An Edge – IoT Framework and Prototype based on Blockchain for Smart Healthcare Applications

Naif Khalaf Al-Shammari
Department of Mechanical Engineering
College of Engineering
University of Ha'il
Ha'il, Saudi Arabia
naif.alshammarif@uoh.edu.sa

Thouheed Ahmed Syed
School of Computing and
Information Technology
REVA University
Bangalore, Karnataka, India
syedthouheed.ahmed@reva.edu.in

Muzamil Basha Syed
School of Computer Science and Engineering
REVA University
Bangaluru, Karnataka, India
muzamilbasha.s@reva.edu.in

Abstract-The Internet of Things (IoT) and the integration of medical devices perform hand-to-hand solutions and comfort to their users. With the inclusion of IoT under medical devices a hybrid (IoMT) is formulated. This features integrated computation and processing of data via dedicated servers. The IoMT is supported with an edge server to assure the mobility of data and information. The backdrop of IoT is a networking framework and hence, the security of such devices under IoT and IoMT is at risk. In this article, a framework and prototype for secure healthcare application processing via blockchain are proposed. The proposed technique uses an optimized Crow search algorithm for intrusion detection and tampering of data extraction in IoT environment. The technique is processed under deep convolution neural networks for comparative analysis and coordination of data security elements. The technique has successfully extracted the instruction detection from un-peer source with a source validation of 100 IoT nodes under initial intervals of 25 nodes based on block access time, block creation, and IPFS storage layer extraction. The proposed technique has a recorded performance efficiency of 92.3%, comparable to trivial intrusion detection techniques under Deep Neural Networks (DNN) supported algorithms.

Keywords-blockchain; intrusion detection; deep neural networking; IoMT; IoT

I. Introduction

Modern day medical infrastructure is expanding with the help of innovative technologies and engineering, such as the Internet on Things (IoT). IoT supports multiple fronts with incorporation on various devices and networking configurations. The IoT enables users to connect and coordinate applications and services via demand-driven configurations. With a series of newer expansions, the IoT has emerged with a new dimension of device configurations under medical applications, termed as Internet of Medical Things (IoMT). The IoMT assures the data are secure and have a defied priority of operation under third party service channels, since the channel of communication is bound to operate under the standard operation policies. The IoMT faces due to security and application concerns on internet-based connectivity. Intrusion detection and managing plays a vital role in handling and improving the overall performance of IoMT's operation. The IoMT's operation can be enhanced with blockchain management. The blockchain technologies assure the dependency of information and priority of operations under medical devices and applications. The blockchain manages the instruction of medical devices via a series of stacks and arrays. These stacks contain the information of nodes and users, maintaining addresses and operation tasks to assure connectivity.

IoMT devices under a predefined IoT ecosystem perform an arbiter role of information management with respect to communication protocols. These protocols restrict the user behavior model and hence cause unexpected intrusion detection. These intrusions can cause system failure and deadlocks in managing information. The flow of connectivity and error rate of such nodes needs to be recorded. The agenda of this research is to provide a reliable solution when encountering such intrusion attacks. The principle order of intrusion detection is based on raising intrusion flags or counters. Thus the IoMT devices can assign a priority in order to the operating standards. The IoMT based intrusion detection technique assures the management of remote incoming devices under error management to provide a systematic behavior and principle operating models. The model of such intrusion detection has to be highlighted with the support of blockchain approaches. The current article also states the operating principles of IoMT protocol enhancement with respect to the validating approaches of intrusion detection system's automation. The current article presents a standard protocol on

Corresponding author: Naif Khalaf Al-Shammari maintaining and reflecting the IoMT operating standards and its primary functionalities when encountering intrusion detection using a blockchain approach.

II. Literature Review

The operating and compatibility standards of IoMT are defined and processed from IoT based environment (ecosystem support, remote accessing, monitoring, and mentoring of information via demand-driven application services). The agenda of implementing IoT is to support economical communication and lay standard operating protocols on the existing ecosystem or infrastructure. Authors in [1] discussed various challenges and implementation protocols of IoMT with reference to the convergence of technological impairment and operating standards under the healthcare sector. Devices and data are sensitive and hence the coordination under remote accessing is a major challenge. Since the protocol of IoT governance has to be improved, a dedicated channel of cross layer protocol (CLP) is discussed in [2] in the view of providing a reliable service and connectivity under IoMT devices. The protocol improves the communication and bandwidth sharing among the systems governed under IoT. With these protocols in place, application-driven services such as in [3] were introduced to support the exclusive claim of services via IoT infrastructure.

Blockchain based instruction enhancement is proposed in [4] to support the variation and filtering of information via an enabled key management based authentication protocol for IoMT servers. This BAKMP protocol is supposed to store the data and monitor the reliability coefficient in order to access IoMT devices and the supporting user information. Detailed security communication challenges are reported in [5]. Authors in [6] present a multi-dimensional medical dataset theory for a telemedicine ecosystem. The model can be enhanced and simulated for IoMT device communication. The reliable TelMED protocol for communication under remote accessing model is discussed in [7]. Security concerns of implementing IoMT are reported in [8] under an approach of highlighting the information and communication barriers for implementation. The study is focused on various malwares or generally intrusion detection with reference to [9, 10]. The functionality of streamlining is a concern of various studies and reports [11, 12] on IoMT-based implementations. The conclusion and observations from this survey lack intrusion detection approach in IoMT devices via blockchain terminology. The blockchain aims to provide a reliable solution in IoMT and the current article discusses the influence of a protocol design on the edge of IoMT implementation.

III. Methodology

The proposed methodology intends to be a reliable source of application and management unit. The detailed description of the proposed IDS framework (Figure 1) in the edge network is as follows: An intrusion detection dataset is generated by injecting several kinds of attacks in the edge network where IoMT data are processed. In order to handle missing, noisy, and inconsistent data, preprocessing is performed on the dataset. To reduce the dimension of the dataset without losing information, PCA (Principal Component Analysis) feature selection algorithm is applied. There are several hyper parameters in the Deep Neural Network (DNN) like the number of layers, the number of epochs, optimization functions, etc.

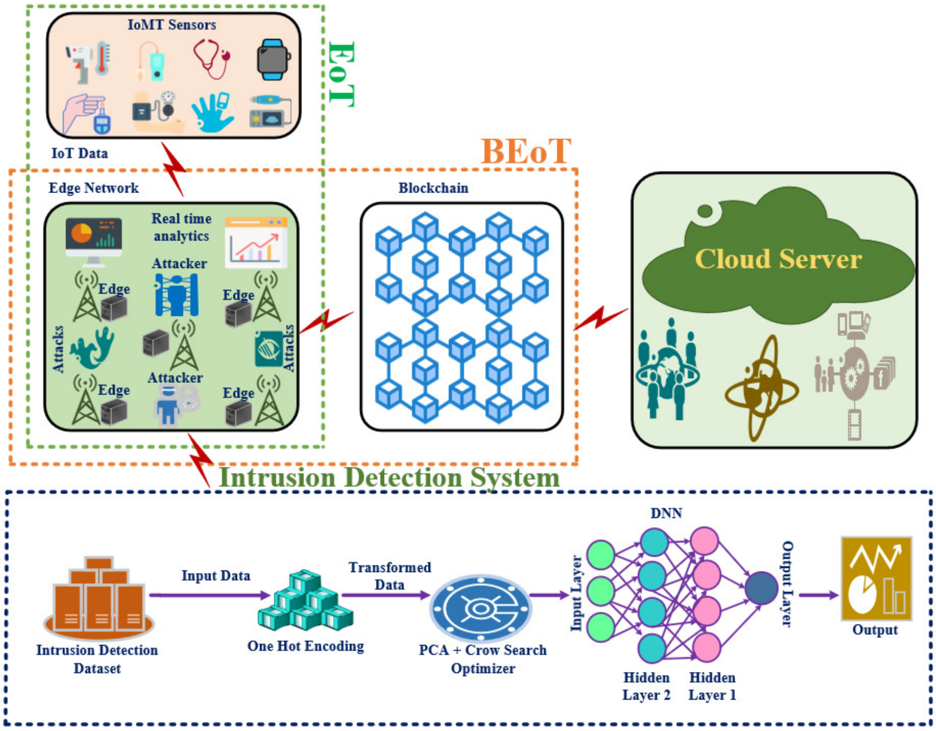

Fig. 1. Proposed system architecture diagram.

Choosing the optimal values for these parameters will help improving the performance of the DNN. In order to accomplish this, Crow Search algorithm is used for hyper parameter tuning. 70% of the dataset is used for training and the remaining 30% is used to validate the proposed system. DNN algorithms are used to train the generated IDS dataset. To prove the effectiveness of the proposed system, the results from various IDS scenarios are compared with several state of the art machine learning algorithms [13]. IoMT sensors are smart enough to acquire and transmit sensitive data to the edge of the network, but as these sensors have poor memory and limited processing units, they are not really smart enough to recognize how data are reliably transmitted or whether an attacker has been spotted during real-time analysis.

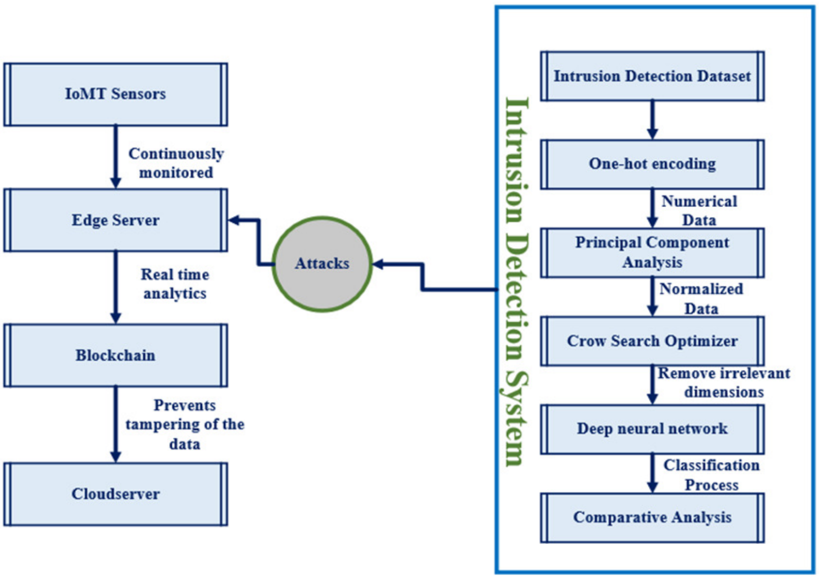

Fig. 2. System modeling design on IDS handling of the IoMT.

IV. MATHEMATICAL PROOF

The proposed model of IoMT-based intrusion detection is presented in Figure. 2. The block diagram shows an understanding of managing and troubleshooting of intrusion via the Crow Optimization algorithm. The process is discussed as follows:

1) Initial Pre-Processing and Setup Hypothesis

The initial configuration includes the setup and environment alignment of the IoMT ecosystem and operating standards. Typically, the IoT environment is stream-lined with basic networking and supporting devices for operation such as assigned routers, switches, end-users devices, and the network bandwidth. The setup of the proposed system must assure the reliability of the medical devices with the operating standards of IoT setup. Consider the initial IoT setup ecosystem devices as $I_D = \left(I_{D_1,}I_{D_2,}I_{D_3\ldots}I_{D_n}\right)$ where n end-user devices are connected and assigned for operations. The process of incorporating medical devices (*MT*) is represented as I_M under the given IoT ecosystem I_D, such that $\left[I_M \subseteq I_D \mid I_M \in I_D / \forall I_{M1},\ldots_{Mn} \subset I_{Dn}\right]$. The operation framework of I_M is reliable for operation. The I_M for each vector set is represented as $I_M = \left(I_{M_1,}I_{M_2,}I_{M_3\ldots}I_{M_n}\right)$ for each order of processing and bandwidth sharing.

2) User Configuration Validation

The overall incoming devices I_M are correlated with the matrix of user evaluation (*U*) as $U = \{U_1, U_2, U_3 \ldots\ldots\}$. The user U_i is associated with the IoT cloud matrix towards pairing users to respective cloud of medical devices I_m such that, the function of correlation is $\left[U_i \in I_i \bigcup I_i = I_1, I_2, I_3 \ldots I_n \mid I_m \subseteq I_i\right]$. The coordination elements are processed under independent devices I_m as $I_m \in I_i$ under open-alignment principle. The user collection of queries are reflected as:

$$Q = \frac{\delta(t - nf)\lambda}{2}\left(\sum_{i=o}^{n}\sum_{j=i+1}^{n-1}\frac{\delta(I_m)_j \times \delta(I_i)}{\delta t}\right) \quad (1)$$

The functional queries are based on $\delta(I_m)$ and $\delta(I_i)$ using user correlation as show in (2):

$$U = \lim_{n\to\infty}\left[\sum_{k=0}^{n}\left(\frac{\delta(Q_k) \times \delta(I_m)}{\delta t}\right) \times \Delta\lambda_t\right] \quad (2)$$

The user to service correlation functions are mapped with respect to query or service on user demand. The rational function values are assured to maintain a difference from $\delta(I_m)$ to prevent repeating. The query filtering operation mode Q_f is processed with reference to user-bandwidth (λ) and internet strength (termed as frequency (f) on operation) as shown in (3)-(5):

$$U = \lim_{n\to\infty} \frac{\delta(t-nf)\lambda_f}{2}\left(\sum_{i=o}^{n}\sum_{j=i+1}^{n-1}\frac{\delta(U_{n-i})_j}{\delta t}\right) \quad (3)$$

$$U = \int_0^\infty \frac{\delta\lambda_f(t-nf)}{2}\times\Delta R\left[\int_0^\infty \frac{\delta(U_{n-i})_j - \delta(I_m)_i}{\delta t}\right] \quad (4)$$

$$U = \left[\frac{\delta\lambda_f(t-nf)}{2}\times\Delta R\right]^{-2}\left[\int_0^\infty \frac{\delta(U_{n-i})_j - \delta(I_m)_i}{\delta t}\right] \quad (5)$$

where (*t-nf*) under the order of operations minimizes the intrusion error or error of connection to frame dependency with respect to rational value (ΔR). The frequency pattern (*f*) is an assurance pattern of $(\Delta\lambda t)$ for bandwidth minimization with each user. (U_{n-1}) is a user's coordination or association with internet (I_m) devices. The relationship is represented in (6):

$$U_R = \left[\frac{\delta\lambda_f(t-nf)}{2}\times\Delta R\right]^{-2}\left[\sum_{i=o}^{\infty}\frac{\delta(U_{n-i})_j}{\delta t}\cup\frac{\delta(I_m)_i}{\delta t}\times\lambda_t\right] \quad (6)$$

3) *Configuration of Intrusion Detection*

An intrusion of user's in internet connection is aligned with reference to connection patterns and configurations of the user devices. The configuration (C_f) is processed with respect to devices (I_m) and users (*U*) such for each device we have $D \Rightarrow (C_f : I_m \to (I_m) \subseteq U)$ under the operation principles of networking. The configuration setup is demonstrated in (7):

$$D^{|} = \left\{\lim_{n\to\infty}\frac{\delta(u\to C_f)}{\delta t}\right\} \cong \left\{\sum_{i=o}^{\infty}\sum_{j=i}^{n-1}\frac{\delta(I_m - I)_j}{\delta t_i}\right\} \quad (7)$$

$$D^{|} = \left\{\lim_{n\to\infty}\frac{\delta(u\to C_f)}{\delta t}\right\} - \lambda_t\left(\sum_{n}^{\infty}\frac{\delta(I_m)}{\delta t}\right) \quad (8)$$

From (8), the intrusion function can be integrated as a part of the configuration setting at user prospective as in:

$$D = \Delta C_f \cup D^{|} \quad (9)$$

The resultant (*D*) values are patterned and mapped with supporting devices' values with a controlled configuration of monitored parameters (*P*) as rate of connection, rate of operation, refreshing rate, and time to reply on a query under IoMT. These parameters are $P = \{P_1, P_2, P_3 ... P_n\}$ on each parameter $P_i \Rightarrow (\subseteq I_m \mid C_f)$ under the operation of networking standards.

4) *Intrusion Evaluation and Secure Communications Framework*

With the rate of configuration inclusion in the users connection as shown in (9), the inter-dependency matrix is evaluated to reframe and process a secure communication channel via IoMT services as shown in (10):

$$I_f = \left|\left[\lim_{n\to\infty}\frac{\delta(I_m)}{\delta t}\right]_0^n \cup \left[\lim_{n\to\infty}\frac{\delta(C_f)}{\delta t}\right]_0^{cf}\right| \quad (10)$$

Thus, the order of alignment (C_f) in configuration is managed and streamlined to detect the lightest change with respect to intrusion detection and report to the administrator. The intrusion support and vector configuration is limited to the range of the networking protocol as shown in (11) and thus, is further expanded into neighboring paradigms of features:

$$\lambda = \frac{1}{2\pi\Delta t_x}\times\left[\int_0^\infty\left(\frac{\delta(I_f)}{\delta t}\times 0.57\times\frac{\delta(U_R)-\delta(I_m)}{\delta t}\right)\right]_0^n \quad (11)$$

$$\lambda_\infty = \frac{(0.57)_{\log_x \Delta T}}{2\pi\Delta t_x}\times\left[\int_0^\infty\left(\frac{\delta(I_f - I_m)\times\delta(U_R)}{\delta t}\right)\right]_0^\infty \quad (12)$$

where λ_∞ is the representation of feature ranges with respect to the device and expanded into the higher grounds of information systems. The bandwidth becomes $\lambda \Rightarrow \lambda_\infty$ on the range shift with ratio of $\left[(0.57)_{\log_x \Delta T}\right]$ for a reference value correction with $\delta(I_f) \mid \delta(I_m)$ as the internet interpretation matrix value. This, expanding (10) is recomposed as:

$$I_f\infty = \left[\lim_{n\to\infty}\frac{\delta(I_m)}{\delta t}\right]_0^\infty \cup \left[\lim_{n\to\infty}\frac{\delta(C_f)}{\delta t}\times\lambda_\infty\right]_0^\infty \quad (13)$$

With respect to (13), the repeated parameters of interdepending devices values in C_f and I_m are expanded to infinite range of network tracking, making the process a reliable approach in shortlisting features set of instruction detection in the IoMT ecosystem.

V. EXPERIMENTAL SETUP AND RESULTS

The IoMT development has varying node cluster density. The throughput and accuracy of the evaluation are reported in Figure 3. The node throughput is gradually improved and a saturation is achieved with reference to improved IoMT enabled IoT nodes under the operating standards.

The resultant throughput is provided on evaluation paradigms of improving IoMT devices and their ratio of computation. The improvisation helps the process of reliable factor improvisation with reference to device density. The accuracy is mapped with reference to the accuracy and validation factor as shown in Figure 4 and Figure 5 respectively. The approach has achieved an accuracy of 92.3% on average.

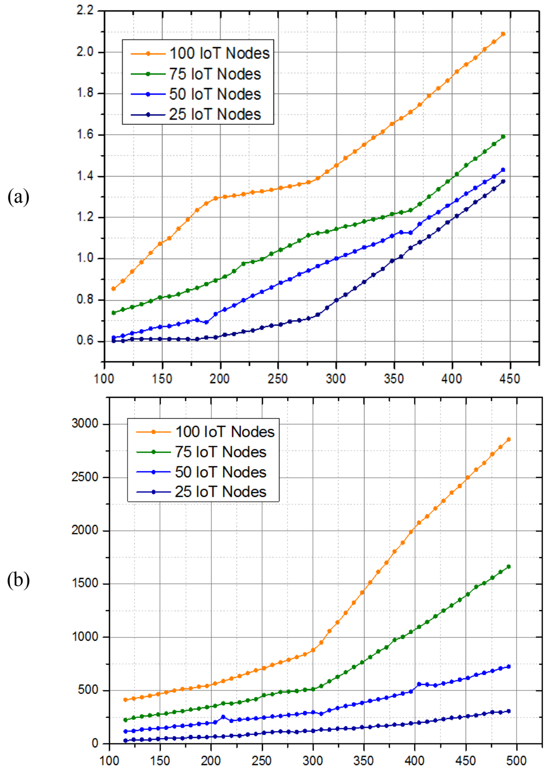

Fig. 3. (a) Throughput evaluation and (b) IoMT based throughput computation.

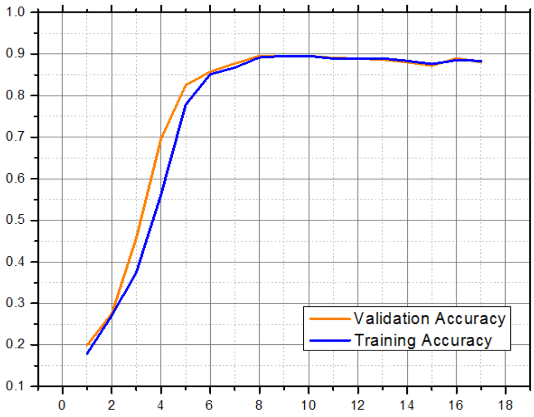

Fig. 4. Accuracy computation on IoMT devices.

VI. CONCLUSION AND FUTURE WORK

The proposed technique was discussed on various highlights and concerns on designing and developing IoMT environment and its respective intrusion detection. The article has also focused its discussion on various algorithmic approaches involved in streamlining IoT and IoMT devices in the cloud ecosystem. Various categories of intrusion detection and attacks were identified, detected, calibrated, studied, and reported. The mathematical representation and orientation approach of intrusion was defined using user-centric techniques in identifying vulnerable nodes/users with a 3-layered approach. The reliability of IoMT devices has increased by strengthening the application framework of healthcare IoT.

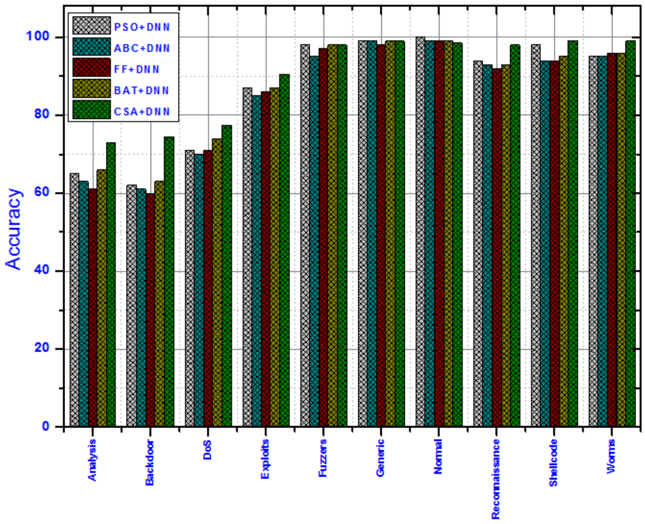

Fig. 5. Accuracy comparison.

ACKNOWLEDGMENT

This research work was funded by the Makkah Digital Gate Initiative under grand no. (MDP-IRI-015-2020). Therefore, the authors gratefully acknowledge the technical and financial support from the Emirate of Makkah Province and King Abdulaziz University, Jeddah, Saudi Arabia.

REFERENCES

[1] G. Joyia, R. Liaqat, A. Farooq, and S. Rehman, "Internet of Medical Things (IOMT): Applications, Benefits and Future Challenges in Healthcare Domain," *Journal of Communications*, vol. 12, no. 4, pp. 240–247, Apr. 2017, https://doi.org/10.12720/jcm.12.4.240-247.

[2] S. Rani, S. H. Ahmed, R. Talwar, J. Malhotra, and H. Song, "IoMT: A Reliable Cross Layer Protocol for Internet of Multimedia Things," *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 832–839, Jun. 2017, https://doi.org/10.1109/JIOT.2017.2671460.

[3] L. Haoyu, L. Jianxing, N. Arunkumar, A. F. Hussein, and M. M. Jaber, "An IoMT cloud-based real time sleep apnea detection scheme by using the SpO2 estimation supported by heart rate variability," *Future Generation Computer Systems*, vol. 98, pp. 69–77, Sep. 2019, https://doi.org/10.1016/j.future.2018.12.001.

[4] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. P. C. Rodrigues, and Y. Park, "BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment," *IEEE Access*, vol. 8, pp. 95956–95977, 2020, https://doi.org/10.1109/ACCESS.2020.2995917.

[5] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in IoMT Communications: A Survey," *Sensors*, vol. 20, no. 17, Jan. 2020, Art. no. 4828, https://doi.org/10.3390/s20174828.

[6] S. T. Ahmed, M. Sandhya, and S. Sankar, "A Dynamic MooM Dataset Processing Under TelMED Protocol Design for QoS Improvisation of Telemedicine Environment," *Journal of Medical Systems*, vol. 43, no. 8, Jul. 2019, Art. no. 257, https://doi.org/10.1007/s10916-019-1392-4.

[7] S. Thouheed Ahmed, M. Sandhya, and S. Sankar, "TelMED: Dynamic User Clustering Resource Allocation Technique for MooM Datasets Under Optimizing Telemedicine Network," *Wireless Personal Communications*, vol. 112, no. 4, May 2020, https://doi.org/10.1007/s11277-020-07091-x.

[8] M. Papaioannou *et al.*, "A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT)," *Transactions on Emerging Telecommunications Technologies*, 2020, Art. no. e4049, https://doi.org/10.1002/ett.4049.

[9] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, "IoMT Malware Detection Approaches: Analysis and Research Challenges," *IEEE Access*, vol. 7, pp. 182459–182476, 2019, https://doi.org/10.1109/ACCESS.2019.2960412.

[10] M. A. Jan, M. Usman, X. He, and A. Ur Rehman, "SAMS: A Seamless and Authorized Multimedia Streaming Framework for WMSN-Based IoMT," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1576–1583, Apr. 2019, https://doi.org/10.1109/JIOT.2018.2848284.

[11] S. Vishnu, S. R. J. Ramson, and R. Jegan, "Internet of Medical Things (IoMT) - An overview," in *2020 5th International Conference on Devices, Circuits and Systems (ICDCS)*, Coimbatore, India, Mar. 2020, pp. 101–104, https://doi.org/10.1109/ICDCS48716.2020.243558.

[12] O. AlShorman, B. AlShorman, M. Al-khassaweneh, and F. Alkahtani, "A review of internet of medical things (IoMT) - based remote health monitoring through wearable sensors: a case study for diabetic patients," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 20, no. 1, pp. 414–422, Oct. 2020, https://doi.org/10.11591/ijeecs.v20.i1.pp414-422.

[13] N. K. Al-Shammari, H. B. Almansour, and M. B. Syed, "Development of an Automatic Contactless Thermometer Alert System Based on GPS and Population Density," *Engineering, Technology & Applied Science Research*, vol. 11, no. 2, pp. 7006–7010, Apr. 2021, https://doi.org/10.48084/etasr.4103.

AUTHORS PROFILE

Naif Khalaf Al-Shammari Academic Qualifications: 1993 B.S., M.E., KSU, rating (4.25/5), 1999 M.S., M.E., KSU, rating (4.56), 2011 Ph.D., B.E., Birmingham University, UK. Professional Experience: 1994-2000 Saudi Electric Company, 2001-2010 Sultan B.A Al Saud Foundation. To date: Mechanical Engineering Department, University of Hail. Research Interests: Rehabilitation Engineering, Robotics & Control Mechanisms, Design of Biomechanical Systems and Bio/Nano-Robotics Dual-Arm & Flexible Manipulator Dynamics, Smart Materials, and Mechatronics Structures.

Syed Thouheed Ahmed works at the REVA University as an Assistant Professor in the School of Computing and Information Technology. He has graduated the B.E Computer Science and Engineering from Visveswaraya Technological University in 2013, M.Tech in Computer Science and Engineering, REVA Institute of Technology and Management (now REVA University), Bangalore in 2015. Currently, he is a Doctoral Fellow at the School of Computers, Information and Mathematical Sciences, BSA CRESCENT University, Chennai. He has published more than 45 research articles and papers in the field of Machine Learning, Big Data Analytics, Telemedicine, Image and Video Processing, Cloud Computing, and IoT at reputed international and national journals and conferences.

Syed Muzamil Basha completed his PhD at VIT university, Vellore, India in January, 2020. His current research interests include BigData Analytics, BlockChain Management, Internet of Things. He has more than 30 publications, which include 21 research papers, 7 international conferences, 6 book chapters, and 2 letters. He is one of the editors of 4 textbooks. He has conducted guest lectures in various Engineering Colleges in India. He received an award for his contribution in 2018 from VIT.