


# Secured and Privacy-Based IDS for Healthcare Systems on E-Medical Data Using Machine Learning Approach

Sudhakar Sengan, PSN College of Engineering and Technology, India

 <https://orcid.org/0000-0003-4901-1432>

Osamah Ibrahim Khalaf, Al-Nahrain University, Iraq

Vidya Sagar P., Koneru Lakshmaiah Education Foundation, India

Dilip Kumar Sharma, Jaypee University of Engineering and Technology, India

Arokia Jesu Prabhu L., CMR Institute of Technology, India

Abdulsattar Abdullah Hamad, Tikrit University, Iraq

## ABSTRACT

Existing methods use static path identifiers, making it easy for attackers to conduct DDoS flooding attacks. This article creates a system using dynamic secure aware routing by machine learning (DAR-ML) to solve healthcare data. A DoS detection system by ML algorithm is proposed in this paper. First, one needs to access the user to see the authorized process. Next, after the user registration, users can compare path information through correlation factors between nodes. Then, they choose the device that will automatically activate and decrypt the data key. The DAR-ML is traced back to all healthcare data in the end module. In the next module, the users and admin can describe the results. These are the outcomes of using the network to make it easy. Through a time interval of 21.19% of data traffic, the findings demonstrate an attack detection accuracy of over 98.19%, with high precision and a probability of false alarm.

## KEYWORDS

DDoS, Healthcare Records, IDS, Inter-Domain Routing, Path Identifiers, Security

## INTRODUCTION

Today's network world is packed with harmful attacks, hacks, crackers, and fraudsters. The most critical aspects of data communication protection are verification, authorization, and auditing (Abdulsahib & Khalaf, 2018). Otherwise, an authentication scheme fails to achieve its primary objective of providing sufficient protection for its developed prototype. As information technology takes over the globe, security has become an inextricable problem (Abdulsahib & Khalaf, 2021). More knowledge is distributed to all parts of the globe from everywhere across the internet due to the remarkably rapid development of different Internet technology types (Alkhafaji et al., 2021). Any device sent across the World wide web could contain sensitive information, and in those instances, the sender and receiver must recognize information security issues before enjoying the ease and efficiency that no other medium can cover (Al-Khanak et al., 2021). Intrusion Detection Systems (IDS) (Ayman

DOI: 10.4018/IJRQEH.289175

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

Dawood et al., 2019), also identified as Intrusion Detection and Prevention Systems, are network appliances that record malicious behavior, record information about it, take action to stop it, and then report it. Intrusion detection systems will notify you if your network is being managed to hack, drop packets, and reconfigure the link to prohibit the client's IP from being blacklisted (Carlos et al., 2021). A robust network protection framework can assist businesses in reducing the risk of data theft and disruption. Network protection helps prevent malicious spyware in your workstations. It also guarantees the privacy of shared knowledge (Dalal & Khalaf, 2021). Massive traffic will wreak havoc on the system's stability and expose vulnerabilities (Duan & Chandrashekar, 2008) (Ferguspon & Senie, 2000).

## **RELATED WORKS**

The technique used divide anomaly-based IDS into the motivation: statistical, supervised, unattended, clustering, soft computing, knowledge-based, and a combination of learners [4]. This research relies on unsupervised, hybrid systems and presents a comprehensive overview of the procedures requiring supervision (Hamad et al., 2021). IDS is tracking and searching for symbols of likely occurrences that intrude on information security, information protection laws, and conventional security procedures in a configured computer network (Hoang et al., 2021). Activities contain a combination of factors that cause, like malware, unauthorized Internet connectivity to system hackers, and authorized network operators endeavoring to misappropriate their protections or add other rights that they are not approved for. A software that optimizes the intrusion prevention process is an IDS (Jebril, 2021).

Although many alternatives for particular Botnet attacks have also been proposed, a practical approach that is not limited to any specific attacks remains uncommon. We are breaking away from such an alternative from related research classes: genetic, behavioral techniques to detect Botnet viruses and vulnerability scanning of Markov chains and Hidden Models (Keerthana et al. 2020; Khalaf & Abdulsahib, 2021).

In IDS and anomaly detection research in the past, Markov models have been used. An overview of Markov's chain-based IDS is discovered in which a flow of audit process occurrences is used to train a Markov chain; hosts created event streams are being screened for model similarity and are categorized as attack flows; they are like the framework (Khalaf & Abdulsahib 2019). These frameworks enable us to identify an attack but not predict, and Markov chains have not been used to predict known susceptible machines' behavior to our correct knowledge (Khalaf & Sabbar 2019; Krichen et al., 2021; Li et al., 2021).

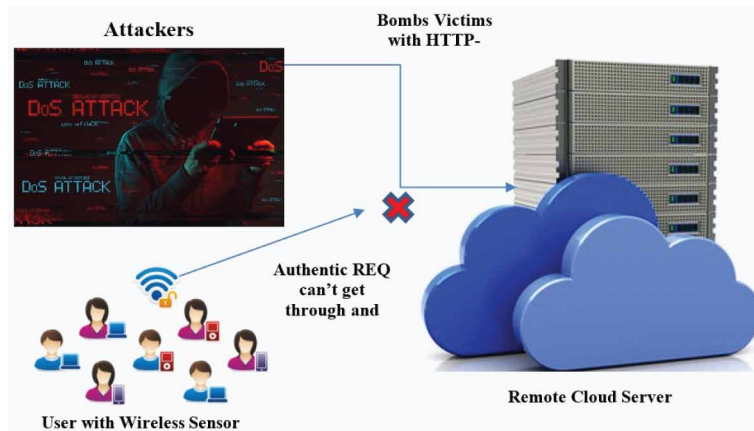
Network Intrusion Detection Systems (NIDS) (Ogudo et al., 2019) have destroyed security optimization algorithms in recent decades. The model Markov has no after-effect asset and is only linked to its previous condition probability. It effectively predicts the massively different random process, as they continue to follow the transmitter probability matrix is assumed between States (Park & Lee, 2001). The transfer probability index is obtained using a statistical method, and the evaluation is used to approximate the probabilistic model (Prasad et al., 2020). Therefore, the Markov model is best suited for the predictive security model in large data samples in communication systems. A validation procedure of Markov includes Bernoulli, Wiener, and Poisson processes (Priyadarshini & Sudhakar (2015). Markov process can be divided into three categories based on continuous or discontinuous state and time parameter: (1) the Markov discretionary process of the Markov chain; (2) the Markov Chain of Consistent and Distinct time; and (3) the constant Markov time chain process of the time domain (Rajasoundaran et al., 2021) (Romero et al., 2021) (Sengan, S et al., 2021).

## **IMPLEMENTATION**

The process of identifying improper, inaccurate, or anomaly behavior is known as DPS-ML. It also assesses irregular behavior in the company's network (Subahi et al., 2020) (Sudhakar & Chenthur

Pandian, 2016). The method of accurately identifying unwanted or suspicious behavior on a device is known as intrusion detection. External attackers aren't assumed to be on the devices they're assaulting. Ongoing hackers have limited access to the device. Inner offenders have been further categorized, and that those who pose like someone else have valid access to personal information, and the most dangerous category, covert intruders who can disable audit control for them (Figure 1).

Figure 1. DDoS attack



## SYSTEM ARCHITECTURE

It's challenging to track down the origins of Denial of Service (DDoS) attacks on the internet. One of the most challenging aspects of tracking down DDoS attacks is that attackers send a request packet to victims via infected systems (zombies) in denying or degrade the service quality. According to a recent study, more than 70 internet operators worldwide have shown that DDoS attacks are rising, with single attacks becoming more challenging and complex. IP traceback relates to the capability to establish the origin of any packets sent over the internet; IP traceback strategies may be used to locate the zombies from which DDoS attack packets were sent (Suleiman et al., 2014; Trn et al., 2021; Wang et al., 2021).

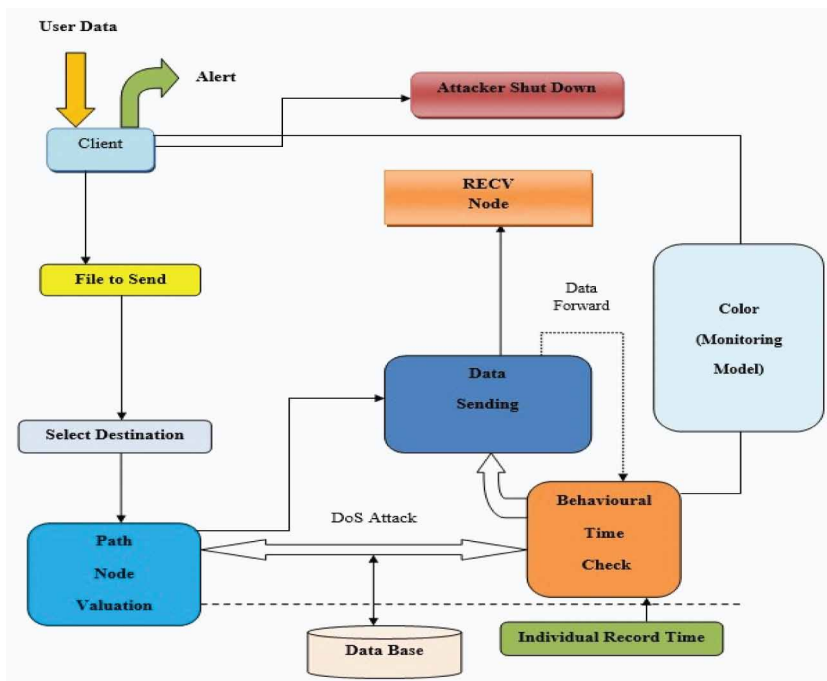
To detect aggressors, a variety of IP traceback methods have been proposed. Probabilistic Packet Marking (PPM) and Deterministic Packet Marking (DPM) are primary methods for tracing IP addresses back (DDPM). These cases necessitate the insertion of markings into individual packets by routers. It also has some disadvantages, such as scalability, high storage requirements, and packet trash susceptibility. Both PPM and DPM involve replicating the current routing program, which is incredibly difficult to achieve. We may prevent packet marking frameworks' inherited flaws by using IP traceback with information-theoretical limits and the number of packets marking in the recommended system (Wisesa et al., 2020) (Xiang et al. 2021; Yaar et al., 2006). The upstream access point through which the packet is introduced, and the packet's target node is used to group packets moving through a wireless connection into flow conditions (Figure 2).

Routers are allowed to collect and monitor information variations of localized flows throughout non-attack times. You can use the terms information difference and entropy distinction synonymously. If a DDoS alarm is triggered, the defendant uses the significant backlash process proposed to discover robots.

## PROPOSED SYSTEM

The design, development, and analysis of the current HMM-based behavioral angle architectural design classify attacks. A substitute method to measuring the based on behavioral distance based on the novel Hidden Markov Model (HMM). A probably equally stochastic procedure is explained by an HMM, in which one differential equation is not measurable but impacts another that generates a sequence of measurable symbols (Zhao et al., 2020; Zheng et al., 2021). The signals detected in machine learning activity distance are process conduct, and the secret conditions are processing tasks performed. Because these secret activities will be identical, it should be possible to compare the two methods' similar visible behavior patterns while no attack is fully operational and recognize a highly social gap when either is successfully attacked. Unlike conventional anomaly detection, which uses a singular HMM to design a single process, our technique utilizes a specific HMM to develop both programs simultaneously. The benefits are: (a) Speedy authentication, (b) No abuser defacing, (c) Protection of the data packet and retention of domain consistency, (d) Simple abusers are stopped, and the alarm is increased, (e) Trace backup helps avoid malicious activity.

Figure 2. System achitecture



## METHODOLOGY

1. **Node Verification:** This module includes the authentication methods of the user and the administrator. The administrator has the authorization to view all processes performed by the user. The user can only access the authorized procedure after the method has been recorded. The

user can access his private details and user data. You can access and start the server to receive data in the server module with a static and stable login.

2. **Path Node Association:** Workgroups split the network. This framework allows us to reach the network's linked and working systems. This part will receive the connected systems and display the users after logging into our process. The user may pick the device to supply its data by transferring files. Disconnected and termination systems are not identified. Users can then equate the path info with node correlation factors. Each node updates its correlation table and circulates the entire system.
3. **Data Allocation:** The user must pick the data transmission device and the transfer file. Selected encryption is done for safe transmission. When data obtained by the chosen destination path, the key instantly activated and decrypted. The stub monitoring will start automatically when the user begins to find behavioral and evolutionary distances.
4. **Monitoring and Authentication:** We must keep track of the client data sent to the recipient along a specific route in our method. Reports are useless until the attacker has tampered with the current information. As a result, we're tracing the history of each piece of information. Finding path differences can be as easy as tracing the information path from one side to another. The Tracking Stub will inform the client that the data information path becomes different from the anticipated pathways by evaluating distance and time intervals.
5. **Admin and Information:** The admin receives all transaction records and attacker data. The administrator has access to all documents and can keep track of the network routes. The administrator is in charge of the entire data history. As a result, the administrator can disable the intruder's service from the report's module.
6. **Security and Privacy:** Services that use Wireless sensor e-Health systems would have to be fully aware of their inherent security risks, and they must consciously design privacy and security designs to protect networks. All security flaws and attack trajectories must be deemed for each system layer, and all security requirements must be addressed efficiently and effectively. Many health professionals and healthcare providers prefer to store medical records on computing devices or information systems and information that are not connected to the Web, aware of the privacy concerns. Health record exchange necessarily requires the formation of services and infrastructure that enable health care providers to transfer clinical security measures to protect patient security and privacy.
7. **Privacy Awareness:** To inform the public about privacy risks or raise awareness, privacy awareness metrics can be integrated into a particular platform. The data security warnings help raise awareness of potential security risks. Privacy awareness devices and services are progressively required to adhere to defined processes such as laws, regulatory requirements, ethical requirements, and enterprise standard operating procedures. Abstract Private Information Lifecycle designs, for example, aid in the authentication of personal data. Furthermore, the patterns of expert knowledge were proposed, and predefined solutions for fulfilling various types of private information were presented. The described pattern is used as part of a standard privacy-aware system design methodology. The author examined how a set of privacy policies and procedures can successfully optimize the effectiveness of an IoT application. They combined the method to apply to the approach for privacy by design and IoT applications. Their method has always been aimed at addressing IoT challenges, and it varies considerably from conventional private information by assigned works.

## RESULTS AND DISCUSSION

This article introduces DAR, our findings, and analysis predicated on the training data set and ML methods successfully implemented. Training datasets are read, stored in a data frame, and transformed into a matrix during the classification phase. Furthermore, these datasets are divided into training and

testing (Figure 3). The training dataset includes 20,000 peaceful data transfers and 21,500 malicious activity transactions, while the training dataset incorporates 10050 benign network transactions and 11,500 potential malicious operations (Figure 4). We detect and analyze the effectiveness of the proposed detection technique against DoS attacks on Wireless systems (Figure 5).

Figure 3. User login page

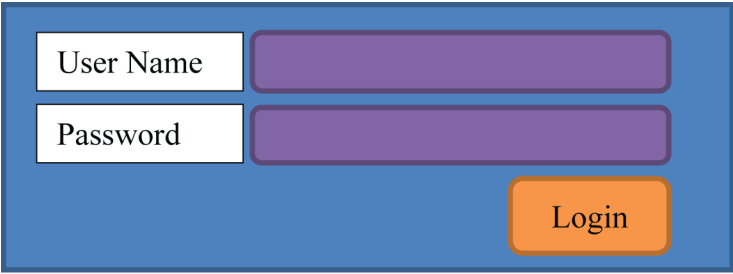


Figure 4. IDS monitoring

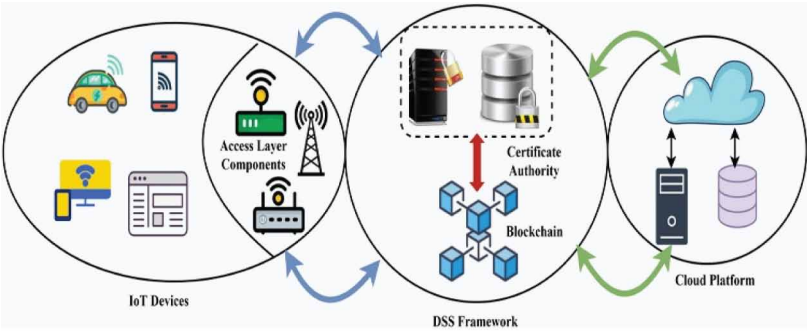
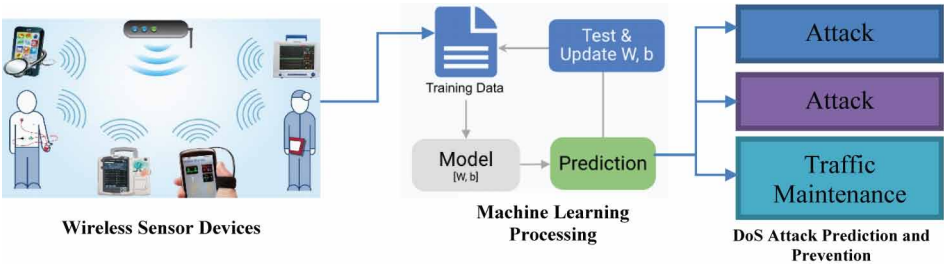


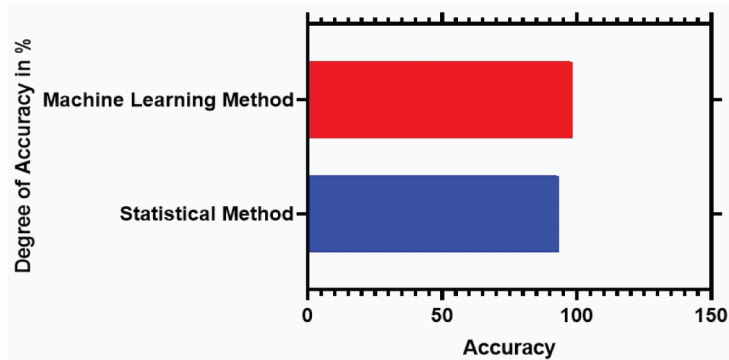
Figure 5. Intruder Detection Data Processing



## Investigate Statistical and Machine Learning Algorithms

We evaluated the performance of our DAR-ML technique to the result found through the statistical method in this portion. Researchers can conclude the report's analysis that the recommended detection system can detect DDoS attacks with a greater degree of accuracy when applied using an ML approach (Figure 6).

Figure 6. Performance analysis of intrusion by ml algorithms



Researchers explored the optimum approach for DAR-ML-based IDS by evaluating our scheme's achievement against multiple known attacks, such as DDoS attacks. We obtained an average Precision of 94.67% and a Recall of 96.19% for multiple attack situations by examining precision-recall curves.

## CONCLUSION AND FUTURE WORK

Integration and analysis of DAR-ML, a mechanism that increased awareness of inter-domain route path identifiers to avoid DoS attack when DAR-ML is used as inter-domain routing items. The technical specifications of DAR-ML have been described and implemented in a 50 nodes model to validate its functionality and performance. It showed quantitative examples from operating prototype experiments. The results indicate that the time it takes to negotiate, DAR-ML is comparatively low (ms), and DAR-ML avoids DoS attacks. The results indicate that the costs of starting the DoS attacks are significantly increased because DAR-ML does not have much overhead since the additional number of GET message is insignificant when the transmission time is 300 sec., and the DAR-ML update rate is considerably lower than the current IP prefix rate on the Web. The latter technology enables our system to differentiate visible and invisible DoS attacks from authorized internet traffic.

Review of DDoS attacks QoS security issues such as Heartbleed and web brute force, improvement of multiple-class sorting, self-configuration of the device, creating approaches for associating activated alarm schemes, and designing protection devices for future work.

## REFERENCES

- Abdulsahib, G. M., & Khalaf, O. I. (2018). Comparison and Evaluation of Cloud Processing Models in Cloud-Based Networks. *International Journal of Simulation-Systems, Science & Technology*, 19(5).
- Abdulsahib, G. M., & Khalaf, O. I. (2018). An Improved Algorithm to Fire Detection in Forest by Using Wireless Sensor Networks. *International Journal of Civil Engineering and Technology*, 9(11), 369–377.
- Abdulsahib, G. M., & Khalaf, O. I. (2021). Accurate and Effective Data Collection with Minimum Energy Path Selection in Wireless Sensor Networks using Mobile Sinks. *Journal of Information Technology Management*, 13(2), 139–153.
- Abdulsahib, G.M., & Khalaf, O.I. (2021). An Improved Cross-Layer Proactive Congestion in Wireless Networks. *International Journal of Advances in Soft Computing and its Applications*, 13(1), 178–192.
- Al-Khanak, E. N., Lee, S. P., Khan, S. U. R., Behboodan, N., Khala, O. I., Verbraeck, A., & van Lint, J. W. C. (2021). A Heuristics-Based Cost Model for Scientific Workflow Scheduling in Cloud. *CMC Computer. Materials and Continua*, 67(3), 3265–3282. doi:10.32604/cmc.2021.015409
- Alkhafaji, A. A., Sjarif, N. N. A., Shahidan, M. A., Azmi, N. F. M., Sarkan, H. M., Chuprat, S., & Al-Khanak, E. N. (2021). Payload Capacity Scheme for Quran Text Watermarking Based on Vowels with Kashida. *CMC Computer, Materials and Continua*, 67(3).
- Dalal, S., & Khalaf, O. I. (2021). Prediction of Occupation Stress by Implementing Convolutional Neural Network Techniques. *Journal of Cases on Information Technology*, 23(3), 27–42. doi:10.4018/JCIT.20210701.oa3
- Dawood, A., Salman, O. I. K., & Muttashar, G. (2019). An adaptive intelligent alarm system for wireless sensor network. *Indonesian Journal of Electrical Engineering and Computer Science*, 15(1), 142–147. doi:10.11591/ijeecs.v15.i1.pp142-147
- Duan, X. Y., & Chandrashekar, J. (2008). Controlling IP spoofing through interdomain packet filers. *IEEE Trans. Depend. Sec. Comput.*, 5(1), 22–35.
- Ferguspon, P., & Senie, D. (2000). Network Image filtering: Defeating denial of service attacks that employ IP source address spoofing. *IETF RFC* 2827.
- Hamad, A. A., Al-Obeidi, A. S., Al-Ta'iy, E. H., Khalaf, O. I., & Le, D. (2021). Synchronization phenomena investigation of a new nonlinear dynamical system 4d by gardano's and lyapunov's methods, *Computers. Materials & Continua*, 66(3), 3311–3327. doi:10.32604/cmc.2021.013395
- Hoang, A. T., Nguyen, X. P., Khalaf, O. I., Tran, T. X., Chau, M. Q., Dong, T. M. H., & Nguyen, D. N. (2021). Thermodynamic Simulation on the Change in Phase for Carburizing Process. *CMC-Computers Materials & Continua*, 68(1), 1129–1145. doi:10.32604/cmc.2021.015349
- Jebril, I. H. (2021). User Satisfaction of Electric-Vehicles About Charging Stations (Home, Outdoor, and Workplace). *Turkish Journal of Computer and Mathematics Education*, 12(3), 3589–3593.
- Keerthana, N., Viji, V., & Sudhakar, S. (2020). A Novel Method for Multi-Dimensional Cluster to Identify the Malicious Users on Online Social Networks. *Journal of Engineering Science and Technology*, 15(6), 4107–4122.
- Khalaf, O. I., & Abdulsahib, G. M. (2019). Frequency estimation by the method of minimum mean squared error and P-value distributed in the wireless sensor network. *Journal of Information Science and Engineering*, 35(5), 1099–1112.
- Khalaf, O. I., & Abdulsahib, G. M. (2021). Optimized dynamic storage of data (ODSD) in IoT based on blockchain for wireless sensor networks. *Peer-to-Peer Networking and Applications*, 1–16.
- Khalaf, O. I., Abdulsahib, G. M., Kasmaei, H. D., & Ogudo, K. A. (2020). A new algorithm on application of blockchain technology in live stream video transmissions and telecommunications. *International Journal of e-Collaboration*, 16(1), 16–32. doi:10.4018/IJeC.2020010102
- Khalaf, O. I., Abdulsahib, G. M., & Sabbar, B. M. (2020). Optimization of Wireless Sensor Network Coverage using the Bee Algorithm. *Journal of Information Science and Engineering*, 36(2), 377–386.

- Khalaf, O. I., Abdulsahib, G. M., & Sadik, M. (2018). A Modified Algorithm for Improving Lifetime WSN. *Journal of Engineering and Applied Sciences (Asian Research Publishing Network)*, 13, 9277–9282.
- Khalaf, O. I., Ajesh, F., Hamad, A. A., Nguyen, G. N., & Le, D. N. (2020). Efficient Dual-Cooperative Bait Detection Scheme for Collaborative Attackers on Mobile Ad-hoc Networks. *IEEE Access: Practical Innovations, Open Solutions*, 8, 227962–227969. doi:10.1109/ACCESS.2020.3045004
- Khalaf, O. I., Ogudo, K. A., & Singh, M. (2021). A Fuzzy-Based Optimization Technique for the Energy and Spectrum Efficiencies Trade-Off in Cognitive Radio-Enabled 5G Network. *Symmetry*, 13(1), 47. doi:10.3390/sym13010047
- Khalaf, O. I., & Sabbar, B. M. (2019). An overview on wireless sensor networks and finding optimal location of nodes. *Periodicals of Engineering and Natural Sciences*, 7(3), 1096–1101. doi:10.21533/pen.v7i3.645
- Krichen, M., Mechti, S., Alrooba, R., Said, E., Singh, P., Ibrahim Khalaf, O., & Masud, M. (2021). A formal testing model for operating room control system using internet of things, *Computers. Materials & Continua*, 66(3), 2997–3011. doi:10.32604/cmc.2021.014090
- Krichen, M., Mechti, S., Alrooba, R., Said, E., & Singh, P. (2021). A formal testing model for operating room control system using internet of things. *Computers, Materials & Continua*, 66(3), 2997–3011. doi:10.32604/cmc.2021.014090
- Li, G., Liu, F., Sharma, A., Khalaf, O. I., Alotaibi, Y., Alsufyani, A., & Alghamdi, S. (2021). Research on the Natural Language Recognition Method Based on Cluster Analysis Using Neural Network. *Mathematical Problems in Engineering*.
- Ogudo, K. A., Muwawa Jean Nestor, D., Ibrahim Khalaf, O., & Daei Kasmaei, H. (2019). A device performance and data analytics concept for smartphones' IoT services and machine-type communication in cellular networks. *Symmetry*, 11(4), 593–609. doi:10.3390/sym11040593
- Osamh & Abdulsahib. (2020). Energy-Efficient Routing and Reliable Data Transmission Protocol in WSN. *International Journal of Advances in Soft Computing and its Application*, 12(3), 45-53.
- Park, K., & Lee, H. (2001). On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets. *ACM SIGCOMM Comput. Commun. Rev.*, 31(4), 15–26. doi:10.1145/964723.383061
- Prasad, S. K., Rachna, J., Khalaf, O. I., & Le, D.-N. (2020). Map matching algorithm: Real-time location tracking for smart security application. *Telecommunications and Radio Engineering*, 79(13), 1189–1203. doi:10.1615/TelecomRadEng.v79.i13.80
- Priyadarshini, A. U., & Sudhakar, S. (2015). Cluster-Based Certificate Revocation by Cluster Head in Mobile Ad Hoc Network. *International Journal of Applied Engineering Research: IJAER*, 10(20), 1604–16018.
- Rajasoundaran, S., Prabu, A. V., Subrahmanyam, J. B. V., Rajendran, R., Kumar, G. S., Kiran, S., & Khalaf, O. I. (2021). Secure watchdog selection using intelligent key management in wireless sensor networks. *Materials Today: Proceedings*. Advance online publication. doi:10.1016/j.matpr.2020.12.1027
- Romero, C. A. T., Castro, D. F., Ortiz, J. H., Khalaf, O. I., & Vargas, M. A. (2021). Synergy between Circular Economy and Industry 4.0: A Literature Review. *Sustainability*, 13(8), 4331. doi:10.3390/su13084331
- Romero, C. A. T., Ortiz, J. H., Khalaf, O. I., & Prado, A. R. (2021). Web application commercial design for financial entities based on business intelligence. *CMC-Computers Materials & Continua*, 67(3), 3177–3188. doi:10.32604/cmc.2021.014738
- Sengan, S., Rao, G. R. K., Khalaf, O. I., & Babu, M. R. (2021). Markov mathematical analysis for comprehensive real-time data-driven in healthcare. *Mathematics in Engineering, Science & Aerospace (MESA)*, 12(1).
- Sengan, S., Sagar, R. V., Ramesh, R., Khalaf, O. I., & Dhanapal, R. (2021). The optimization of reconfigured real-time datasets for improving classification performance of machine learning algorithms. *Mathematics in Engineering, Science & Aerospace (MESA)*, 12(1).
- Subahi, A. F., Alotaibi, Y., Khalaf, O. I., & Ajesh, F. (2020). Packet drop battling mechanism for energy-aware detection in wireless networks. *Computers, Materials and Continua*, 66(2), 2077–2086. doi:10.32604/cmc.2020.014094

Sudhakar, S. (2012). Secure Packer Encryption and Key Exchange System in Mobile Ad hoc Network. *Journal of Computational Science*, 8(6), 908–912. doi:10.3844/jcssp.2012.908.912

Sudhakar, S., & Chenthur Pandian, S. (2016). Hybrid Cluster-based Geographical Routing Protocol to Mitigate Malicious Nodes in Mobile Ad Hoc Network. *International Journal of Ad Hoc and Ubiquitous Computing*, 21(4), 224–236. doi:10.1504/IJAHUC.2016.076358

Suleiman, N., Abdulsahib, G., Khalaf, O., & Mohammed, M. N. (2014). Effect of Using Different Propagations of OLSR and DSDV Routing Protocols. *Proceedings of the IEEE International Conference on Intelligent Systems Structuring and Simulation*, 540–545. doi:10.1109/ISMS.2014.99

Tavera, C. A., Ortiz, J. H., Khalaf, O. I., Saavedra, D. F., & Aldhyani, T. H. H. (2021). Wearable Wireless Body Area Networks for Medical Applications. *Computational and Mathematical Methods in Medicine*, 2021, 1–9. doi:10.1155/2021/5574376 PMID:33986824

Tran, T. X., Nguyen, X. P., Nguyen, D. N., Vu, D. T., Chau, M. Q., Khalaf, O. I., & Hoang, A. T. (2021). Effect of poly-alkylene-glycol quenchant on the distortion, hardness, and microstructure of 65Mn steel. *CMC-Computers Materials & Continua*, 67(3), 3249–3264. doi:10.1109/ISMS.2014.99

Wang, X., Liu, J., Khalaf, O. I., & Liu, Z. (2021). Remote Sensing Monitoring Method Based on BDS-Based Maritime Joint Positioning Model. *CMES-Computer Modeling in Engineering & Sciences*, 127(2), 801–818. doi:10.32604/cmes.2021.013568

Wisesa, O., Adriansyah, A., & Khalaf, O. I. (2020). Prediction Analysis Sales for Corporate Services Telecommunications Company using Gradient Boost Algorithm. *2nd International Conference on Broadband Communications, Wireless Sensors and Powering, BCWSP*, 101–106.

Wisesa, O., Andriansyah, A., & Khalaf, O. I. (2020). Prediction Analysis for Business To Business (B2B) Sales of Telecommunication Services using Machine Learning Techniques. *Majlesi Journal of Electrical Engineering*, 14(4), 145–153. doi:10.29252/mjee.14.4.145

Xiang, X., Li, Q., Khan, S., & Khalaf, O. I. (2021). Urban water resource management for sustainable environment planning using artificial intelligence techniques. *Environmental Impact Assessment Review*, 86, 106515. doi:10.1016/j.eiar.2020.106515

Yaar, A. P., & Song, D. (2006). StackPi.: New packet marking and filtering mechanisms for DDoS and IP spoofing defense. *IEEE J. Sel. Areas Commun.*, 24(10), 1853–1863.

Zhao, H., Chen, P. L., Khan, S., & Khalafe, O. I. (2020). Research on the optimization of the management process on internet of things (IoT) for electronic market. *The Electronic Library*. Advance online publication. doi:10.1108/EL-07-2020-0206

Zheng, X., Ping, F., Pu, Y., Montenegro-Marin, C. E., & Khalaf, O. I. (2021). Recognize and regulate the importance of work-place emotions based on organizational adaptive emotion control. *Aggression and Violent Behavior*, 101557. doi:10.1016/j.avb.2021.101557

*Sudhakar Sengan is presently working as Professor and Director International Relation, Department of Computer Science and Engineering, PSN College of Engineering and Technology (Autonomous), Tirunelveli-627152, Tamil Nadu, India. He is received PhD degree in Information and Communication Engineering from Anna University, Chennai, Tamil Nadu, India. And received his ME degree in the Faculty of Computer Science and Engineering from Anna University, Chennai, Tamil Nadu, India, in 2007. He is presently working as Professor and Director International Relation, Department of Computer Science and Engineering, PSN College of Engineering and Technology (Autonomous), Tirunelveli-627152, Tamil Nadu, India. He has 20 years of Experience in Teaching / Research / Industry. He has published papers in 100 International Journals, 20 International Conferences and 10 National Conferences. His research interest includes Network Security, Information Security and Mobile Ad Hoc Network. He has filled 18 Indian and 3 International Patents in various field of interest. He is a member of different professional bodies like MISTE, MIEEE, MIAENG, MIACSIT, MICST, MIE and MIEDRC. He guided more than 100 Projects for UG & PG students in engineering streams. He is the Recognized Research Supervisor at Anna University under the faculty of Information and Communication Engineering. He received an Honorary Doctorate award (Doctor of Letters-D.LITT.) from International Economics University; SAARC Countries in Education and Students Empowerment in April 2017. He is currently guiding many research scholars in various Universities. He delivered Guest Lectures at Various Autonomous Institutions and Universities. He is Doctoral Committee Member for many scholars in reputed Universities. He has published 3 Textbooks for Anna University, Chennai Syllabus.*

*Osamah Ibrahim Khalaf is Senior Engineering and Telecommunications Lecturer in Al-Nahrain University. He has hold 17 years of university-level teaching experience in computer science and network technology and has a strong CV about research activities in computer science and information technology projects. He has had many published articles indexed in (ISI/Thomson Reuters) and has also participated and presented at numerous international conferences. He has a patent and has received several medals and awards due to his innovative work and research activities. He has good skills in software engineering, including experience with .Net, SQL development, database management, mobile applications design, mobile techniques, Java development, android development, and IOS mobile development, Cloud system and computations, website design. I am Editor in Chief and main guest editor in many Scopus and SCI index journals. His brilliant personal Strengths are in highly self-motivated team player who can work independently with minimum supervision, strong leadership skills, and an outgoing personality. He got his B.Sc. in the software engineering field from Al Rafidain University College in Iraq. Then he got his M. Sc. in the computer engineering field from Belarussian National Technical University. After that, he got his PhD in computer networks from the faculty of computer systems & software engineering at -University of Malaysia, Pahang. He has overseas Work experiences at University in Binary University in Malaysia and University Malaysia Pahang.*

*P.Vidya Sagar is an Indian academician who is serving as an Associate Professor in the Department of Computer Science & Engineering in KL University Vijayawada, Andhra Pradesh, India. He got the Ph.D. (Computer Science & Technology) from Sri Krishnadevaya University, Andhra Pradesh, India, in 2016. M.Tech. (Computer Science & Engineering) from Acharya Nagarjuna University, Andhra Pradesh, India, 2010. The major domain/specialization of doctorate is Software Engineering application with Deep Learning, Image processing, Data Mining and Networking. I had around 10 yrs of IT industrial experience with major MNC's & I am currently acting as a reviewer/editorial member if international journals and organising members for international conferences.*

*Dilip Kumar Sharma is presently working in Department of Mathematics, Jaypee University of Engineering and Technology, Guna (M.P.), India. He did his M.Sc.(Mathematics) from Government PG College Guna (M.P.) in the year 1998 and M.Tech. (Future studies and planning) from School of Future studies and planning, Devi Ahilya University Indore (M.P.) in the year 2002. He did his Ph.D. from JUIT Wakanaghat, Solan (H.P.) in the year 2009. He has about 16 years teaching experience. He is Senior member of IEEE, Bombay Section. He is life member of Forum for Interdisciplinary Mathematics (FIM) and Indian Science Congress. He has published many research papers in reputed international journals and presented research papers in Conferences. He has visited NUS Singapore and Concordia University, Montreal, Canada. He is also a member of editorial board of the JUET Research Journal of Science and Technology. He has supervised 3 Ph.D. scholars and one post-Doctoral fellow sponsored by NBHM, DAE, Mumbai and he is currently supervising two Ph.D. scholars.*

*L.Arokia Jesu Prabhu working as Associate Professor, Department of Computer Science and Engineering, CMR Institute of Technology, Hyderabad, India. He has a total of 12 years of experience in teaching and research. He has obtained his Doctoral of Philosophy (Ph.D.) from Anna University, Chennai in the year 2020. His-areas of research are Medical Imaging, Cloud and IOT. He has published several papers in national and international refereed journals and conferences. He is a life member of professional organizations such as CSTA and IAENG.*