

Securing an IoT Medical System Using AI and a Unidirectional Network Device: Application to a Driver

Georges EL HAJAL^a, Roy ABI ZEID DAOU^{b, c1}, Yves DUCQ^a and Josef BOERCSOEK^d

^a Univ. Bordeaux, IMS laboratory, France

^b Biomedical Technologies Department, Lebanese German University, Lebanon

^c MART Learning, Education and Research Center, Chananir, Lebanon

^d University of Kassel, Institute for Computer Architecture and System Programming, Germany

Abstract. Security in systems and networks has always been a major issue for IT administrators. When it comes to medical applications, this concern is much more important due to the sensitivity of data and the risks that may be caused due to alteration or falsification of such critical information. The proposed paper presents a solution to assure the best security possible in such an environment. Thus, based on an application that monitors a driver's health while driving his car, a data diode will be implemented in order to assure security of the system by forcing unidirectional flow of network data to the healthcare provider side. Added to that, an AI-based program will be developed to verify the confidentiality, the integrity and the availability of the exchanged data and to check the patient health for abnormalities. Every sub-part of the system has been tested separately and results have shown that falsified data has been filtered out of the received end, e.g. the healthcare provider side.

Keywords. Cyber physical security, driver health, integrity, availability and confidentiality of data, unidirectional network device, AI algorithms

1. Introduction

The internet of things, or IoT, is a system of interrelated computing devices communicating through the internet allowing them to send and receive data. It allows the interaction between the physical world and the digital world. Sensors and actuators interact with the physical world and transform the data to the digital world. IoT technologies are contributing in the significant growth of generated data from medical appliances. Moreover, data security, confidentiality, integrity and availability are the challenges facing IoT applications and platforms due to the fast involvement of distributed diverse devices [1].

The eminence of IoT devices has been coupled with the increase of security vulnerabilities and exploitation. Most IoT systems utilize an architecture focusing on the connectivity with the cloud servers via gateways. Unfortunately, privacy and security risks are severe consequences of this architecture [2]. The communication between sensors and the IoT gateways might also be very susceptible to attack. Distributed

¹ Corresponding author, email: r.abizeiddaou@lgu.edu.lb

Denial-of-Service (DDoS) attacks can result in significant infrastructure collapse when targeting cloud servers. Moreover, a centralized server presents a risk to the entire system in case of a malware infection by generating a single point of failure.

In addition, IoT systems are not homogeneous in terms of security requirements, resource availability and networked devices. The devices operate in an open environment, which yields to increasing cyber physical risks and accessibility by adversaries.

The proposed application is integrated for drivers when doing their driving activity. Some sensors are deployed to measure their vital signs continuously and to inform healthcare providers whenever a medical issue is encountered. This is mainly applied for drivers having a medical history as heart failure, diabetes or even epilepsy. Thus, the main objective is to provide a secured transmission of data in order to make sure that the healthcare provider, or even the developed software, takes the right decision concerning the driver's health.

The proposed application is implemented for elderly people and being monitored remotely by healthcare providers; so, the proposed system relied on a telemedicine approach. Thus, the objective of this work is to make sure that the same data, sent from the patient side, is securely received for analysis by the healthcare provider to ensure the best follow up possible to this category of people.

Safety and security are highly recommended since this application deals with medical data. Thus, this paper will present a novel approach to ensure that the data, sent by the patient's device and processed by the healthcare provider tools, is authentic, confidential and available. The architecture of this systems consists of three main entities: the patient part where the sensors are placed, a gateway server that receives the data collected from the different patients to forward them to the required healthcare provider and the healthcare backend server that receives and analyses the data. So, to reach this objective, the proposed solution consists of two layers:

- a hardware layer of defense provided by installing a data diode (a unidirectional hardware device) between the gateway server and the backend server;
- a software layer of defense provided by an AI-based software installed on the gateway server. This software must identify, authenticate the receiver and check the data.

Thus, the novelty of this solution consists of presenting a solution combining both software and hardware to provide security for the overall system. This multi-layer security approach is not being adopted in almost all applications.

The rest of the paper is organized as follows. In Section 2, the applied tools and a description of the proposed solution will be presented. Section 3 shows the implementation of the proposed solution, also the analysis and the obtained results will be presented. Finally, Section 4 ends up with a conclusion and proposes some future works.

2. Proposed Solution

As already presented, the solution consists of two main levels: the unidirectional data diode and the AI-based software. Figure 1 shows the architecture of the system before and after implementing the solution. In more details, the figure to the left represents the three entities (*i.e.* the patients' sensors, the gateway server and the healthcare provider server) whereas the figure to the right represents the security add ins, mainly implemented in the intermediate layer.

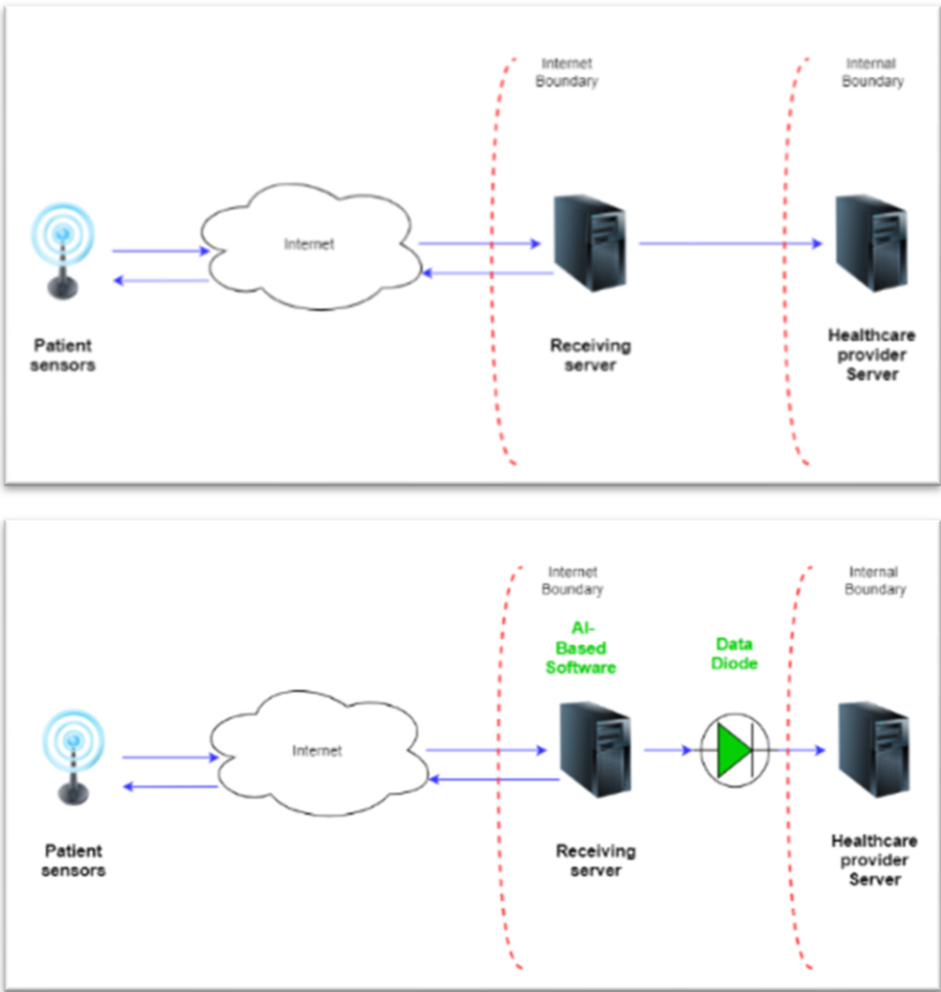


Figure 1. System architecture without (to the left) and with (to the right) the security modules/protocols
In more details, the system consists of three entities:

- A patient equipped by a heart rate sensor and a SpO2 sensor to check his health while driving;
- A gateway server (IoT gateway) to receive the health data of multiple patients using this application. An AI-based software will monitor the incoming data to check for irregularities from the network and device perspectives, *i.e.* the IP, the time frame between sending of consecutive data, the formatting, etc... Also, it checks the health of the patient for abnormal measurements, and notifies the healthcare provider to reassess the patient health to contact him in case of a major problem;
- The healthcare provider's server that is used to monitor the patients' health.

Note that the unidirectional network device (Data Diode) will be installed between the IoT gateway and the healthcare provider's server to protect the internal system from malicious attacks [3].

Although not all vulnerabilities have been resolved, this work deals with most frequent and common ones according to OWASP API top ten security list [4].

Concerning the hardware layer, using an air gapped (isolated) network has been the most effective way to ensure that a network can't be compromised remotely. Air gapped systems ensure that, in case of a cyber security attack, no data can be communicated to the outside. The two most famous frameworks for cyber-attacks, the Lockheed Martin Cyber Kill Chain [5] and the MITRE ATT&CK [6] have described in their approaches the reconnaissance and the communication with the Command and Control (C&C) as vital for the success of any Cyber-attack. Data diodes provide security from these two phases because of the physical nature of unidirectional flow of data that doesn't allow the devices to interchange information.

As for the software layer, an AI-based software is installed on the input side of the exchange server to assess data transferred to the inside and to block any malicious action. Using Artificial Intelligence applications provide great security features, high transparency and enhance efficiency[7]. The development of edge computing permitted data generated by the IoT devices to be transferred to the edge gateways for further process and analysis before being forwarded to the servers that are used by the monitoring personnel.

Figure 2 represents a DFD to show the way data flows from the patient's side to the healthcare provider end considering all security measurements proposed in this solution.

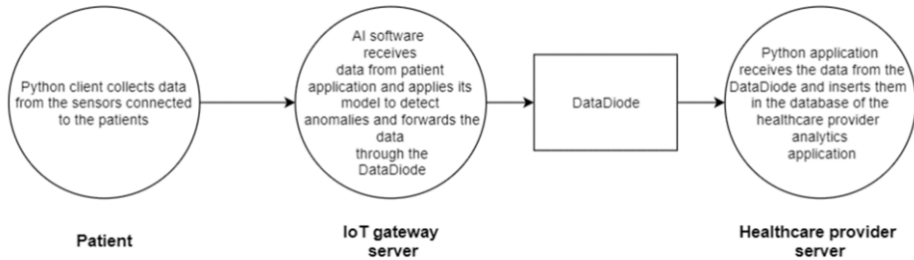


Figure 2. Scenario for the flow of data from the patient side to the healthcare provider backend

3. Implementation of the Proposed Solution

The solution divides the system into two segments: The first segment is the one between the patient (*P*) and the exchange server (the IoT gateway in this application) (*IoTg*), whereas the second segment is the one between the *IoTg* and the server of the healthcare provider (*HcP*).

On the patient's side, a *raspberry pi zero* is equipped by an SPo2 sensor, heart rate sensor, and a GPS hat with 3G/4G & LTE Base HAT. The data of the patient is sent using a python script that collects all data from the sensors and send them to a Python Web application on the *IoTg* server via an Internet connection. The *IoTg* is connected to the input part of the Data Diode and the output part of the Data Diode is connected the server of the medical healthcare personnel. The AI application controls the sending of data from the input part and a python application handles data reception on the output part of the Data Diode to insert it in the database of the healthcare provider analytics application.

The preparation of the data for machine learning is essential in order to generate a model capable of detecting the anomalies later on. So, at first, the data was collected and

analysed. The anomalies detected and considered a priority to be handled by the system were:

- 1- Only the SPo2 value is different with more than 20% value deviation relative to the average of the patient.
- 2- Only the heart rate value is different with more than 20% value deviation relative to the average of the patient.
- 3- Attack on the API itself by a malicious actor.
- 4- Traffic is coming from the same user agent but from the different IP.
- 5- Traffic is coming from the different user agent but from the same IP.
- 6- SQL injection on the Web Application.
- 7- All the data is correct but different IP of original patient.
- 8- The data sent by the user is not within the specified interval.

To train the AI/ML algorithms the following features were selected: user, spo2 value, heart rate value, GPS longitude value, GPS latitude value, date and time, IP, user-agent as shown in Figure 3 below.

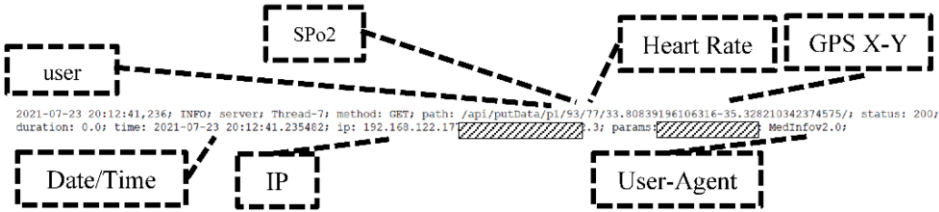


Figure 3. Features used for training AI/ML algorithms

The second step was to collect and label the data. We collected data values of normal traffic, then data values with medical issues, and at last, data values after simulating cyber-attacks using hping3 [8] to perform a DOS attack and Ettercap [9] for Man In the Middle attack from a KALI Linux machine. Our final dataset contained 27% normal traffic, 38% medical issue traffic and 35% cyber-attack related traffic.

Matlab R2018a was used to help us determine the best machine learning classifier that can achieve the highest accuracy. After applying 23 machine learning algorithms that are shown in Figure 4 below, some gave us a 100% accuracy while others gave us 37.9% accuracy. Added to that, we noticed that the KNN algorithm was the best for our data since it gave us 100% accuracy in all its variances. Based on these results, *KNeighborsClassifier* was used from “scikit-learn” [10] to be implemented in the python AI application.

KNN is a supervised classification algorithm. It generated new data points based on the closest data points or the k number. The latter should be large enough to limit noise in data, but also small enough in order not to interfere with the other classes [11]. So, different values of k were calculated in order to preserve the accuracy. For each value, the mean error was calculated. Figure 5 shows the accuracy value with respect to the value of k . Thus, one can find that any value below 19 is a good value for k .

1.1 ☆ Tree Last change: Fine Tree	Accuracy: 100.0% 8/8 features	1.13 ☆ KNN Last change: Medium KNN	Accuracy: 100.0% 8/8 features
1.2 ☆ Tree Last change: Medium Tree	Accuracy: 100.0% 8/8 features	1.14 ☆ KNN Last change: Coarse KNN	Accuracy: 100.0% 8/8 features
1.3 ☆ Tree Last change: Coarse Tree	Accuracy: 96.4% 8/8 features	1.15 ☆ KNN Last change: Cosine KNN	Accuracy: 100.0% 8/8 features
1.4 ☆ Linear Discriminant Last change: Linear Discriminant	Accuracy: 83.2% 8/8 features	1.16 ☆ KNN Last change: Cubic KNN	Accuracy: 100.0% 8/8 features
1.5 ☆ Quadratic Discriminant Last change: Quadratic Discriminant	Failed 8/8 features	1.17 ☆ KNN Last change: Weighted KNN	Accuracy: 100.0% 8/8 features
1.6 ☆ SVM Last change: Linear SVM	Accuracy: 89.7% 8/8 features	1.18 ☆ Ensemble Last change: Boosted Trees	Accuracy: 37.9% 8/8 features
1.7 ☆ SVM Last change: Quadratic SVM	Accuracy: 100.0% 8/8 features	1.19 ☆ Ensemble Last change: Bagged Trees	Accuracy: 100.0% 8/8 features
1.8 ☆ SVM Last change: Cubic SVM	Accuracy: 100.0% 8/8 features	1.20 ☆ Ensemble Last change: Subspace Discriminant	Accuracy: 79.7% 8/8 features
1.9 ☆ SVM Last change: Fine Gaussian SVM	Accuracy: 100.0% 8/8 features	1.21 ☆ Ensemble Last change: Subspace KNN	Accuracy: 99.4% 8/8 features
1.10 ☆ SVM Last change: Medium Gaussian SVM	Accuracy: 99.7% 8/8 features	1.22 ☆ Ensemble Last change: RUSBoosted Trees	Accuracy: 37.9% 8/8 features
1.11 ☆ SVM Last change: Coarse Gaussian SVM	Accuracy: 96.5% 8/8 features	2 ☆ Quadratic Discriminant Last change: 'Covariance structure' = 'Diagonal'	Accuracy: 42.3% 8/8 features
1.12 ☆ KNN Last change: Fine KNN	Accuracy: 100.0% 8/8 features		

Figure 4 . Applied Machine learning algorithms and results

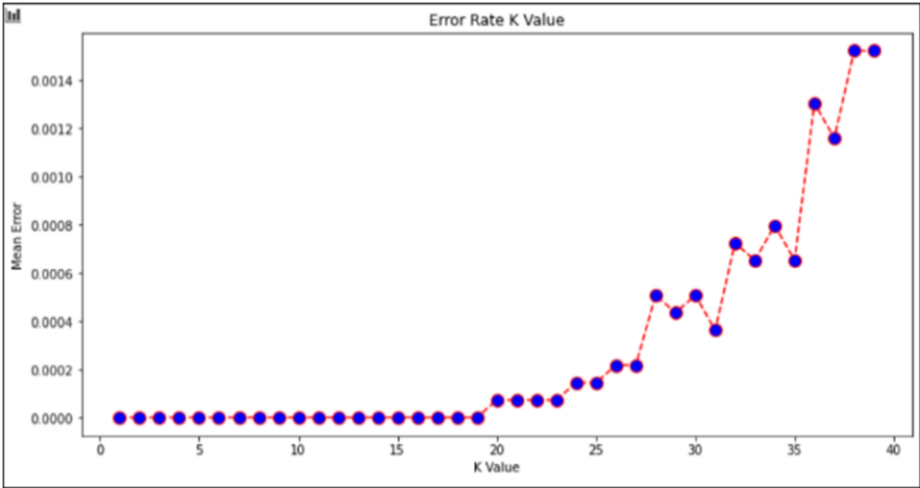
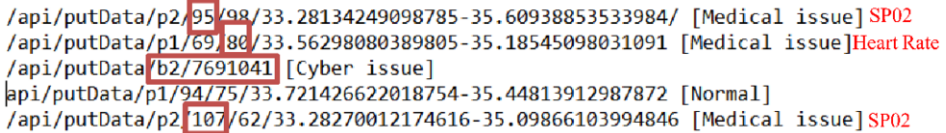


Figure 5. K-value vs Mean Error Value

Finally, the provided classifier was used in the AI application. The application will continuously read the received data and use the classifier to predict its nature and acts accordingly upon it. If it is normal traffic, the data is forwarded to the healthcare provider through the data diode. If it is a medical issue, the data will be labelled with a warning to notify the healthcare provider upon receipt. If it is classified as a cyber-attack, the application will block the IP of the sender and notifies the IT admin of the system of the issue. Figure 6 shows how the AI application is working flawlessly.



```

/api/putData/p2/95/98/33.28134249098785-35.60938853533984/ [Medical issue] SP02
/api/putData/p1/69/80/33.56298080389805-35.18545098031091 [Medical issue]Heart Rate
/api/putData/b2/7691041 [Cyber issue]
/api/putData/p1/94/75/33.721426622018754-35.44813912987872 [Normal]
/api/putData/p2/107/62/33.28270012174616-35.09866103994846 [Medical issue] SP02

```

Figure 6. AI application detecting normal or medical issues or Cyber issues.

From the Healthcare provider end, a python application will receive the data and forward them to the application used by the healthcare personnel to monitor the system.

After applying the AI algorithm, the hitting percentage was 100 for the KNN algorithm as 75% of the 54.000 packets were used for the training and 25% were used for testing. Added to that, neither the AI algorithm nor the data diode have caused any delay on data transmission between the patient device and the healthcare provider as time recordings were achieved first without implementing the security tools and it was then achieved after implementing the different peripherals and the time differences were very small, almost neglected.

4. Conclusions and future works

In the paper, an AI-based algorithm was implemented as a tool in the IoT gateway to ensure secure data transactions between the IoT distributed application. Added to that, to further enhance security, a unidirectional device known as Data Diode from our previous work [3] can provide additional layer of protection to the overall system.

The following main contributions are listed below:

1. Proposition of a novel architecture for IoT edge computing of medical devices to ensure security and privacy of transferred data. The proposed architecture uses mobile IoT technologies for communication;
2. Implementation of an AI-based application model to secure and authenticate framework for IoT devices in order to protect the sensor nodes' sensitive data from cyber-attacks. Furthermore, this solution provides automation of the threat detection and notification diffusion;
3. Experimental evaluation performance metrics of the proposed architecture regarding throughput, network usage, computational resources, transaction latency, and communication costs.

Building upon this work, our next step is to ameliorate our AI to secure the platform by classifying and prioritizing vulnerabilities based on aggregation of multiple sources of inputs such as CVSS score, the Exploit DB and other PoC providing websites.

References

- [1] J. Granjal, E. Monteiro and J. Sá Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," *IEEE Communications Surveys Tutorials*, vol. 17, no. 3, pp. 1294-1312, 2015.
- [2] H. Garg and M. Dave, "Securing IoT Devices and SecurelyConnecting the Dots Using REST API and Middleware," in *4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 2019.
- [3] G. EL HAJAL, R. DAOU ABI ZEID, Y. DUCQ and J. Börcsök, "Designing and validating a cost effective safe network: application to a PACS system," in *Fifth International Conference on Advances in Biomedical Engineering (ICABME)*, Tripoli, Lebanon, 2019.
- [4] OWASP, "OWASP API Security Project," [Online]. Available: <https://owasp.org/www-project-api-security/>. [Accessed 07 2021].

- [5] L. Martin, "the Cyber Kill Chain," 07 2021. [Online]. Available: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>.
- [6] T. M. Corporation, "MITRE ATT&CK," 07 2021. [Online]. Available: <https://attack.mitre.org/>.
- [7] M. Dhingra, M. Jain and R. Jadon, "Role of artificial intelligence in enterprise information security: A review," in Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2016 .
- [8] "hping3," 2021. [Online]. Available: <https://tools.kali.org/information-gathering/hping3>.
- [9] "ETTERCAP," 2021. [Online]. Available: <https://www.ettercap-project.org/>.
- [10] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot and E. Duchesnay, "Scikit-learn: Machine Learning in {P}ython," *Journal of Machine Learning Research*, vol. 12, pp. 2825--2830, 2011.
- [11] K. Taunk, S. De, S. Verma and A. Swetapadma, "A Brief Review of Nearest Neighbor Algorithm for Learning and Classification," in *International Conference on Intelligent Computing and Control Systems (ICCS)*, Madurai, India, 2019.