An SDN-AI-Based Approach for Detecting Anomalies in Imbalance Data Within a Network of Smart Medical Devices

Zabeehullah, Fahim Arif, and Nauman Ali Khan
National University of Sciences and Technology

Qazi Mazhar ul Haq
Yuan Ze University

Muhammad Asim and Sadique Ahmad
Prince Sultan University

***Abstract*—The Internet of Medical Things (IoMT) has become a novel paradigm for real-time healthcare applications. Artificial intelligence (AI) based efforts have been made to address the security challenges of IoMT, the problem of imbalance data still exists, due to which AI algorithms cannot sufficiently learn malicious traffic behavior and fail to identify rare anomalies in imbalance data accurately. Therefore, in this article, we propose an intelligent model based on software defined networking and deep learning (DL) to handle the heterogeneous, complex, and distributed architecture. To tackle the imbalance challenge, the proposed model utilizes generative adversarial network (GAN) to generate plausible synthetic data for minor class traffic. It combines autoencoder-driven DL models with reconstruction error and Wasserstein distance-based GAN. When compared to naive and advanced techniques, the proposed model produced noticeably better results on an imbalance dataset and outperformed these techniques by 4.78% and 4.54% in terms of accuracy and F1-score values, respectively.**

Digital Object Identifier 10.1109/MCE.2024.3389292
Date of publication 16 April 2024; date of current version 8 October 2024.

2162-2248 © 2024 IEEE

Published by the IEEE Consumer Technology Society

Internet of medical Things (IoMT) is frequently used to refer to the Internet of Things (IoT) as it relates to health applications.[1] By 2022, the global value of this industry is expected to surpass US$158 billion,[2] with linked medical devices directly responsible for about one-third of this expense. The diagnosis, tracking, and treatment of chronic illnesses such as diabetes, dementia, Parkinson's disease, epilepsy, seizure disorders, and sleep disorders are important uses for the IoMT. However, due to its complex, distributed, heterogeneous, and dynamic nature, IoMT devices are incompatible with traditional network infrastructure resulting in inefficient resource utilization.[3] Another challenge associated with the IoMT is the accurate detection of anomalies from imbalanced data. Most of the collected data comprises normal flows, with rare malicious behaviors capable of causing service failure. Within this category, specific types of attacks are exceptionally rare. As the frequency, sophistication, and complexity of cyberattacks increase, this imbalance of data between normal and malicious behaviors presents a significant hurdle for most artificial intelligence (AI) models. Their struggle lies in effectively securing systems due to the difficulty in learning and recognizing these rare anomalies.

This article aims to tackle the aforementioned challenges of IoMT by proposing an architecture based on software defined network (SDN) and deep learning (DL), where SDN can effectively manage the heterogeneity, complexity, and distributed nature of the IoMT and imbalance data challenge in SDN-IoMT is addressed by employing the generative adversarial network (GAN). The main contributions of this work are as follows.

- The proposed model employed SDN and generative adversarial network-autoencoder (GAN-AE) to accurately detect anomalies within imbalance data in a network of smart medical devices.
- The performance of the proposed GAN-AE model is compared with baseline (LSTM) and advanced ($\mathrm{CNN}_{\mathrm{AE}}$) techniques to evaluate the proposed model thoroughly. All models have been trained and evaluated in the same setting to ensure a fair comparison.
- The proposed model undergoes testing and evaluation within a simulated environment using the SDN-IoMT imbalance dataset. The evaluation employs a tenfold cross-validation technique to demonstrate balanced results.

RELATED WORK

In the literature, efforts have been made to address the challenge of anomaly detection and prevention in IoMT by employing SDN and AI-based techniques. Wagan et al.[4] combined two DL methods to perform IoMT anomaly detection. According to the performance assessment, it achieved individual accuracy of 92.95% and multimodal joint accuracy of 89.67%. In Zachos et al.[5] the proposed AIDS depends on machine learning approaches to detect irregularities in the IoMT data taking into account the computing overhead. Radoglou-Grammatikis et al.[6] addressed cybersecurity challenges in healthcare, specifically focusing on the IEC 60870-5-104 protocol. In Huang et al.[7] a hotel anti-epidemic management system was proposed to disinfect the used rooms by using UV LEDs through WiFi communication with the front desk computer and, therefore, it can protect quests from virus infection. Alazab et al.[8] presented an overview and recent advances of digital twins for healthcare 4.0. An architecture of digital twins for healthcare is also proposed. Furthermore, they presented several use cases of digital twins. Adil et al.[9] presented a detailed survey of healthcare IoT applications in the context of AI-enabled EEC technology to identify unresolved security challenges that need attention from the research community and healthcare stakeholders and then suggest potential research directions to give a clear future insight.

The literature review highlights that no existing work has been found that specifically addresses the smart healthcare imbalance data for detecting minor class attacks. To the best of our knowledge, this article represents the first attempt to detect minor class attacks and anomalies by applying SDN and AI.

PROPOSED METHODOLOGY

The imbalance data in the IoMT environment make it extremely difficult to precisely identify

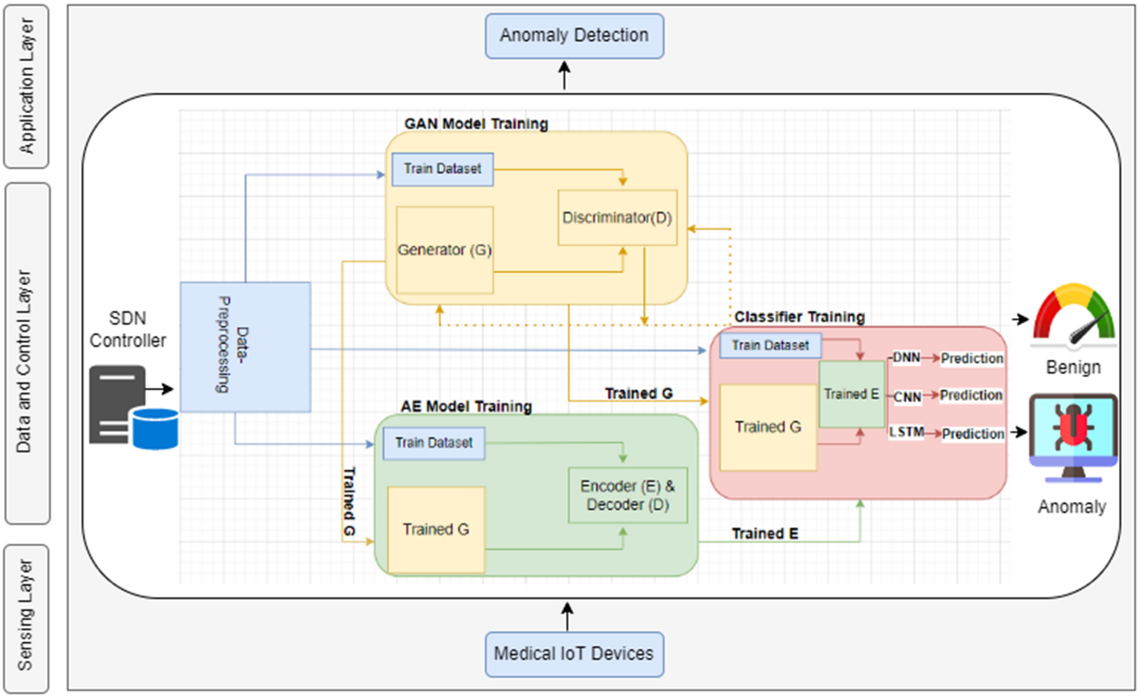

FIGURE 1. Schematic diagram of the proposed SDN-AI IoMT architecture.

and categorize anomalies and cutting-edge attacks. Medical data is one area where this problem is especially common. This problem exists mainly because many AI and DL models have biases that make them prefer the majority classes and make it difficult to detect minor class abnormalities. To address this problem, we have proposed a multilayered architecture consisting of a sensing layer, data and control layer, and application layer. The schematic diagram of the proposed method is presented in Figure 1. The sensing layer includes a range of IoMT devices, including actuators and medical sensors. These sensors are used for detecting blood pressure, temperature, and heart rate. This layer is primarily responsible for collecting and forwarding data to the next layer. The data layer is the second layer in the proposed model, and it includes various networking hardware such as switches and routers that support SDN. This layer is critical in enabling the seamless transfer of data across switches. The control layer is the system's primary control hub. Within this layer, the SDN controller has a global view of the entire network and manages various aspects, such as effectively managing congestion, optimizing routing, ensuring Quality of Service, and augmenting security measures. To detect and classify abnormalities in the imbalance dataset, we integrated the GAN-AE DL model into the SDN controller in our framework. The following section thoroughly explains each module in the GAN-AE system.

Data Preprocessing:

Raw data have been prepared and cleaned so that it can be used by DL algorithms. The dataset is processed using a variety of methods. Lines containing nonnumeric characters or empty values are initially removed to ensure that their impact on the performance of the test model is minimal. Because DL algorithms perform best with numerical data, nonnumerical values are converted to numerical equivalents using the label encoder, specifically sklearn. Furthermore, because the order of segments could affect model performance unexpectedly, the output label is encoded once. Data standardization is performed using the MinMax scalar function to improve the model performance.

Synthetic Data Generation With GAN:

Using the refined dataset, the generative model is constructed and trained using the synthetic data generation module. The generative model we employed is called boundary equilibrium generative adversarial network (BEGAN), and it functions similarly to the AE. We constructed the generator using the same architecture as the discriminator's decoder and the discriminator itself as a symmetric five-layer AE model. The system first divides the provided dataset into classes before creating generative models for each divided subdataset, which is then used to train the BEGAN model. In other words, generative models are constructed in an equal number as classes, and each generative model only generates synthetic data that corresponds to a specific class after training. Establishing the criterion for terminating the training process is critical to using the BEGAN model for minor class anomalies detection. This decision has a significant impact on the effectiveness of anomaly detection because it is directly related to the synthetic data used to train the detection model. The ability of BEGAN to estimate training convergence using the equilibrium concept distinguishes it from other GAN models. The following is the BEGAN convergence formula:

$$\mathbb{C}.\mathbb{M} = \lambda(a) + |\alpha\lambda(a) - \lambda(G(z))|. \tag{1}$$

The term $\lambda(.)$ represents the reconstruction error function in (1), while α represents the diversity ratio for a specific dataset class.

The convergence measure (M) is used to terminate the training phase of a generative model. The system input parameter is treated as a threshold value throughout training, and the training process is terminated if the convergence measure (M) falls below the designated threshold. We set the (M) threshold value at 0.058 in our proposed paradigm.[10] Following generative model training, the system employs the trained generator to generate synthetic data based on the classes. After that, the generated synthetic dataset is combined with the real training data. In the following steps, both the AE and the detection model are trained on the expanded dataset. Originally designed to generate generative models for each class, the synthetic data generation module can also be designed as a single model, embedding class attributes within the input space by leveraging the conditional GAN architecture.

Algorithm 1. Training of Autoencoder with generators.

```
INPUT : Training DataSet (TD) $TD_{\text{train}}$ and set of generators $\mathbf{G}$
Initialization of AE parameters $\mu^0_{AE}$
for $G_i \in \mathbf{G}$, where $1 \leq i \leq k$ do
    $\mathbf{z} = \{z_j\}j = 1, 2, 3. \ldots, m_i$
    Synthetic DataSet (SD) = $G_i(\mathbf{z})$
end for
Expanded Dataset (ED) $= TD_{\text{train}} \cup SD_1 \cup \ldots\ldots\ldots \cup SD_k$
$\mu_{AE} = Train_{AE}(\mu^0_{AE}, ED)$
$\mu_E = Encoder(\mu_{AE})$
OUTPUT: Trained Encoder $(\mu_E)$
```

AE Training:

The AE model is first trained to carry out dimension reduction and feature extraction procedures in order to build an effective anomaly detection model. The generative model discriminator's design and the AE architecture in our proposed model are the same. An AE model is constructed, trained on the expanded dataset, and then the trained encoder is applied to the feature extraction process. Algorithm 1 represents AE's entire training procedure. It is noteworthy that the input layer of the detection models is the trained encoder, which is placed first. It is set up only to be a feature extractor and is set not to learn anymore when training detection models.

Predictive Model Training:

At this point, we used deep neural network (DNN), convolutional neural network (CNN), and long short term memory (LSTM) algorithms to categorize abnormalities. Due to its inherent features, our DNN model, which has two hidden layers, performed well in identifying anomalies using the supplied fine-tuned datasets. CNN is the second classifier, and it was created mainly to analyze picture datasets. To make it suitable for IoMT imbalance data classification in terms of layers and input data space, a few structural modifications are needed. Hence, rather than transforming the input data into 2-D space, the CNN is built utilizing one-dimensional (1-D)

Algorithm 2. Generators-based classifier training.

```
INPUT : Training DataSet (TD) $TD_{\text{train}}$, set of generators $\mathbf{G}$, and Trained Encoder $(\mu_E)$
Initialization of classifier parameters $\chi^0$
for $G_i \in \mathbf{G}$, where $1 \leq i \leq k$ do
    $\mathbf{z} = \{z_j\} j = 1, 2, 3. \ldots, m_i$
    Synthetic DataSet (SD) = $G_i(\mathbf{z})$
end for
Expanded Dataset (ED) = $TD_{\text{train}} \cup SD_1 \cup \ldots\ldots\ldots \cup SD_k$
Trainable state of $\mu_E$ is set to false
Build $\chi^0_{\mu_E}$ = Model-Concatenation $(\mu_{AE}, \chi^0)$
$\chi_{\mu_E}$ = Train-Classifier $(\chi^0_{\mu_E}, ED)$
OUTPUT: Trained Encoder $(\chi_{\mu_E})$
```

convolutional layers for the classification of the IoMT imbalance dataset. Consequently, the CNN model is comprised of one fully connected layer and two 1-D convolutional layers. LSTM is the third classification of the DL model. It consists of two recurrent layers with LSTM units and a fully connected layer. For the analysis of temporally linked characteristics, LSTM is especially helpful. The output layer of all DL models has multi-valued fields when the goal is to identify anomalies. Using the trained generators and encoder, Algorithm 2 describes the comprehensive method for training the predictive model. To put it briefly, the training of the detection model comes first, followed by data preparation, before the anomaly detection and classification model operates. We use G-CNN_{AE} to describe our model. In addition, we have categorized the predictive models into three groups for a thorough comparison:

- LSTM, which is referred to as the naive DL model.
- CNN_{AE}, which is model combined with AE and is called an advanced DL model.
- G-CNN_{AE}, which is the proposed model.

In the application layer, security and medical experts analyze the current situation and take the necessary and appropriate actions.

EXPERIMENTAL SETUP AND EVALUATION METRICS

The proposed model is implemented in the SDN-IoMT environment with the Mininet 2.3.0 simulation tool.[11] Then, a DL model using the TensorFlow framework is employed inside the ONOS SDN controller. TensorFlow v2.12.0, the most recent version, is installed in the setup. A laptop equipped with an eighth generation Intel Core i9 processor, 16 GB of RAM, and a 1 TB hard drive is used to run the simulations.

Hyperparameters and Implementation

In the proposed methodology, the GAN discriminator is designed with three layers. The first hidden layer comprises 80 neurons along with 50 latent space dimensions. Consequently, the generator's hidden layer also includes 80 neurons with a 50-D latent space. The activation function employed is ReLU. It is noteworthy that the AE functions as a feature extractor, and its architecture mirrors that of the discriminator. Moreover, we established the threshold for the convergence of GAN at 0.058. The process to train the model halts if it falls below this threshold or when epochs reach 280. Similarly, the AE training concludes after 300 epochs. For classification, we have selected three models: DNN, CNN, and LSTM, each configured with two hidden layers. In the DNN, the one-layer contains 32 neurons, and the second has 16 neurons. Our CNN employs a 1-D-CNN architecture with two convolutional layers. The first layer is equipped with 32 convolutional filters, while the second layer functions as a fully connected layer with 16 neurons. ReLU is utilized as the activation function within the CNN. The last model we used for classification is LSTM, where each layer consists of 64 connected LSTM cells. In addition, we concatenated a fully connected layer with 32 neurons to the LSTM. After a thorough examination of the literature,[12] it is clear that no publicly dataset is currently available related to SDN-based smart medical devices to analyze and assess the efficiency of the proposed technique. There is just one dataset available for SDN-IoT environments in the literature, and it is mostly focused on network traffic intrusion detection.[13] Furthermore, there is just one dataset available for the Internet of Healthcare Things (IoHT) known as ECU-IoHT;[14] however, this dataset did not take SDN integration into account and instead focused solely on the IoT-Healthcare domain. Through an extensive literature review,

TABLE 1. **Comparison between the SDN-IoMT dataset and existing datasets.**

Ref.	Imbalance	SDN	IoMT
[13]	No	Yes	No
[14]	No	No	Yes
[15]	Yes	No	No
SDN-IoMT	Yes	Yes	Yes

it is found that both datasets mentioned above are not imbalance datasets.

Considering the proposed model, we undertook the simulation and development of an SDN-IoMT imbalance dataset that leverages both Sarica and Angin[13] and Ahmed et al.[14] techniques. To achieve this, three types of smart medical sensors are simulated within an SDN-based environment: a temperature sensor, a blood pressure sensor, and a heart rate sensor. The temperature sensor generates data every 10 seconds, while the blood pressure sensor produces a large volume of values primarily useful for attack detection. Meanwhile, the heart rate sensor generates data more frequently compared to the first two sensors. In line with the approach outlined in Sarica and Angin,[13] a similar topology and packet sending rate for normal traffic are used. The generation and recording of this normal traffic executed both with and without the presence of malicious traffic. Four types of attacks are conducted—Nmap port scan, ARP poisoning, DoS attack, and Smurf attack—to assess the robustness of the proposed technique. Dataset consists of 57,895 instances, and each instance comprises 18 attributes. The SDN-IoMT dataset is highly imbalanced, with three out of five classes (ARP Spoofing, Nmap PortScan, Smurf Attack) comprising less than 10% of the overall training data. With a weight of 0.53%, the Smurf Attack class has the lowest weight. This imbalance has a major effect on how the proposed model is trained. In addition, simulations are performed in an SDN-based environment during the dataset's creation process. A comparison between the imbalance SDN-IoMT dataset and state-of-the-art existing datasets is presented in Table 1.

TABLE 2. SDN-IoMT imbalance dataset distribution.

Class	Training	Weight%	Testing	Weight%
Normal	33,637	83 %	13,894	80%
DoS Attack	4,458	11%	1,476	8.5%
ARP Spoofing	1,366	3.37 %	1,077	6.2%
Nmap PortScan	851	2.1 %	677	3.9%
Smurf Attack	215	0.53 %	243	1.4%
Total	**40,527**	**100%**	**17,368**	**100%**

As part of our methodology, we divided the dataset into training and testing sets, allocating 70% for training and 30% for testing purposes. The distribution of the dataset is detailed in Table 2. The evaluation of the proposed technique is conducted using four standard metrics: accuracy, precision, recall, and F1-score.

Results and Discussion

In this section, the achieved results are discussed. It is important to note that the utilized SDN-IoMT dataset exhibits an imbalance, particularly within its minor and major classes. To enhance the classification accuracy, the proposed model generates synthetic data for minor classes based on their weights within the overall dataset. In experimentation, synthetic data are exclusively generated for those minor classes constituting less than 10% of the total distribution. Consequently, 5000 synthetic data points are generated for each of the following classes: ARP Spoofing, Nmap PortScan, and Smurf Attack, utilizing a trained GAN model.

The proposed model utilized a tenfold cross-validation technique, and the results are presented in Table 3. Each fold's results are meticulously displayed, providing a comprehensive understanding. The performance of the proposed model is evaluated on a test dataset using a confusion matrix, depicted in Figure 2. The clarity of the confusion matrix illustrates the proposed model's precise and efficient classification across all five classes, notably the minor ones. The comparison between the proposed model and the baseline DL models based on

TABLE 3. Findings of tenfold technique.

Metrics	Models	1	2	3	4	5	6	7	8	9	10
Accuracy(%)	**LSTM**	83.70	83.56	84.10	84.42	84.26	84.29	84.12	83.89	83.82	83.33
	CNN_{AE}	89.63	89.23	88.90	89.46	89.80	89.40	90.23	90.44	89.62	89.88
	G.CNN_{AE}	94.21	94.18	94.43	94.39	94.61	94.59	94.70	94.36	94.40	94.54
Recall(%)	**LSTM**	98.89	98.25	98.03	98.72	98.15	98.53	98.21	98.96	98.90	98.35
	CNN_{AE}	98.59	98.52	98.43	98.52	98.21	98.30	99.14	99.65	98.14	98.16
	CNN_{AE}	99.32	99.16	99.57	98.89	98.56	99.45	99.78	99.73	99.45	99.34
Precision(%)	**LSTM**	72.18	73.05	72.59	73.10	73.21	73.35	73.26	73.19	73.14	73.29
	CNN_{AE}	80.10	81.25	80.31	80.23	80.29	80.56	80.64	80.79	81.25	81.65
	G.CNN_{AE}	86.40	86.65	86.51	86.62	86.23	86.46	86.69	86.83	86.89	86.91
F1-Score(%)	**LSTM**	83.20	83.72	83.83	83.97	84.15	84.49	84.11	83.98	83.96	83.89
	CNN_{AE}	88.69	88.51	88.56	88.86	89.12	88.87	88.64	88.93	89.12	88.71
	G.CNN_{AE}	93.20	93.28	93.15	93.81	93.14	93.29	93.05	93.56	93.21	93.69

accuracy, recall, precision, and F1-score is presented in Figure 3. The proposed model achieved the highest accuracy and precision values of 94.44% and 99.32%, respectively. Furthermore, the recall and F1-score values of the proposed model are 99.35% and 93.34%, respectively. The results indicate that the proposed technique has outperformed both the naive and advanced baseline DL models. The accuracy and F1-score values for each class are detailed in Table 4. The proposed model outperformed the naive LSTM and advanced (CNN_{AE}) DL models by 4.78% and 4.54% in terms of accuracy and F1-score values, specifically on the extremely minor class (Smurf Attack), which accounts for only 0.53% of the overall dataset. This indicates a significant 4–5% improvement by the proposed model on the extremely minor class. In addition, the proposed model exhibited an 8–10% better result compared to competitors on normal classes and major classes such as DoS and ARP.

While the proposed model holds potential for enhancing classification performance, there is still the challenge of relatively low detection rates across certain classes. In particular, the proposed model observed to have relatively low

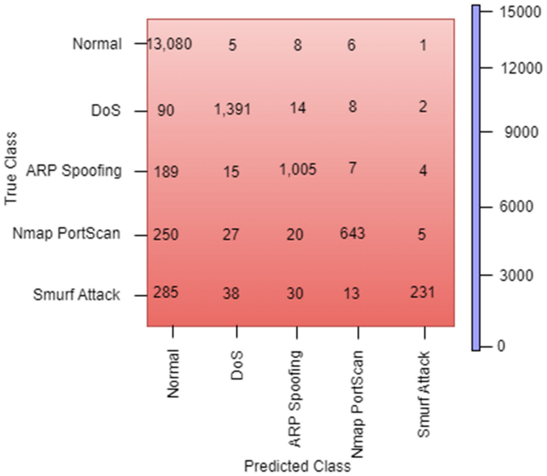

FIGURE 2. Confusion matrix of the proposed model (G.CNN_{AE}).

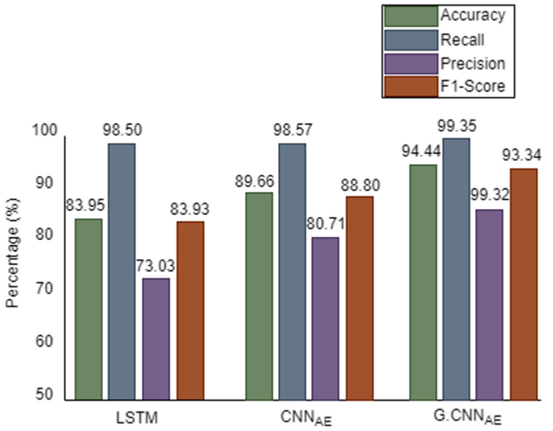

FIGURE 3. Comparison of the proposed framework ($G.\text{CNN}_{\text{AE}}$) against the naive (LSTM) and advanced (CNN_{AE}) DL models.

TABLE 4. Per-class Accuracy and F1-Score values of the proposed model against naive and advanced DL models.

Metric	Class	LSTM	CNN_{AE}	$G.CNN_{AE}$
Accuracy (%)	**Normal**	83.70	90.67	94.14
	DoS	84.63	89.90	94.23
	ARP	83.89	90.32	93.33
	Nmap	83.78	89.23	94.98
	Smurf	84.63	89.66	94.90
F1-Score (%)	**Normal**	82.42	85.79	92.97
	DoS	84.95	89.26	94.90
	ARP	45.88	81.34	91.43
	Nmap	12.76	16.56	23.78
	Smurf	10.34	15.67	22.89

detection rates for the Smurf class. Moreover, the proposed model is computationally expensive to some extent because the SDN controller and AI models demand certain level of computational resources.

CONCLUSION

In this article, we proposed a SDN and DL-based framework for anomaly and attack detection in an environment where a network of smart IoMT devices collects a huge amount of imbalance data. Specifically, the SDN architecture is integrated with an IoMT network to handle its complex, heterogeneous, and distributed architecture. Subsequently, a DL model based on GAN-AE is deployed at the control plane to improve the detection mechanism for minor class attacks and anomalies. The effectiveness of the proposed model is demonstrated in terms of accuracy, precision, and F1-score through experimental evaluation on an SDN-IoMT imbalance dataset. In addition, the performance of the proposed model is compared against both naïve and advanced DL techniques. In the future, the aim is to train the model on different imbalance datasets to further enhance the detection of minor class attacks in a network of various fields of life.

ACKNOWLEDGMENTS

The authors would like to thank Prince Sultan University for their valuable support.

REFERENCES

1. Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, “The future of healthcare Internet of Things: A survey of emerging technologies,” *IEEE Commun. Surv. Tut.*, vol. 22, no. 2, pp. 1121–1167, Second Quarter 2020.
2. S. Baker and W. Xiang, “Artificial intelligence of things for smarter healthcare: A survey of advancements, challenges, and opportunities,” *IEEE Commun. Surv. Tut.*, vol. 25, no. 2, pp. 1261–1293, Second Quarter 2023.
3. L. N. Tidjon, M. Frappier, and A. Mammar, “Intrusion detection systems: A cross-domain overview,” *IEEE Commun. Surv. Tut.*, vol. 21, no. 4, pp. 3639–3681, Fourth Quarter 2019.
4. S. A. Wagan, J. Koo, I. F. Siddiqui, N. M. F. Qureshi, M. Attique, and D. R. Shin, “A fuzzy-based duo-secure multi-modal framework for IoMT anomaly detection,” *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 35, no. 1, pp. 131–144, 2023.
5. G. Zachos, I. Essop, G. Mantas, K. Porfyrakis, J. C. Ribeiro, and J. Rodriguez, “An anomaly-based intrusion detection system for Internet of medical things networks,” *Electronics*, vol. 10, no. 21, 2021, Art. no. 2562.
6. P. Radoglou-Grammatikis et al., “Modeling, detecting, and mitigating threats against industrial healthcare systems: A combined software defined networking and reinforcement learning approach,” *IEEE Trans. Ind. Inform.*, vol. 18, no. 3, pp. 2041–2052, Mar. 2022.
7. K.-C. Huang, N.-C. Tai, and C.-Y. Hsien, “Consumer systems for healthcare and wellbeing,” Jul. 2022, doi: 10.1109/ICCE-Taiwan55306.2022.9869075.
8. M. Alazab et al., “Digital twins for healthcare 4.0–Recent advances, architecture, and open challenges,” *IEEE Consum. Electron. Mag.*, vol. 12, no. 6, pp. 29–37, Nov. 2023.
9. M. Adil, M. K. Khan, A. Farouk, M. A. Jan, A. Anwar, and Z. Jin, “AI-driven EEC for healthcare IoT: Security challenges and future research directions,” *IEEE Consum. Electron. Mag.*, vol. 13, no. 1, pp. 39–47, Jan. 2024.
10. D. Berthelot, T. Schumm, and L. Metz, “Began: Boundary equilibrium generative adversarial networks,” 2017, *arXiv:1703.10717*.
11. B. Lantz, B. Heller, and N. McKeown, “A network in a laptop: Rapid prototyping for software-defined networks,” in *Proc. 9th ACM SIGCOMM Workshop Hot Topics Netw.*, 2010, pp. 1–6.

12. F. De Keersmaeker, Y. Cao, G. K. Ndonda, and R. Sadre, “A survey of public IoT datasets for network security research,” *IEEE Commun. Surv. Tut.*, vol. 25, no. 3, pp. 1808–1840, Third Quarter 2023.
13. A. K. Sarica and P. Angin, “A novel SDN dataset for intrusion detection in IoT networks,” in *Proc. 16th Int. Conf. Netw. Serv. Manage.*, 2020, pp. 1–5.
14. M. Ahmed, S. Byreddy, A. Nutakki, L. F. Sikos, and P. Haskell-Dowland, “ECU-IoHT: A dataset for analyzing cyberattacks in Internet of Health Things,” *Ad Hoc Netw.*, vol. 122, 2021, Art. no. 102621.
15. M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the KDD CUP 99 data set,” in *Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl.*, 2009, pp. 1–6.

Zabeehullah is currently working toward the Ph.D. degree in computer software engineering from the National University of Sciences and Technology, Pakistan. His research interests include deep learning, Internet of Medical Things, SDN, and IoMT security. Contact him at zabeeh.phdcse@students.mcs.edu.pk.

Fahim Arif received the Ph.D. degree in software engineering from National University of Sciences and Technology, Pakistan, in 2002. His research interests include remote sensing, and machine learning. Contact him at fahim@.mcs.edu.pk.

Nauman Ali Khan received the Ph.D. degree in communication and information systems from the University of Science and Technology of China, Hefei, China. His research interests include machine learning, social network analysis, social-tie inference, and prediction. Contact him at nauman@mcs.edu.pk.

Qazi Mazhar ul Haq received the Ph.D. degree in electronics and computer engineering from the National Taiwan University of Science and Technology, Taipei, Taiwan, in 2021. His research interests include object detection, incremental learning, anomaly detection, image processing, deep learning. Contact him at qazi@saturn.yzu.edu.tw.

Muhammad Asim received the Ph.D. degree in computer science and technology from Central South University, Changsha, China, in 2022. His current research interests include artificial intelligence, 5G/6G communication systems, and autonomous vehicles. Contact him at masim@psu.edu.sa.

Sadique Ahmad received the Ph.D. degree from the Department of Computer Sciences and Technology, Beijing Institute of Technology, Beijing, China, in 2019. His research interests include deep learning, image processing and video action detection. Contact him at ahmad01.shah@gmail.com.