

Hybrid software defined network-based deep learning framework for enhancing internet of medical things cybersecurity

Yahya Rbah¹, Mohammed Mahfoudi², Mohammed Fattah¹, Younes Balboul¹, Kaouthar Chetioui¹,
Said Mazer¹, Moulhime Elbakkali¹, Benaissa Bernoussi¹

¹Laboratory of Artificial Intelligence, Data Sciences, and Emerging Systems, National School of Applied Sciences,
Sidi Mohamed Ben Abdellah University, FES, Morocco

²Innovative Systems Engineering Laboratory, National School of Applied Sciences, Abdelmalek Essaadi University, Tetuan, Morocco

Article Info

Article history:

Received Dec 29, 2023

Revised Feb 2, 2024

Accepted Feb 29, 2024

Keywords:

Deep learning

Internet of medical things

Intrusion detection system

Software defined networks

Convolutional neural networks

Bidirectional long short-term
memory

ABSTRACT

The rapid growth of the internet of medical things (IoMT) has escalated cyber-attack risks in healthcare. With IoMT devices proliferating in healthcare facilities, conventional intrusion detection methods face challenges. Our study proposes a hybrid framework merging software defined network (SDN) controllers with deep learning (DL) techniques, including convolutional neural networks (CNN) and bidirectional long short-term memory (Bi-LSTM). This approach introduces a unique combination enabling dynamic and efficient IoMT security management. By integrating CNN and Bi-LSTM, the system can handle diverse IoMT data types, offering a comprehensive threat detection solution. Unlike traditional methods, our hybrid solution seamlessly adapts to the evolving threat landscape of healthcare IoT systems. Urgency arises from the critical need to fortify IoMT security amid escalating cyber threats. The complex nature of IoMT networks poses challenges for conventional methods, making our exploration of a hybrid SDN-based DL framework imperative. With a background in cybersecurity and a focus on healthcare IoT, we recognize the urgency to develop a solution that enhances detection accuracy and ensures real-time responsiveness in healthcare settings. Our proposed method, validated using the "IoT-healthcare security" dataset, demonstrates a high detection accuracy of 99.97% and speed efficiency of less than 1.8 seconds, outperforming current techniques.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Yahya Rbah

Laboratory of Artificial Intelligence, Data Sciences, and Emerging Systems

National School of Applied Sciences, Sidi Mohamed Ben Abdellah University

FES, Morocco

Email: rbah.yahya@gmail.com

1. INTRODUCTION

Various industries, including health care, home appliance manufacturers, and energy companies, have extensively adopted the internet of things (IoT). The growing use of this technology in the field has significantly transformed our daily lives [1]. The internet of medical things (IoMT), a subset of the IoT, encompasses many technologies, such as embedded medical devices, elderly monitoring wearables, internet-connected clinical devices, and hospital rooms for remote surgery [2]. They allow remote access to the patient's condition, including chronic disease management, heart rate, and blood pressure [3].

While the IoMT ecosystem confers considerable benefits, its pervasive and wide-open nature makes it a prime target for emerging cyberattacks and threats [4]. These devices' widespread interconnectivity and

continuous data exchange make them a primary target for various threat actors to perform anomalous activities against [5]. For instance, the attacker injects malware or malicious software into the network devices to gain unauthorized access. Such attacks include denial of service (DoS), man in the middle (MITM) and ransomware. Unfortunately, these attacks are becoming increasingly common and pose a significant risk to the confidentiality, integrity and availability of data [6]. Therefore, attacks conducted on the IoMT can cause devastating effects, resulting in severe damage compared to traditional enterprises and industries [7]. For instance, an attacker could shock a patient, potentially causing death, if they gain remote control of a smart pacemaker [8]. In the literature, some research [9]–[11] has focused on the implementation of encryption and authentication solutions for the IoMT environment. Such approaches often require significant computational resources and can be challenging to implement on medical devices with limited resources. Recently, several approaches [4], [12], [13] have used artificial intelligence (AI) technologies to provide relevant insights for classification, decision-making and cyber-attack. However, their overall performances remain low due to the complexity of the attacks. In addition, existing detection systems still need to be improved to detect new cyber-attacks. In addition, existing detection systems tend to be trained on standard datasets designed for conventional detection systems. Identifying specific types of medical attacks is difficult due to the limited availability of public datasets that monitor attacks in the IoMT environment. Therefore, such environments require an adaptive, cost effective, scalable intrusion detection systems (IDS) to deal with emerging cyber-attacks [4].

Software defined network (SDN) is emerging as a new network management paradigm to meet the demand for programmatic network management [14]. Although the combination of SDN and IoT enhances IoMT functionality and safety by enabling remote and complete network control without direct contact with IoMT devices, an effective IDS is necessary to protect the system from a wide range of threats. Deep learning (DL), a branch of machine learning (ML), involves the use of multiple hidden layers to extract high-level features from raw data [15], [16]. Using this approach in intrusion detection can help detect such malicious threats. This work proposes a hybrid DL-based SDN system for effective and efficient intrusion detection in the IoMT environment. The proposed method is embedded in the SDN architecture. This provides robustness, flexibility, and scalability. Our model combines the advantages of the convolutional neural networks (CNNs) to extract distinctive features and the capacity of the bi-directional LSTM to capture short- and long-term relations in a single hybrid deep CNN-bidirectional long short-term memory (Bi-LSTM) model. The paper's main contributions are:

- We proposed a scalable SDN-based detection system using a hybrid DL approach (i.e., CNN-BiLSTM) for the IoMT. The proposed framework does not overload the IoMT resources.
- We used a recently developed and advanced IoMT dataset (i.e., the IoT-healthcare security dataset) to evaluate the performance of the proposed model.
- We used common and advanced performance evaluation measures (i.e., detection accuracy, recall, precision, F1 score, and time complexity.) to evaluate the proposed system rigorously.
- We have evaluated the performance of the proposed model against two established benchmark models, gated recurrent unit (GRU)-BiLSTM and graph neural network (GNN)-BiLSTM.
- We provided a detailed comparison with the latest benchmarked algorithms. The proposed approach outperforms both in terms of accuracy and computation complexity.

The remainder of this study is structured as follows: in section 2, the background is provided along with related work. Section 3 contains materials and methods, including the proposed model, dataset description, preprocessing techniques, evaluation measures and experimental setup. A detailed evaluation of the results and a comparative analysis with state-of-the-art techniques is presented in section 4. The paper concludes in section 5 with future directions.

2. BACKGROUND AND RELATED WORK

Conventional internet architecture has become a complex system due to decentralization, with many network components involving different layers, such as switches, routers, and middleboxes. As a result, the traditional network architecture cannot respond to the dynamic features of modern applications [17]. SDN based approaches are considered more relevant to ensure IoMT environments' security against internal and external cyberattacks [18]. Essentially, SDN is very useful in addressing the security issues related to IoT devices. Such network can effectively deal with security threats dynamically and flexibly without burdening IoT devices [19]. ML and DL are other significant technologies that are increasingly working to achieve the same objectives [20]. Such technologies can be intertwined and combined to address many IoT security threats [21], [22].

An IDS refers to software or hardware that detects and responds to intrusions [23]. It protects against unauthorized access and manipulation of the computer system or network resources [24]. In terms of functionality, IDSs are divided into two categories: i) host-based intrusion detection systems (HIDS) and

ii) network-based intrusion detection systems (NIDS). HIDS systems work on any device that is connected to the Internet, while NIDS is often deployed or placed at key points in the network to ensure that it captures traffic which is more susceptible to attack [25]. There are basically two intrusion detection strategies, namely i) anomaly-based IDSs and ii) signature-based IDSs [26]. The anomaly-based IDSs compare trusted behavior patterns with novel behavior on regular activity monitoring. Signature-based IDSs are focused on recognizing intrusion patterns as a signature, and is perfected by regularly updating the signatures database with the newest trends or zero-day attack patterns [27].

Recently, ML and DL techniques have been applied in network security due to their ability to discriminate data. Halman and Alenazi [13] introduced a comprehensive study of the crucial issue of generalized detection of threats and attacks in the SDNs environments of healthcare systems. They proposed the machine learning-based cyberattack detector (MCAD) to detect attacks on healthcare systems using ML in SDNs. The proposed system is analyzed using network key performance indicators (KPIs). The authors considered various attack scenarios corresponding to real-world scenarios to test the proposed system's effectiveness. Liaqat *et al.* [7] presented a hybrid DL SDN mechanism for detecting malicious multi-vector evolved IoMT botnets (i.e., theft, reconnaissance, and distributed denial of service (DDoS)). Moreover, the proposed method leverages the resource constrained devices of the IoT without exhausting them. The proposed framework performs better in both accuracy and time efficiency. Khan and Akhuzada [12] presented an SDN-based LSTM and CNN hybrid DL to detect malware in IoMT. The proposed framework is deployed at the application layer of the SDN layer. The authors have used the latest publicly available dataset of IoT malware to evaluate their system. The proposed method better detects and prevents sophisticated IoMT threats with low computation overhead. Wahab *et al.* [4] presented a (Cu-LSTM-GRU) SDN-based framework for detecting cyber threats in the IoMT environment. The CICDDoS2019 dataset was used to evaluate the performance of the proposed model. The proposed technique outperformed the current literature with 99.01% accuracy. Haseeb *et al.* [28] presented a ML, SDN-based big data framework for the IoMT system that effectively manages network devices and improves healthcare data delivery. Moreover, the proposed system includes an IDS and implements security using the SDN architecture to address the unpredictability of unknown threats. The proposed system is validated against existing work using dynamic network measures. Table 1 summarizes the detection approach, employed algorithms, accuracy measurements, and limitations of state-of-the-art machine/DL-based IDS designed for IDS within SDN IoMT networks.

Most of the presented studies were carried out using conducted using ML and DL approaches trained on unreliable and outdated datasets, such as “UNSW-NB15”, “NSLKDD”, “CICDDoS2019”, “Bot-IoT” and “ToN-IoT”. A recently published dataset has been created in [29] to address this issue. This dataset, known as “IoT-healthcare security”, reflects IoMT's heterogeneous nature. The IoT-healthcare security is more appropriate for IoMT environments, reflecting real-world IoMT-based cyberattacks to validate the proposed IDS performance.

Table 1. State of the art ML/DL-based IDSs in SDN IoMT networks

| Reference | Year | Detection approach | Algorithm | Dataset | Accuracy (%) | Limitations |
|--------------------------|------|---------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|--------------------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Halman and Alenazi [13] | 2020 | A ML-based cyber-attacks detector (MCAD) to detect attacks for healthcare systems using ML in SDNs. | KNN, DT, RF, NB, LR, XGB, and Adaboost. | Generated dataset. | 99.24% | <ul style="list-style-type: none"> - Not evaluated on current benchmark datasets. - Time complexity is not considered. - Comparison is made with ML algorithms. |
| Liaqat <i>et al.</i> [7] | 2020 | A hybrid DL-driven SDN mechanism for detecting malicious multi-vector evolved IoMT malware botnets (i.e., theft, DDoS, and reconnaissance). | CNN-cuDNNLSTM. | Bot-IoT. | 99.99% | <ul style="list-style-type: none"> - Network traffic only, Bot-IoT not focused on IoMT network. - Only for malware attack detection. |
| Khan and Akhuzada [12] | 2021 | A hybrid DL SDN-based CNN and LSTM to detect sophisticated malware in IoMT. | CNN-LSTM. | IoT | 99.83% | <ul style="list-style-type: none"> - The dataset is relevant for IoT network traffic data only, and not applicable for IoMT. - Only for malware attack detection. |
| Wahab <i>et al.</i> [4] | 2022 | a (Cu-LSTM+GRU) SDN-enabled framework for detecting cyber threats in the IoMT environments. | Cu-LSTM+GRU. | CICDDoS2019. | 99.01% | <ul style="list-style-type: none"> - Network traffic only, CICDDoS2019 not IoMT network specific. |

3. PROPOSED MODEL

In this section, we detail our proposed IDS methodology, covering network topology, attack detection architecture, dataset pre-processing, and performance metrics. We provide insights into tools and experimental methodology for a comprehensive understanding.

3.1. Network model

SDN represents an advanced networking paradigm with significant capabilities. Basically, SDN consists of three layers and their respective APIs (i.e., northbound and southbound). Figure 1 depicts the fundamental architectural representation of the SDN with the proposed detection mechanism at the control layer [17]. The application layer differs from the other layers in that it only ensures the thorough execution of the commands issued by the other layers [30]. The control layer provides programmable functions that adequately link the emerging external communication technologies, i.e., IoT, in the data layer [31]. The IoT communication nodes can be further controlled by the control plane. The SDN control layer dynamically analyzes all traffic transmitted over the IoT networks. Thus, SDN provides aggregated services, i.e., customized, scalable and secure IoT [32].

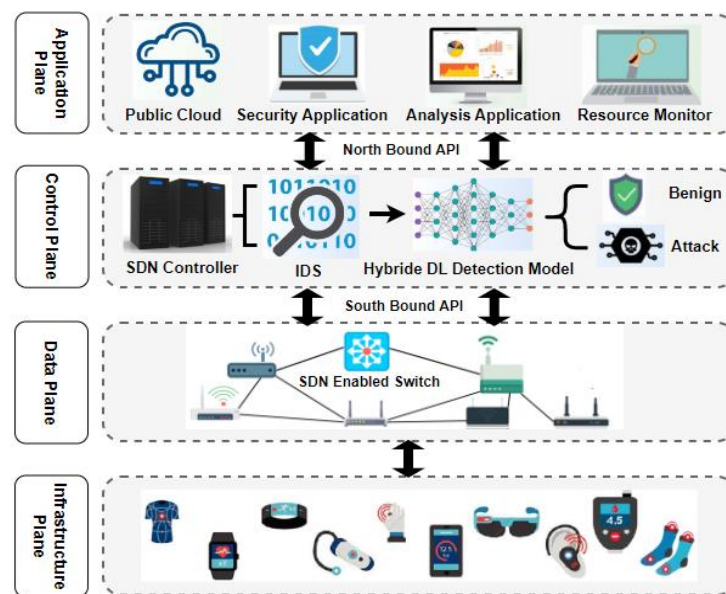


Figure 1. SDN-based architecture for IoMT

To overcome the emanating cyber-attacks in the IoMT, we proposed a CNN-BiLSTM model. The developed model is integrated into the SDN control plane for several reasons. First, the control layer is the kernel of the SDN network's centralized intelligence, and routing decisions are made at this level [7]. Second, the proposed system at the control layer allows the underlying restricted IoMT devices to be easily leveraged without exhaustion, making it a more appropriate IoMT breakthrough. Furthermore, the proposed framework is scalable and manageable as it is customizable, centralized and extensible across all SDN controllers.

3.2. Proposed hybrid attack detection system

We present a hybrid DL-SDN based framework to detect sophisticated attacks in the IoMT system. The proposed framework comprises CNN and Bi-LSTM. The schematic overview of the proposed model (i.e., CNN-BiLSTM) is depicted in Figure 2, and the algorithm is given in Algorithm 1. The model implementation architecture consists of four main components: data collection, data preprocessing, the CNN-BiLSTM model, and decision judgement, as illustrated in Figure 2. Furthermore, the proposed hybrid DL network consists primarily of 1D convolution, pooling, bidirectional-LTSM, dropout, flattening and fully connected layers. The proposed method is considered as an enhancement of CNN-LSTM, whereby each cell of LSTM is augmented with two cell hidden states, respectively for a forward and a backward sequence. Furthermore, the proposed model incorporates the major properties of both CNN and LSTM, making it efficient for certain types of sequence-based tasks, such as sequence classification in network traffic analysis.

Algorithm 1: CNN-BiLSTM Network for Network Attack Detection

Require: Input df = dataset

- 1: Set F features = f_1, \dots, f_n from df set as Subset, where $n = no.of\ selected\ features$
- 2: Split df features into training, and testing
- 3: Procedure Build_CNN_BiLSTM_Model
- 4: Add a Conv1D layer with 64 filters, kernel size 3, and ReLU activation
- 5: Add MaxPooling1D layer with pool size 1
- 6: Add a Reshape layer to reshape output to (-1, 64)
- 7: Add a Dense layer with 128 units and ReLU activation
- 8: Add Dropout layer with rate 0.5
- 9: Add Bidirectional LSTM layer with units 64 and return_sequences=False
- 10: Add a Dense layer with 1 unit and sigmoid activation for binary classification
- 11: Compile the model with binary_crossentropy loss and Adam optimizer (learning_rate = 0.001)
- 12: Add EarlyStopping callback for monitoring validation accuracy
- 13: Build_CNN_BiLSTM_Model
- 14: Train the model using $X_{train_cnn_bilstm}$ and y_{train} for 10 epochs and batch size 32
- 15: Perform validation split of 33%
- 16: Algorithm End

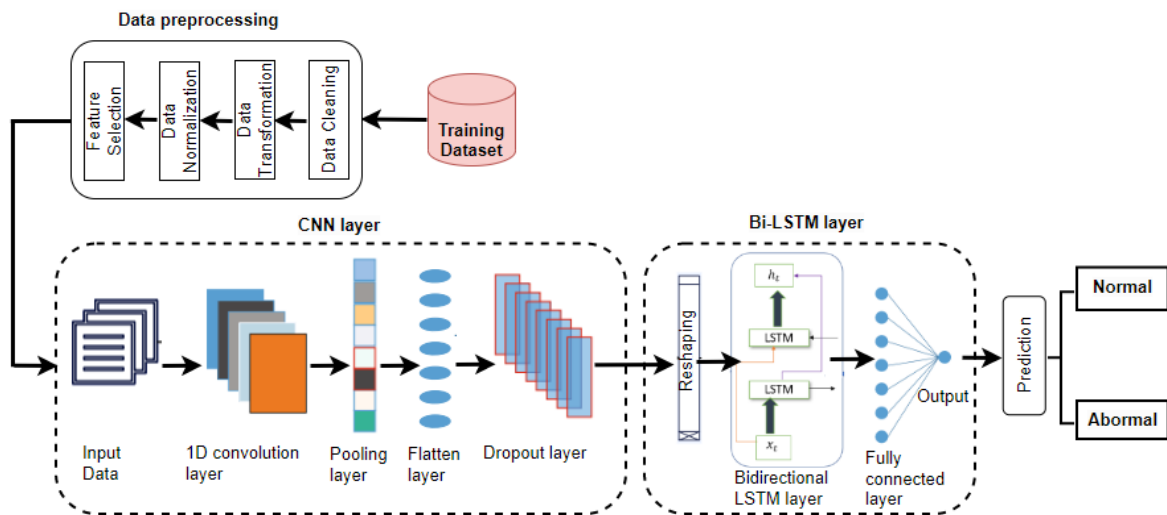


Figure 2. Proposed CNN-BiLSTM model architecture

The model architecture is sequential, starting with a sequence of CNN layers, followed by a BiLSTM layer, and ending with an output layer designed for binary classification. Algorithm 1 describes the steps to build a CNN-BiLSTM model for network attack detection. It starts by reshaping the input data and then builds the model's architecture using Conv1D, MaxPooling1D, reshape, dense, dropout, and BiLSTM layers. Table 2 shows the details of the 1D CNN-BiLSTM, with layer names and hyperparameter settings for each layer.

Table 2. Parameters' settings of the CNN-BiLSTM model

| Layers | Neurons/kernel |
|---------------|---------------------------|
| Conv1D | 64 filters, kernel size 3 |
| Dense layer | 128 units |
| Bi-LSTM layer | units 64 |
| Dense layer | 1 unit |

3.3. Dataset description

We used the "IoT-healthcare security" dataset [29] in our system to include the IoMT network attacks. This dataset includes both normal and malicious network traffic, generated through the IoT-Flock tool in a healthcare IoT context [33]. In the "IoT-healthcare security" dataset, the testbed infrastructure was split into

two separate networks: the estimated and intruder networks. The estimated network consisted of message queuing telemetry transport (MQTT) devices sending and receiving data on the network [34]. These medical devices have been built on a single physical Linux machine with the IoT flock. In addition, the constrained application protocol (COAP) server and MQTT broker were running on separate machines. The second network in the testbed is the intruder network, containing several attack elements that can perform various attacks, namely BruteForce, MQTT publish-flood, MQTT DDoS and SlowITE, on targeted medical servers or devices. Using Wireshark to collect the network packet flows, the application and network layer characteristics of the IoMT traffic were subsequently extracted from the generated PCAP files and saved to a CSV file with the corresponding traffic labels using a Python utility [33]. The dataset contained 108541 samples of benign (class 0) and 80153 malicious (class 1). Further details can be found in [34].

3.4. Pre-processing

Preparing the dataset for building the CNN-BiLSTM model involves essential steps such as data cleansing, transformation, normalization, and feature selection. These techniques are vital for optimizing the dataset and ensuring its suitability for model training. Pre-processing is crucial to enable effective utilization of the data in constructing the CNN-BiLSTM architecture.

3.4.1. Data transformation

The initial step involved removing rows with missing data from the dataset to improve data quality and the accuracy of the scoring model. In DL-based approaches, data is usually processed in a numerical matrix. For this reason, we used the label encoder functions in Sklearn to transform all non-numerical features into numerical values. In addition, the output labels were encoded as one-hot encoding, as the order of the categories can negatively affect the validation of the proposed model's performance. The one-hot encoding method is used to count the unique value of each feature. Each value is assigned a unique index [27].

3.4.2. Data normalization

According to the DL algorithm applied, the data normalization technique normalizes the values of the features to the range [-1, 1] or [0, 1]. The data normalization shortens training time and speeds up model convergence. To increase the proposed algorithm's effectiveness and obtain productive results, moving all values towards a scaled variant is necessary, as this eliminates the effects of gross influence [7]. The min-max scalar function was applied to normalize the feature vectors of the IoT-healthcare security dataset.

3.4.2. Feature selection

After preprocessing, we used the Chi-squared test feature selection method to remove irrelevant and redundant features from the dataset to reduce processing time and improve model efficiency. Therefore, we have selected the ten most significant features from the "IoT healthcare security" dataset. This dataset is then shuffled and randomly divided into training and test parts of 80% and 20% respectively.

3.5. Evaluation metrics

The present work evaluates the performance of the proposed model using common performance evaluation measures (i.e., accuracy, recall, precision, F1 score, ROC) and memory and time complexity. The mathematical formulas of the standard evaluation metrics used in this research are presented from (1) to (4),

- Accuracy is the percentage of records labelled correctly [35].

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} \quad (1)$$

- Precision is the number of records correctly predicted [26].

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

- Recall is the number of correct predictions out of all records [36].

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

- F1-score is the harmonic mean of precision and recall [37].

$$F1_Score = 2 * \frac{precision*recall}{(precision+recall)} \quad (4)$$

Where: TP, TN, FP, and FN are true positive, true negative, false positive, and false negative respectively. The true positive represents attack traffic correctly classified as an attack, while the true negative indicates the normal traffic that is correctly classified as normal. The false positive relates to the normal network traffic misclassified as an attack, while the false negative relates to the attack traffic misclassified as normal [34]. Further, these values are derived from the confusion matrix. The confusion matrix defines the overall performance of a classifier; it shows and compares the predicted values with the actual values. Table 3 shows the confusion matrix of binary classification [38].

Table 3. Confusion matrix

| Confusion matrix | | Predicted Label | |
|------------------|-------------------|-------------------|-------------------|
| | | Positive (attack) | Negative (normal) |
| Actual label | Positive (attack) | True positive | False negative |
| | Negative (normal) | False positive | True negative |

To better evaluate the proposed model, we have also calculated another measure of performance called the area under the curve (AUC) – the receiver operative characteristic (ROC) indicates the classification model's performance at all classification levels. The ROC represents a plot of false positive rate against true positive rate, whereby a low classification level means an increase in both false positive and true positive rates [39]. The AUC indicates the overall system performance; The more area below the curve, the higher the performance and efficiency of the model [17].

In addition to the above performance measures, we also considered the memory and time complexity of the proposed algorithm. The memory usage metric indicates the required memory consumption for an IDS to perform its classification task. Detection time is the delay between the input of data and the detection of benign or malicious traffic by the algorithm.

3.6. Experimental setup

To implement the proposed models, the utilization of Google Colaboratory with its provided resources, including the Intel–Xeon CPU, Tesla–K80 accelerator, and 13 GB RAM, allows for efficient training and testing of ML and DL models. The Tesla–K80 accelerator, with 12 GB GDDR5 VRAM, is particularly beneficial for accelerating DL computations. Python, with its extensive libraries and frameworks, is a suitable choice for implementing machine and DL models. Pandas facilitates data manipulation and preprocessing, NumPy is essential for efficient matrix operations, Scikit-learn provides tools for data preprocessing and model evaluation, and Matplotlib aids in visualizing data and results. The integration of TensorFlow with its Keras backend offers a powerful and flexible environment for developing and experimenting with DL models. The chosen parameters and hyperparameters, such as the optimizer (Adam), activation function (ReLU), learning rate (0.001), and loss function (categorical cross-entropy), are standard choices in DL and have been proven effective in various applications. There are 153,474 trainable parameters in total, tuning and optimizing these parameters are crucial steps to achieve the best model performance. It's common to perform random or grid search techniques to get the optimal combination of hyperparameters.

4. RESULTS AND DISCUSSIONS

To provide a complete evaluation of our proposed hybrid DL system (i.e., CNN-BiLSTM), the system was compared with two well-known DL-based hybrid reference models (GRU-BiLSTM and GNN-BiLSTM). This section also comprehensively compares the proposed model with recent benchmarks. Table 4 presents the obtained experimental results of our proposed hybrid classifier, evaluated using the IoT Healthcare security dataset for binary classification. It can be observed from Table 4 that the CNN-BiLSTM algorithm performs best, with an accuracy of 99.97%, a precision score of 99.95%, a recall score of 100% and a test loss of 0.0004, which is better compared to the other hybrid DL approaches GNN-BiLSTM and GRU-BiLSTM. GRU-BiLSTM had the lowest accuracy of 99.87% for binary classification, as shown in the graph in Figure 3. The complexity in time and space measures how a method consumes computational resources. The proposed model was examined in the context of the total elapsed time required to better evaluate our proposed working system. The training phase is not included as it was mainly done offline. Testing is critical to show the efficiency and performance of the model. Our proposed hybrid approach took only 1.8 seconds to complete the test of 18870 samples, which is relatively low with GRU-BiLSTM and GNN-BiLSTM with a testing time of 3.07 and 3.35 seconds respectively as shown in Figure 4.

Table 4. Performance evaluation of hybrid DL models used for binary classification tasks

| Models | Accuracy (%) | Precision (%) | Recall (%) | F-measure (%) | Execution time (S) | Memory size (MB) |
|------------|--------------|---------------|------------|---------------|--------------------|------------------|
| CNN-BiLSTM | 99.97 | 99.95 | 100 | 99.97 | 1.8 | 1737.86 |
| GRU-BiLSTM | 99.87 | 99.77 | 99.92 | 99.85 | 3.07 | 2022.72 |
| GNN-BiLSTM | 99.89 | 99.98 | 99.77 | 99.88 | 3.35 | 2180.06 |

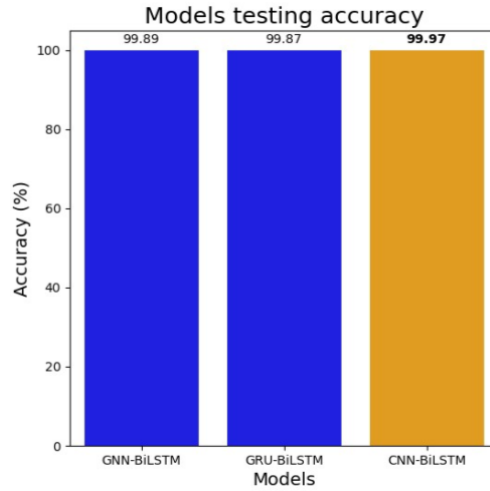


Figure 3. Testing accuracy results of the hybrid DL classifiers

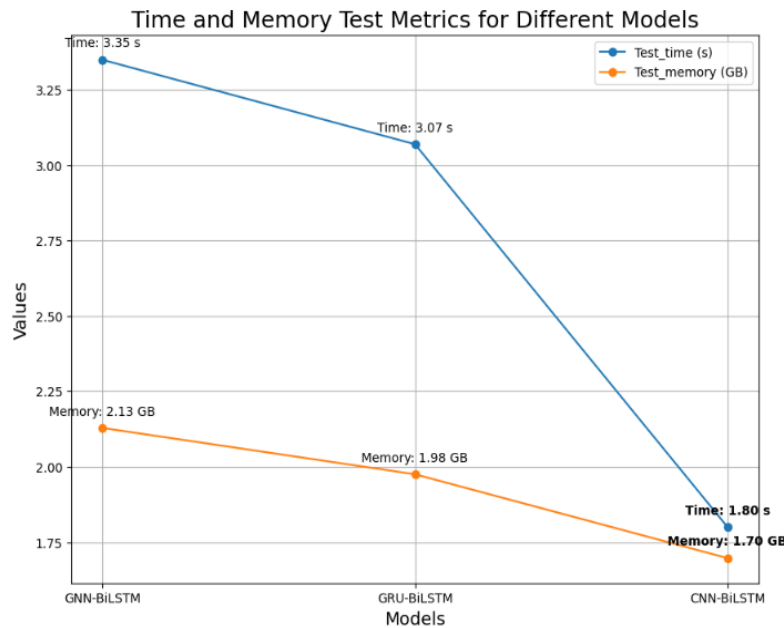


Figure 4. Prediction time (in seconds) and memory size (in GB) of hybrid DL detectors

The CNN-BiLSTM confusion matrix on the IoT-healthcare security test set is shown in Figure 5. A thorough examination of the confusion matrix reveals that the proposed approach correctly identifies the attack samples and misses a few samples (4 malicious samples as normal). The ROC metric can also be used to evaluate the effectiveness of the IDS. Figure 6 shows the ROC curve of CNN-BiLSTM in binary classification on the IoT-healthcare security test set. The proposed technique achieved an AUC of 1.00 for classifying network traffic records as malicious or normal. This indicates the proposed method's robustness and ability to achieve better performance in binary classification. Our proposed hybrid CNN-BiLSTM algorithm was compared with state-of-the-art algorithms for detailed analysis.

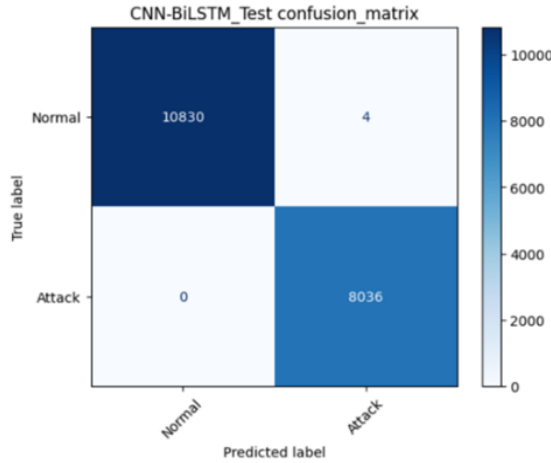


Figure 5. The CNN-BiLSTM confusion matrix

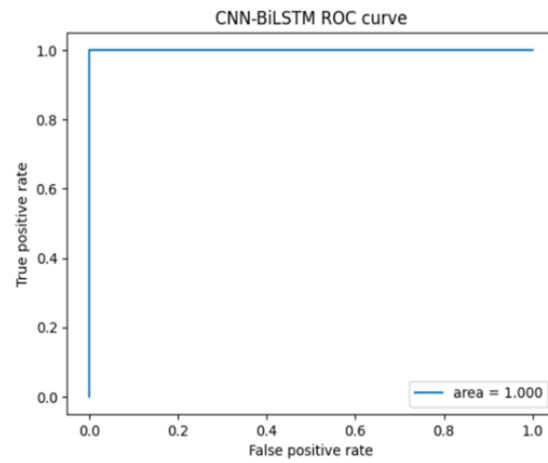


Figure 6. The CNN-BiLSTM ROC curve

As previously mentioned, different datasets are employed for applying the ML and DL algorithms and performing the traffic classification in IoMT network. Furthermore, they may apply different hyperparameters and configurations. Therefore, comparing different hybrid DL-enabled IDSs is complicated based on their experimental results. Table 5 compares related works based on the proposed algorithms, datasets, evaluation metrics, and detection time. According to the findings, our work achieved the best results for binary classification on the IoT-healthcare security dataset compared to other work in the literature and the other two classifiers used in this study, GNN-BiLSTM and GRU-BiLSTM. Indeed, the proposed model obtained the highest accuracy level 99.98% compared to related work [4], [12], [13] which achieved accuracy levels of 99.24%, 99.83%, and 99.01% respectively. Furthermore, when attack samples are tested using our approach, the average network attack detection time is 1.8 seconds. The results demonstrate that our CNN-BiLSTM approach is efficient regarding all performance measures and effectively mitigates cyber-attacks in the IoMT environment.

Selecting network dataset features is typically more challenging when dealing with diverse IoT protocols, including MQTT, AMQP, and CoAP, as well as conventional protocols ICMP, UDP, and TCP. All switches must route network traffic using OpenFlow to the SDN controller, particularly in an SDN-enabled network. Hence, the proposed system provides the optimal performance in a complex IoMT network with minimum effort in feature engineering and selection. However, due to feature self-learning and model weight adaptation, the proposed DL system requires time for training the model [39].

Table 5. Comparison with current related works

| References | Models | Accuracy (%) | Precision (%) | Recall (%) | F-measure (%) | Execution time (S) | Dataset |
|-------------|--------------|--------------|---------------|------------|---------------|--------------------|-------------------------|
| [13] (2020) | MCAD ML | 99.24 | 99.01 | 99.00 | 98.95 | - | Generated |
| [12] (2021) | CNN-LSTM | 99.83 | - | - | - | 1.2 | IoT |
| [4] (2022) | Cu-LSTM+ GRU | 99.01 | 99.04 | 98.80 | 99.12 | 0.019 | CICDDoS2019 |
| Proposed | CNN-BiLSTM | 99.97 | 99.95 | 100 | 99.97 | 1.8 | IoT-Healthcare security |

5. CONCLUSION

This paper presents a hybrid DL-based SDN detection approach to combat sophisticated IoMT attacks. In the proposed approach, an SDN-enabled attack detection mechanism has been used for the IoMT, as SDN efficiently addresses the heterogeneity of the network. Therefore, integrating SDN and IoMT enables accurate network activity monitoring policies to detect malicious traffic. Extensive experiments on the IoT Healthcare security dataset evaluated the performance of the proposed approach. The experimental findings indicate the proposed hybrid CNN-BiLSTM method outperforms the existing benchmark approaches with an accuracy of 99.97%, precision and F1-score of 99.95% and 99.97%, respectively. Moreover, the proposed mechanism has a very low computation time of 1.8 seconds. The CNN-BiLSTM is benchmarked against state-of-the-art IDSs focusing on the same area to provide additional, comprehensive analysis and scalability. While the proposed method excels in various aspects, a potential area for future research involves addressing its limitation in detecting insider attacks. To enhance the system's capabilities, future work will focus on

extending its functionality to identify specific malicious activities such as ransomware and DDoS attacks, providing a more comprehensive and adaptive threat detection framework.




REFERENCES

- [1] M. Centenaro, C. E. Costa, F. Granelli, C. Sacchi, and L. Vangelista, "A survey on technologies, standards and open challenges in satellite IoT," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 3, pp. 1693–1720, 2021, doi: 10.1109/COMST.2021.3078433.
- [2] S. S. Hameed *et al.*, "A hybrid lightweight system for early attack detection in the IoMT fog," *Sensors*, vol. 21, no. 24, 2021, doi: 10.3390/s21248289.
- [3] S. E. Chafi, *et al.*, "Resource placement strategy optimization for smart grid application using 5G wireless networks," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 4, pp. 3932–3942, 2022, doi: 10.11591/ijece.v12i4.pp3932-3942.
- [4] F. Wahab *et al.*, "An AI-driven hybrid framework for intrusion detection in IoT-enabled E-health," *Computational Intelligence and Neuroscience*, vol. 2022, 2022, doi: 10.1155/2022/6096289.
- [5] M. Moradi, M. Moradkhani, and M. B. Tavakoli, "Security-level improvement of IoT-based systems using biometric features," *Wireless Communications and Mobile Computing*, vol. 2022, 2022, doi: 10.1155/2022/8051905.
- [6] R. A. Elsayed, R. A. Hamada, M. I. Abdalla, and S. A. Elsaid, "Securing IoT and SDN systems using deep-learning based automatic intrusion detection," *Ain Shams Engineering Journal*, vol. 14, no. 10, 2023, doi: 10.1016/j.asej.2023.102211.
- [7] S. Liaqat, A. Akhuzada, F. S. Shaikh, A. Giannetsos, and M. A. Jan, "SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT)," *Computer Communications*, vol. 160, pp. 697–705, 2020, doi: 10.1016/j.comcom.2020.07.006.
- [8] R. M. S. Priya *et al.*, "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," *Computer Communications*, vol. 160, pp. 139–149, 2020, doi: 10.1016/j.comcom.2020.05.048.
- [9] B. D. Deebak and F. Al-Turjman, "Secure-user sign-in authentication for IoT-based eHealth systems," *Complex and Intelligent Systems*, vol. 9, no. 3, pp. 2629–2649, 2023, doi: 10.1007/s40747-020-00231-7.
- [10] M. A. Khan, I. U. Din, T. Majali, and B. S. Kim, "A survey of authentication in internet of things-enabled healthcare systems," *Sensors*, vol. 22, no. 23, 2022, doi: 10.3390/s22239089.
- [11] M. Mamdouh, A. I. Awad, A. A. M. Khalaf, and H. F. A. Hamed, "Authentication and identity management of IoT devices: achievements, challenges, and future directions," *Computers and Security*, vol. 111, 2021, doi: 10.1016/j.cose.2021.102491.
- [12] S. Khan and A. Akhuzada, "A hybrid DL-driven intelligent SDN-enabled malware detection framework for internet of medical things (IoMT)," *Computer Communications*, vol. 170, pp. 209–216, 2021, doi: 10.1016/j.comcom.2021.01.013.
- [13] L. M. Halman and M. J. F. Alenazi, "MCAD: A machine learning based cyberattacks detector in software-defined networking (SDN) for healthcare systems," *IEEE Access*, vol. 11, pp. 37052–37067, 2023, doi: 10.1109/ACCESS.2023.3266826.
- [14] T. M. Alshammari and F. M. Alserhani, "Scalable and robust intrusion detection system to secure the IoT environments using software defined networks (SDN) enabled architecture," *International Journal of Computer Networks and Applications*, vol. 9, no. 6, pp. 678–688, 2022, doi: 10.22247/ijcna/2022/217701.
- [15] S. J. Horestani, S. Soltani, and S. A. H. Seno, "A deep neural network architecture for intrusion detection in software-defined networks," *Computer and Knowledge Engineering*, vol. 5, no. 2, 2022, doi: 10.22067/CKE.2022.75815.1055.
- [16] Sharipuddin *et al.*, "Intrusion detection with deep learning on internet of things heterogeneous network," *IAES International Journal of Artificial Intelligence*, vol. 10, no. 3, pp. 735–742, 2021, doi: 10.11591/ijai.v10.i3.pp735-742.
- [17] J. Malik, A. Akhuzada, I. Bibi, M. Imran, A. Musaddiq, and S. W. Kim, "Hybrid deep learning: an efficient reconnaissance and surveillance detection mechanism in SDN," *IEEE Access*, vol. 8, pp. 134695–134706, 2020, doi: 10.1109/ACCESS.2020.3009849.
- [18] D. Javeed, T. Gao, M. T. Khan, and D. Shoukat, "A hybrid intelligent framework to combat sophisticated threats in secure industries," *Sensors*, vol. 22, no. 4, 2022, doi: 10.3390/s22041582.
- [19] A. K. Sarica and P. Angin, "Explainable security in SDN-based IoT networks," *Sensors*, vol. 20, no. 24, pp. 1–30, 2020, doi: 10.3390/s20247326.
- [20] Z. Lv, L. Qiao, A. Kumar Singh, and Q. Wang, "AI-empowered IoT Security for Smart Cities," *ACM Transactions on Internet Technology*, vol. 21, no. 4, 2021, doi: 10.1145/3406115.
- [21] S. Prabakaran *et al.*, "Predicting attack pattern via machine learning by exploiting stateful firewall as virtual network function in an SDN network," *Sensors*, vol. 22, no. 3, 2022, doi: 10.3390/s22030709.
- [22] E. M. Zeleke, H. M. Melaku, and F. G. Mengistu, "Efficient intrusion detection system for SDN orchestrated internet of things," *Journal of Computer Networks and Communications*, vol. 2021, 2021, doi: 10.1155/2021/5593214.
- [23] A. Ahmim, F. Maazouzi, M. Ahmim, S. Namane, and I. B. Dhaou, "Distributed denial of service attack detection for the internet of things using hybrid deep learning model," *IEEE Access*, vol. 11, pp. 119862–119875, 2023, doi: 10.1109/ACCESS.2023.3327620.
- [24] Y. Rbah *et al.*, "Security and privacy on the internet of medical things," *Networking Technologies in Smart Healthcare*, pp. 119–143, 2022, doi: 10.1201/9781003239888-6.
- [25] I. Idrissi, M. Boukabous, M. Azizi, O. Moussaoui, and H. El Fadili, "Toward a deep learning-based intrusion detection system for iot against botnet attacks," *IAES International Journal of Artificial Intelligence*, vol. 10, no. 1, pp. 110–120, 2021, doi: 10.11591/ijai.v10.i1.pp110-120.
- [26] F. Khan, M. A. Jan, R. Alturki, M. D. Alshehri, S. T. Shah, and A. U. Rehman, "A secure ensemble learning-based fog-cloud approach for cyberattack detection in IoMT," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 10, pp. 10125–10132, Oct. 2023, doi: 10.1109/TII.2022.3231424.
- [27] V. Hnamte and J. Hussain, "DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system," *Telematics and Informatics Reports*, vol. 10, 2023, doi: 10.1016/j.teler.2023.100053.
- [28] K. Haseeb, I. Ahmad, I. I. Awan, J. Lloret, and I. Bosch, "A machine learning sdn-enabled big data model for iomt systems," *Electronics*, vol. 10, no. 18, 2021, doi: 10.3390/electronics10182228.
- [29] F. Hussain *et al.*, "IoT healthcare security dataset," *IEEE Dataport*, doi: 10.21227/9w13-2t13.
- [30] S. K. Keshari, V. Kansal, and S. Kumar, "A systematic review of quality of services (QoS) in software defined networking (SDN)," *Wireless Personal Communications*, vol. 116, no. 3, pp. 2593–2614, 2021, doi: 10.1007/s11277-020-07812-2.
- [31] S. Khorsandroo, A. G. Sánchez, A. S. Tosun, J. M. Arco, and R. D. -Corin, "Hybrid SDN evolution: A comprehensive survey of the state-of-the-art," *Computer Networks*, vol. 192, 2021, doi: 10.1016/j.comnet.2021.107981.
- [32] S. E. Chafi, *et al.*, "Cloud computing services, models and simulation tools," *International Journal of Cloud Computing*, vol. 10, no. 5–6, pp. 533–547, 2021, doi: 10.1504/IJCC.2021.120392.




- [33] F. Hussain *et al.*, “A framework for malicious traffic detection in iot healthcare environment,” *Sensors*, vol. 21, no. 9, 2021, doi: 10.3390/s21093025.
- [34] A. Khacha, R. Saadouni, Y. Harbi, and Z. Aliouat, “Hybrid deep learning-based intrusion detection system for industrial internet of things,” *International Symposium on Informatics and its Applications*, 2022, doi: 10.1109/ISIA55826.2022.9993487.
- [35] Y. Rbah *et al.*, “Machine learning and deep learning methods for intrusion detection systems in IoMT: A survey,” *2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology, IRASET 2022*, 2022, doi: 10.1109/IRASET52964.2022.9738218.
- [36] M. Norouzi, Z. G. -Aydın, Ö. C. Turna, M. Y. Yağci, M. A. Aydın, and A. Souri, “A hybrid genetic algorithm-based random forest model for intrusion detection approach in internet of medical things,” *Applied Sciences*, vol. 13, no. 20, Jan. 2023, doi: 10.3390/app132011145.
- [37] E. Yıldırım, M. Cicioğlu, and A. Çalhan, “Fog-cloud architecture-driven internet of medical things framework for healthcare monitoring,” *Medical & Biological Engineering & Computing*, vol. 61, no. 5, pp. 1133–1147, 2023, doi: 10.1007/s11517-023-02776-4.
- [38] J. Du, K. Yang, Y. Hu, and L. Jiang, “NIDS-CNNLSTM: network intrusion detection classification model based on deep learning,” *IEEE Access*, vol. 11, pp. 24808–24821, 2023, doi: 10.1109/ACCESS.2023.3254915.
- [39] R. Chaganti, W. Suliman, V. Ravi, and A. Dua, “Deep learning approach for SDN-enabled intrusion detection system in IoT networks,” *Information*, vol. 14, no. 1, 2023, doi: 10.3390/info14010041.

BIOGRAPHIES OF AUTHORS






Yahya Rbah    born in 1993 in Taourirt (Morocco), is a Ph.D. student in Computer Science, at the National School of Applied Sciences, Sidi Mohamed Ben Abdellah University of FES, Morocco. He holds a Master degree in Internet of Things and Mobile Systems from National School of Applied Sciences, Sidi Mohamed Ben Abdellah University of FES in 2018, and a Professional License in Networks and Telecommunication from the Faculty of Sciences of Rabat, University of Mohammed V in 2016. His research focuses on computer systems, networks, and security, data science, and software engineering. He can be contacted at email: rbah.yahya@gmail.com.






Mohammed Mahfoudi    born in 1986 in Sefrou, Morocco. He earned a graduate engineer degree in Telecommunications and Networks from the National School of Applied Sciences of Fez in 2010. His professional journey includes roles as a Technical Support Engineer at Huawei Technology and a trainer at the Superior Institute of Applied Technologies. Mahfoudi later achieved a Ph.D. in Telecommunications from Sidi Mohamed Ben Abdellah University, Fez. Presently, he serves as an Assistant Professor at Abdelmalek Essaadi University. He can be contacted at email: m.mahfoudi@uae.ac.ma.






Mohammed Fattah    received his Ph.D. in Telecommunications and CEM at the University of Sidi Mohamed Ben Abdellah (USMBA) Fez, Morocco, 2011. He is a professor in the Department of Electrical Engineering of the High school of technology at the Moulay Ismail University (UMI), Meknes, Morocco and he is a responsible of the research team 'Intelligent Systems, Networks and Telecommunications', IMAGE laboratory, UMI. He can be contacted at email: m.fattah@umi.ac.ma.






Younes Balboul    is a professor at the National School of Applied Sciences at Sidi Mohamed Ben Abdellah University (USMBA) in Fez, Morocco. He is also a 2010 graduate of the National Institute of Posts and Telecommunications (INPT) in Morocco, where he earned a degree in engineering. He is a member of the Laboratory of Artificial Intelligence, Data Sciences, and Emerging Systems. He can be contacted at email: younes.balboul@usmba.ac.ma.






Kaouthar Chetioui    is a professor researcher in ENSA, Sidi Mohamed Ben Abdellah University, Fez, Morocco. She received the Ph.D. degree on Networks and Information Security from University Mohammed V in Rabat, Morocco, in 2017. She is a technical program member at several international conferences. Obtained several certifications from Ec-council, Fortinet, AWS, Juniper, Huawei, Cisco and Microsoft on Cloud computing, security and networking. Her research interests include systems security, network security, and security in IoT. She can be contacted at email: kaoutharchetioui@gmail.com.






Said Mazer    born in 1978. He received the Ph.D. degree in electronics and signal processing from the University of Marne-La-Vallée, Champs-sur Marne, France. He is currently a full Professor with the National School of Applied Sciences of Fez, Morocco. He is member of IASSE Laboratory, University of Sidi Mohamed Ben Abdellah Fez. His research interests include the development of microwave-photonics devices for radio-over fibre and wireless applications and he is involved in network security. He can be contacted at email: said.mazer@usmba.ac.ma.



Moulhime El Bekkali    holder of a doctorate in 1991 from the USTL University - Lille 1- France, he worked on antennas printed and their applications to microwave radar. Since 1992, he was a professor at the Graduate School of Technology, Fez (ESTF) and he was a member of the Transmission and Data Processing Laboratory (LTTI). In 1999, he received a second doctorate in electromagnetic compatibility from Sidi Mohamed Ben Abdellah University (USMBA). Currently, he works in the telecommunication domain, he is a professor at the National School of Applied Sciences (ENSAF) and member of the LIASSE laboratory at Sidi Mohamed Ben Abdellah University. He can be contacted at email: moulhime.el.bekkali@gmail.com.



Benaissa Bernoussi    born in 1959. He received the Ph.D. degree in applied mathematics from the University of Perpignan, France. He is currently a Professor with the National School of Applied Sciences of Fez, Morocco. He is membre of IASSE Laboratory, University of Sidi Mohamed Ben Abdellah Fez. He is involved in numerical analysis, cryptography and cloud computing. He can be contacted at email: bbernou@gmail.com.