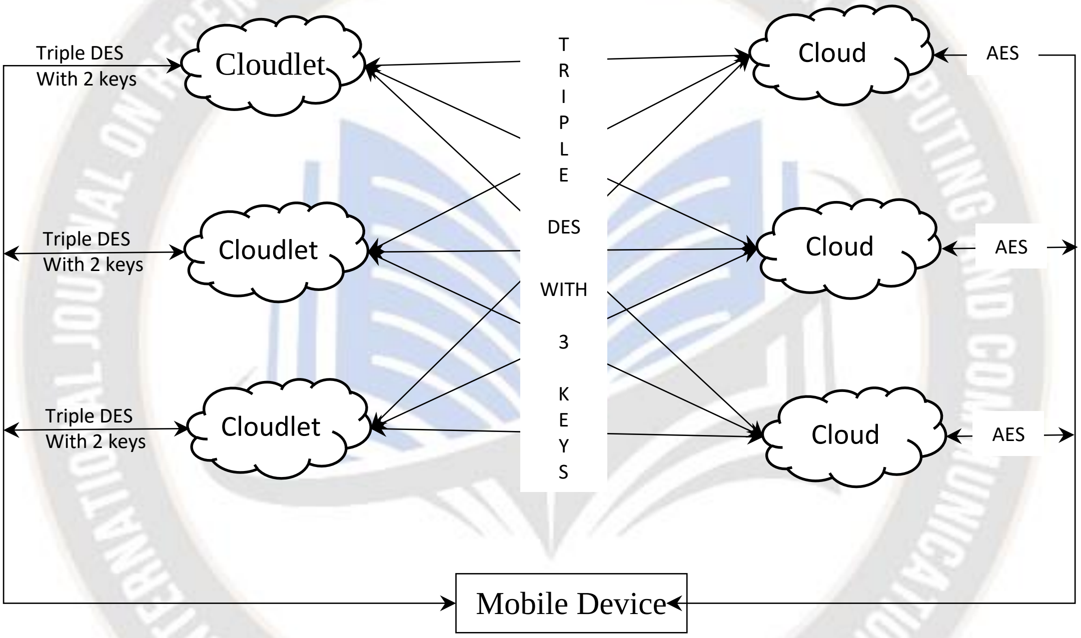

Fig. 3.1 System Model

In the proposed system model, the mobile device can offload the task for computation to any cloudlet or any cloud server. The cloudlet can also offload the task to cloud if required. Existing encryption techniques are used while offloading the task to cloudlet and cloud. Triple DES with 2 different keys is used while offloading the task by the mobile device to cloudlet. The task is decrypted in the cloudlet and is computed. Once the process is completed, cloudlet encrypts using the same Triple DES with 2 different keys to send the results to the mobile device. If the task need to be forwarded to the cloud server by the cloudlet, then Triple DES with 3 different keys is used while offloading the task by cloudlet to cloud server. The task is decrypted in the cloud server and is computed. Once the process is completed, cloud encrypts using the same Triple DES with 3 different keys to send the results to the cloudlet. AES is used while offloading the task by the mobile device to the cloud server. The task is decrypted in the cloud server and is computed. Once the process is completed, cloud server encrypts using the same AES[16] to send the results to the mobile device.

The power consumption by the mobile device and the completion time are the two important parameters considered in this paper.

Completion time when the task is offloaded from mobile device to cloudlet:

- Time for encrypting the task using Triple DES with 2 different keys in mobile device
- Time to offload the task from mobile device to cloudlet

***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

- Time to decrypt the task using decryption process of Triple DES with 2 different keys in cloudlet.
- Time to process the task in the cloudlet.
- Time for encrypting the task using Triple DES with 2 different keys in cloudlet.
- Time to send the results from cloudlet to mobile device.
- Time to decrypt the task using decryption process of Triple DES with 2 different keys in mobile device.

Completion time when the task is offloaded from cloudlet to cloud server:

- Time for encrypting the task using Triple DES with 3 different keys in mobile device
- Time to offload the task from cloudlet to cloud server
- Time to decrypt the task using decryption process of Triple DES with 3 different keys in cloud server.
- Time to process the task in the cloud server.
- Time for encrypting the task using Triple DES with 3 different keys in cloud server.
- Time to send the results from cloudlet to mobile device.
- Time to decrypt the task using decryption process of Triple DES with 3 different keys in cloudlet.

Completion time when the task is offloaded from mobile device to cloud server:

- Time for encrypting the task using AES in mobile device
- Time to offload the task from mobile device to cloud server
- Time to decrypt the task using decryption process of AES in cloud server.
- Time to process the task in the cloud server.
- Time for encrypting the task using AES in cloud server.
- Time to send the results from cloud server to mobile device.
- Time to decrypt the task using decryption process of AES in mobile device.

IV. RESULTS AND DISCUSSION

The most popular programming language, Python is used for simulating the proposed system, SCM_DTO. The graphs shown in Fig. 2 – Fig. 6 are the results taken as an average of 25 runs of the simulation. The computation time, communication time, average running time and energy of the mobile device are the parameters which are used to evaluate the performance of the proposed algorithm, SCM_DTO.

Computation time: Time taken to divide the task into sub tasks if required + Time taken to compute the task either in the device or any cloud server.

Communication time:

Case 1: Offload task by Mobile device to one of the cloud server directly.

- Time taken to offload the task by mobile device to any cloud server + Time taken to offload the task by cloud server to mobile device.

Case 2: Offload task by Mobile device to one of the cloud server via cloudlet.

- Time taken to offload the task by mobile device to any cloudlet + Time taken to offload the task by cloudlet to cloud server + Time taken to offload the task by cloud server to cloudlet + Time taken to offload the task by cloudlet to mobile device.

Case 3: Offload task by Mobile device to one of the cloudlet

- Time taken to offload the task by mobile device to any cloudlet + Time taken to offload the task by cloudlet to mobile device.

Average Running Time: The time from when the simulation started to the time at which simulation is completed.

Energy Consumption by the mobile device:

- During encryption process of the task using Triple DES with 2 different keys/Triple DES with 3 different keys/AES encryption algorithms
- During offloading process from mobile device to cloudlet or cloud server
- While receiving the results from cloudlet or cloud server
- During decryption process of the results using Triple DES with 2 different keys/Triple DES with 3 different keys/AES encryption algorithms

The performance of the proposed algorithms, SCM_DTO is enhanced when compared to ECDH-SAHE by 15.69%, 23.99%, 15.49%, 63.94%, and 56.2% in terms of computation time, communication time, and average running time, energy of the mobile device for varying data size, and energy of the mobile device for varying number of instructions respectively. The learning automata is used to enhance the performance of the proposed algorithm. In ECDH-SAHE, the data is categorized based on sensitivity and is stored in various cloud servers whereas the proposed

***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

algorithm, SCM_DTO offloads the data to various cloudlets or cloud using various encryption techniques, Triple DES with 2 different keys, Triple DES with 3 different keys or AES.

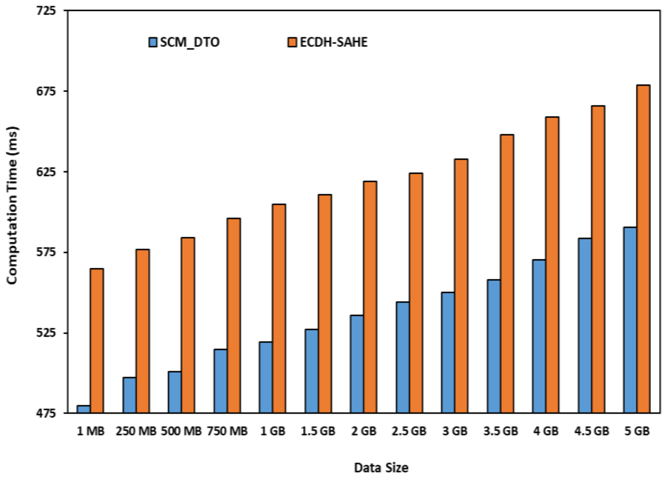

Fig. 2 Computation Time for varying data size

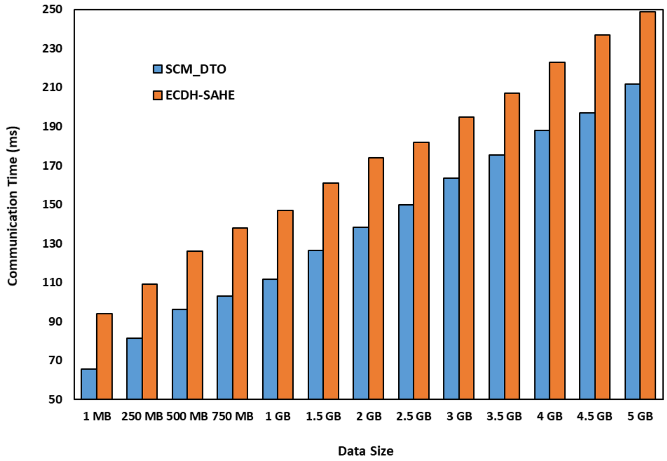

Fig. 3 Communication Time for varying Data Size

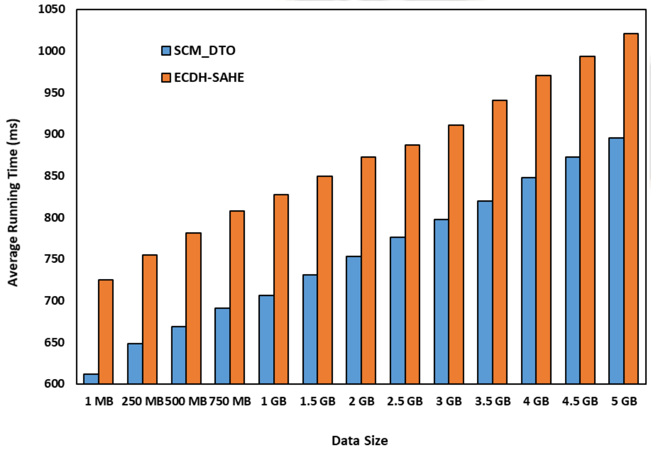

Fig. 4 Average Running Time for varying data size

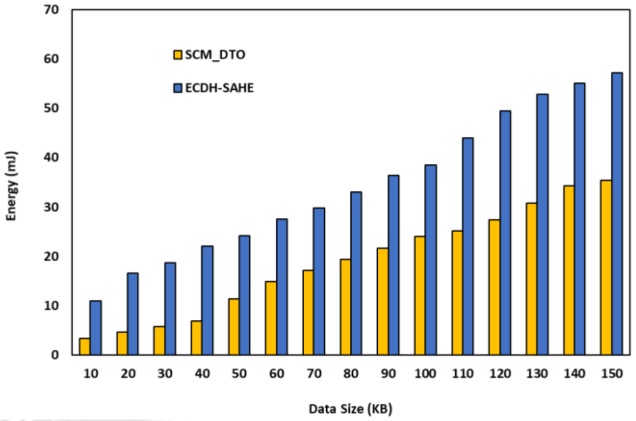

Fig. 5 Energy for varying data size

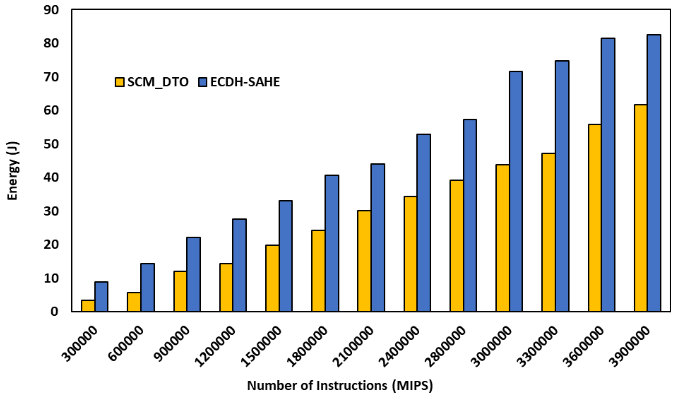

Fig. 6 Energy for varying number of instructions

V. SUMMARY

In this section, a communication model for dynamic task offloading which is secured for multi-cloud environment is proposed. In this model, cloudlets are also involved. Many-to-many communication is maintained among the cloudlets and the cloud servers. The encryption technique used while offloading the tasks to the cloudlet by the mobile device is triple DES with 2 keys. The encryption technique used while offloading the tasks to the cloud server by the cloudlet is triple DES with 3 keys and the encryption technique used while offloading the task to the cloud by the mobile device is AES. The parameters used to test the performance of the simulated version of the proposed algorithm are computation time, communication time, average running time, and energy consumed by the mobile device for varying data size and varying number of instructions. The performance of the proposed algorithm is compared with ECDH-SAHE and is proved to be performing better 15.69%, 23.99%, 15.49%, 63.94%, and 64.18% in terms of computation time, communication time, and average running time, energy of the mobile device for varying data size, and energy of the mobile device for varying number of instructions respectively.

***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

REFERENCES:

[1]. Luo, S., Wen, Y., Xu, W. and Puthal, D., 2019. Adaptive task offloading auction for industrial CPS in mobile edge computing. IEEE Access, 7, pp.169055-169065.

[2]. Ren, J., Li, J., Liu, H. and Qin, T., 2021. Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT. Tsinghua Science and Technology, 27(4), pp.760-776.

[3]. Rahbari, D. and Nickray, M., 2020. Task offloading in mobile fog computing by classification and regression tree. Peer-to-Peer Networking and Applications, 13(1), pp.104-122.

[4]. Jacek Marecki, & Dr. Sunita Chaudhary. (2022). Electrical Structure for Embedded Commuter Vision for Automobile Sector. Acta Energetica, (02), 44–51. Retrieved from http://actaenergetica.org/index.php/journal/article/view/468

[5]. Nguyen, D.C., Pathirana, P.N., Ding, M. and Seneviratne, A., 2020. Privacy-preserved task offloading in mobile blockchain with deep reinforcement learning. IEEE Transactions on Network and Service Management, 17(4), pp.2536-2549.

[6]. Li, Y., Zeng, D., Gu, L., Zhu, A. and Chen, Q., 2020, December. Task offloading in trusted execution environment empowered edge computing. In 2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS) (pp. 316-323). IEEE.

[7]. Gudni Johannesson, & Nazzal Salem. (2022). Design Structure of Compound Semiconductor Devices and Its Applications. Acta Energetica, (02), 28–35. Retrieved from http://actaenergetica.org/index.php/journal/article/view/466

[8]. Kim, S., 2020. New application task offloading algorithms for edge, fog, and cloud computing paradigms. Wireless Communications and Mobile Computing, 2020.

[9]. Qureshi, D. I. ., & Patil, M. S. S. . (2022). Secure Sensor Node-Based Fusion by Authentication Protocol Using Internet of Things and Rfid. Research Journal of Computer Systems and Engineering, 3(1), 48–55. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/41

[10]. Li, J., Dai, M. and Su, Z., 2020. Energy-aware task offloading in the Internet of Things. IEEE Wireless Communications, 27(5), pp.112-117.

[11]. Guo, H., Liu, J., Ren, J. and Zhang, Y., 2020. Intelligent task offloading in vehicular edge computing networks. IEEE Wireless Communications, 27(4), pp.126-132.

[12]. Samad, A. . (2022). Internet of Things Integrated with Blockchain and Artificial Intelligence in Healthcare System. Research Journal of Computer Systems and Engineering, 3(1), 01–06. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/34

[13]. Cozzolino, V., Tonetto, L., Mohan, N., Ding, A.Y. and Ott, J., 2022. Nimbus: Towards Latency-Energy Efficient Task Offloading for AR Services. IEEE Transactions on Cloud Computing.

[14]. Ben Ammar, M., Ben Dhaou, I., El Houssaini, D., Sahnoun, S., Fakhfakh, A. and Kanoun, O., 2022. Requirements for Energy-Harvesting-Driven Edge Devices Using Task-Offloading Approaches. Electronics, 11(3), p.383.

[15]. Maloth, Bhav Singh. (2016). Privacy-Preserving Scalar Product Computation over Personal Health Records. International Journal of Computer Engineering In Research Trends. 3. 42-46.

[16]. Chiba, Z., El Kasmi Alaoui, M. S., Abghour, N., & Moussaid, K. (2022). Automatic Building of a Powerful IDS for The Cloud Based on Deep Neural Network by Using a Novel Combination of Simulated Annealing Algorithm and Improved Self- Adaptive Genetic Algorithm. International Journal of Communication Networks and Information Security (IJCNIS), 14(1). https://doi.org/10.17762/ijcnis.v14i1.5264 (Original work published April 12, 2022)

[17]. (2022). Bug2 algorithm-based data fusion using mobile element for IoT-enabled wireless sensor networks. Measurement: Sensors. 100548. 10.1016/j.measen.2022.100548.

[18]. Roy, S. S., Mallik, A., Gulati, R., Obaidat, M. S., & Krishna, P. V. (2017, January). A deep learning based artificial neural network approach for intrusion detection. In *International Conference on Mathematics and Computing* (pp. 44-53). Springer, Singapore

[19]. Abouhogail, R. A. (2022). Untraceable Authentication Protocol for IEEE802.11s Standard. International Journal of Communication Networks and Information Security (IJCNIS), 13(3). https://doi.org/10.17762/ijcnis.v13i3.5090 (Original work published December 25, 2021)

[20]. Viswanathan, P., & Krishna, P. V. (2013). A joint FED watermarking system using spatial fusion for verifying the security issues of teleradiology. *IEEE Journal of Biomedical and Health Informatics*, *18*(3), 753-764.

[21]. Maloth, Bhav Singh & Lakshmi, M & Kumar, Dr & Parashuram, N. (2017). International Journal on Recent and Innovation Trends in Computing and Communication Improved Trial Division Algorithm by Lagrange"s Interpolation Function. International Journal on Recent and Innovation Trends in Computing and Communication. 5. 1227-1231.

[22]. Maloth, Bhav Singh & Anusha, R. & Reddy, R. & Devi, S.Chaya. (2013). Augmentation of Information Security by Cryptography in Cloud Computing. www.ijcst.com. 4.