International Journal of Medical Engineering and Informatics

ISSN online: 1755-0661 - ISSN print: 1755-0653
https://www.inderscience.com/ijmei

Anomaly detection architecture for smart hospitals based on machine learning, time series, and image recognition analysis: survey

Somaya Haiba, Tomader Mazri

DOI: 10.1504/IJMEI.2023.10058832

Article History:

Received:	11 October 2022
Last revised:	08 April 2023
Accepted:	07 July 2023
Published online:	18 November 2025

Anomaly detection architecture for smart hospitals based on machine learning, time series, and image recognition analysis: survey

Somaya Haiba* and Tomader Mazri

Networks and Telecommunication Systems,
Advanced Systems Engineering Laboratory,
Department of Electrical Engineering,
National School of Applied Sciences,
Kenitra, Morocco
Email: somaya.haiba@uit.ac.ma
Email: Tomader.mazri@uit.ac.ma
*Corresponding author

Abstract: Smart hospital networks are considered the most sensitive networks for anomalies; any tiny existence might produce very different dangerous scales. The usual anomaly detections dedicated to this kind of network are not able to analyse all the different categories and proprieties of the generated data, because the majority of them rely only on time series analysis which is not able to cover all the circulated pieces of information. For that, in this paper, we will survey a proposed anomaly detection architecture that can dominate all the data categories that exist inside the e-health network using image recognition as well as time-series analysis.

Keywords: E-healthcare monitoring network; IoMT; smart hospitals; E-health anomaly; anomaly detection; machine learning; time-series analysis; IoT security; ImageGray analysis; medical data; Cybersecurity.

Reference to this paper should be made as follows: Haiba, S. and Mazri, T. (2025) 'Anomaly detection architecture for smart hospitals based on machine learning, time series, and image recognition analysis: survey', *Int. J. Medical Engineering and Informatics*, Vol. 17, No. 7, pp.1–14.

Biographical notes: Somaya Haiba a PhD student at the Advanced System Engineering Laboratory at the National School of Applied Sciences, Kenitra. She starts her researcher at 2020 in IoMT cybersecurity.

Tomader Mazri earned his HDR in Networks and Telecommunications Systems from Ibn Tofail University. He obtained his PhD in Microelectronics and Telecoms from Sidi Mohamed Ben Abdellah University/INPT in Rabat. He is currently a Professor at the National School of Applied Sciences of Kenitra and a permanent member of the Department of Electrical Engineering, Networks and Telecommunication Systems and Advanced System Engineering Laboratory. He is a Professor of Networks and Telecommunication Systems, ENSA Kenitra

1 Introduction

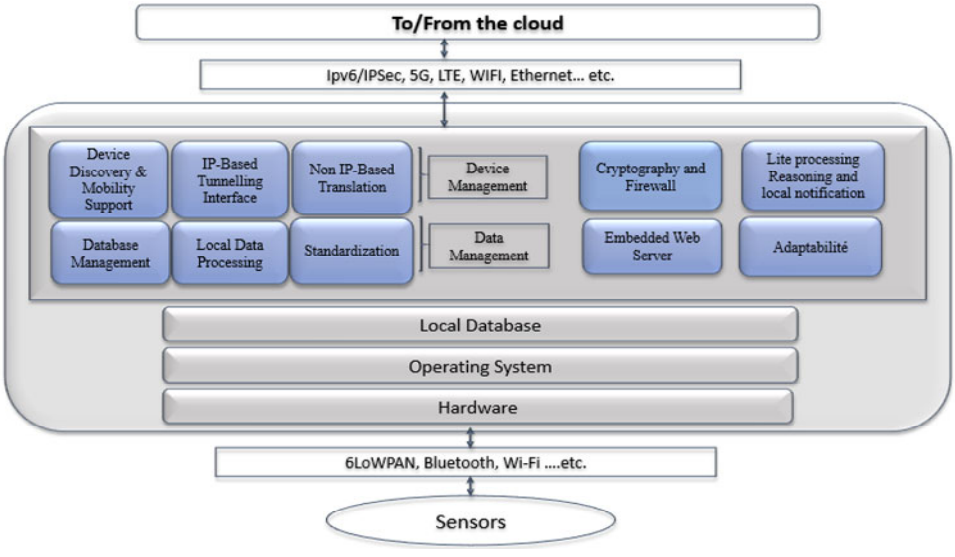
E-healthcare systems are directly associated with human lives, so it has the priority to respond the high availability and high performance as much as possible (Pramanik et al., 2019). For that, we will try to study how possible we can reach a high-quality anomaly detection, knowing that is hard to manage the security and the use safety of the large mass market-oriented internet of medical things (IoMT) devices with any data protection, or security management that they came with. Furthermore, the majority of the existing anomaly detection directed to IoT networks may not cover all the specific data that exist inside such a network as smart hospitals. The E-healthcare monitoring system is a network system based on the newest digital technologies like the IoMT and telecommunications tools to deliver healthcare services when healthcare staff and patients indirectly interact with each other (Hameed et al., 2015). After what we experienced in the COVID-19 pandemic, these kinds of systems are highly bespoke. But the real implementation is still in the earliest stage cause of many reasons, such as being unsure of the circulated data and the distributed device security (Azeez and der Vyver, 2019). Including IoMT devices in healthcare, is a huge and risky step. The distribution of mobile-connected materials inside a smart hospital network means in the cybercriminal term the distribution of opportunities to break down this network especially, that the majority of people are not aware of the secure use of this kind of device, the thing that can produce a lot of types of anomalies. Knowing that this kind of issue is unacceptable in multiple areas, in E-healthcare monitoring networks (Alghanmi, 2022). The global meaning of an anomaly is any unexpected variation in the usual data patterns, or also any extra event that does not conform to the expected workflow (Chandola, 2009). Indeed, it would be triggered for the analytical data, if, for example, the device does not allow some values to be overtaken or a specific rest timer is exceeded for a certain period (Diro et al., 2021). Otherwise, the existence of any inexplicable change can be identified as an anomaly, especially if it breaks the normal pattern of the particular metric data (Haji and Ameen, 2021). So, anomaly detection comes to detect such patterns whose behaviour is considered abnormal as compared to normal nodes (Said et al., 2021). While detecting anomalies inside intelligent systems in real-time is becoming more and more challenging due to the including of all the big data of our days. The old approaches such as visualisations and dashboards can not keep track of the velocity of today's IoT anymore (Canedo and Skjellum, 2016). Therefore, we will propose an architecture of detection dedicated to the E-healthcare network, especially the smart hospital networks, and survey the adequate techniques that would be appropriate, following these sections; First, we will give an overview of the architecture's services in the E-health system based on IoMT. secondly, we identify the types of anomalies that can exist inside this kind of system. Then in the last section, we present our proposed architecture of anomaly detection suitable to the characteristics of the studied network data.

2 Smart hospitals architecture

The smart hospital architectures are built to share information as digital records of the patient chart in real-time with several entities (Rodrigues et al., 2016). It is generally deployed by the IoMT technologies which are integrated with the fog layer and cloud. It splits the entire system into four global areas, each one has its functionalities and priorities to manage and treat the collected data from several IoMT sensors. In general, the smart hospital networks are provided by an architecture of, IoMT devices responsible for continually collecting the patient vital signs, microcontrollers are responsible in their turn for unifying the patient data, and the fog devices where the pre-processed functionality will be done. All the collected data are transferred to the cloud as the final stage for storage and more processes (Monteiro et al., 2018).

- IoMT: These devices are the fastest-growing sector of the IoT market. Its value was predicted to reach $176 billion in 2026 (Bonetto et al., 2012). As known there is a different mock-ups of these devices so, it is necessary to standardise the collected data before sending it to the fog layer due to the heterogeneous formats that the data may take (Talaminos-Barroso, 2016).
- The microcontroller: This is responsible for data integration. It is a microchip self-contained computer. It relates to the sensors. In general, it enables connectivity and control for things that are desired to connect to the internet. To fulfill, the prototype of this architecture, the 32 bits microcontrollers are highly deployed in appliances and medical devices. It offers some standard security features like protection from tampering, reverse engineering, a cryptographic bootloader, a cryptographic hardware accelerator, and memory protection Units. Furthermore, it provides an interface with wide communication standards and diverse references of devices.
- Fog layer: It is a tie that stretches from the external, edges of where data is generated to where it will be stored, whether in the cloud or any internal data centre (Azeez and der Vyver, 2019). Generally, they are a set of smart gateways. The fog layer adds the missing features that data needs to be pushed to the cloud and provides the required local analysis for the data (Rahmani et al., 2018; Monteiro et al., 2018). The newest Fog Framework offers more possibilities for processing data appropriately to quickly respond to urgent incidents. The E-healthcare monitoring systems differentiate from the other IoT applications by having several used features of remote monitoring which require a high degree of reliability and security. The edge and fog computing in the healthcare paper review represents in detail the provided qualities of fog and explains its benefits for E-healthcare network monitoring (Dash et al., 2019).
- The cloud layer: Where the data was stored and analysed on a larger scale. Here, some public clouds are highly recommended, such as Amazon, due to their flexibility of management and high availability (Al-Issa et al., 2019).

Figure 1 Fog layer and its services (see online version for colours)



Source: Dash et al. (2019)

3 E-health-care networks anomalies

The E-healthcare network based on IoMT is like any other network which integrates IoT technologies (Costin et al., 2018). The misunderstanding of what we are handling, increases the alerts of wrong decisions incidents, leading to a risk of setting up more security breaches (Chandola, 2009). For that well recognising what and how are the outliers the used ADS must alerts is essential. An anomaly by definition represents a specific data point that exits outside the norm or indicates random irregularity, or deviation out of the context (Ahmed, 2018). Often known as outliers and they can result from several causes like an intrusion attack on one or a set of devices (Hady et al., 2020). We can global the types of anomaly behaviour into three global categories

- Point-wise anomalies present the individual data instances that don't shape with the expected pattern in a dataset, usually, they are caused by individual device damage, an intrusion attack, or just an anomalous record.
- The Collective anomaly is a subset of the data which is an outlier within the entire dataset, they are called a collective outlier. These types are flagged only when we examine discrete time series together. The individual points do not deviate from the normal in a specific range of observation, they are more significant within a combination.
- Contextual anomalies or also conditional outliers; refer to a significant data point that deviated from the normal data points in a certain context. the difference in this type of anomaly depends on the context of the given data, which means the same normal instance in a given context can be abnormal in another one. This anomaly type is driven by combining the behavioural features and contextual because

observing the same point through different contexts will not always indicate a deviation of the behaviour (Asfaw et al., 2010).

E-healthcare data anomalies usually are a result of attacks defined as "illegitimate access or disclosure of the protected health information that compromises the privacy and security of it" (Seh et al., 2020). The researchers cluster the E-healthcare data breaches into six types reported by Privacy Rights Clearinghouse from 2005 until 2019; hacking, intentional insider attacks, physical damage, loss or theft of portable devices, stationary computer loss, and unknown approaches. The analysis illustrates that it was in height exponential year after year at the time of the study, this exposure was most of the time caused by hacking attacks, which is evident that the E-healthcare industry has always been the favourite target for hackers especially after including the insecure IoMT within the unattended system this compromising 90.49% of health records will be exposed in our days (Haji and Ameen, 2021).

4 The detection model within smart hospitals

To distinguish between benign and anomaly data we must know what are the data proprieties that circulate within the studied networks. The smart hospital, in general, generates digital records from patients' charts in real-time, it provides information patient-centred which must be available securely and instantly to authorised users (Rodrigues et al., 2016). This kind of data includes information from all clinicians engaged in treating patients, and that means different data types need to be manipulated efficiently and classified to get the purpose of our study. The E-health data are usually as medical images, biomedical signals, local analytics data mining to mine the vast unstructured biomedical literature, or multi-level analytics (Pramanik et al., 2019). Thus, we can rely on two types of analysis based on; Time-series model data are usually used to describe the dependencies of the response on a predictor variable. This method is necessary to make a set of inferences from source data by calculating the correlation through repeated responses over time, it simplifies the analysis and the observation of the huge data behaviour. And ImageGray is an image recognition detection technique based on ML analyse relies on automated recognition of patterns and regularities in gray images data, which proves its qualification in several fields like image analysis, bioinformatics data, data compression, and computer graphics it also implements ML models to automate the image analysis and define its component. As we explain above the E-healthcare domain differentiates from the other IoT applications by having the most used feature of remote monitoring with sophisticated circulated data which requires a high degree of reliability. The protection of the healthcare network is highly essential (Ukil et al., 2016). Therefore, we chose to centralise the detection of anomalies by implementing the analysis along with the Fog layer, to improve efficiency and reduce the amount of data transported to the cloud (Rahmani et al., 2018). Taking into consideration that this layer of smart hospital architecture responds to almost resources that this kind of analysis needs especially for those based on machine learning. The proposed approach detects the most anomalies sophisticated in our target networks, analysing all the data circulated without infecting the entire workflow of the network.

4.1 Related work

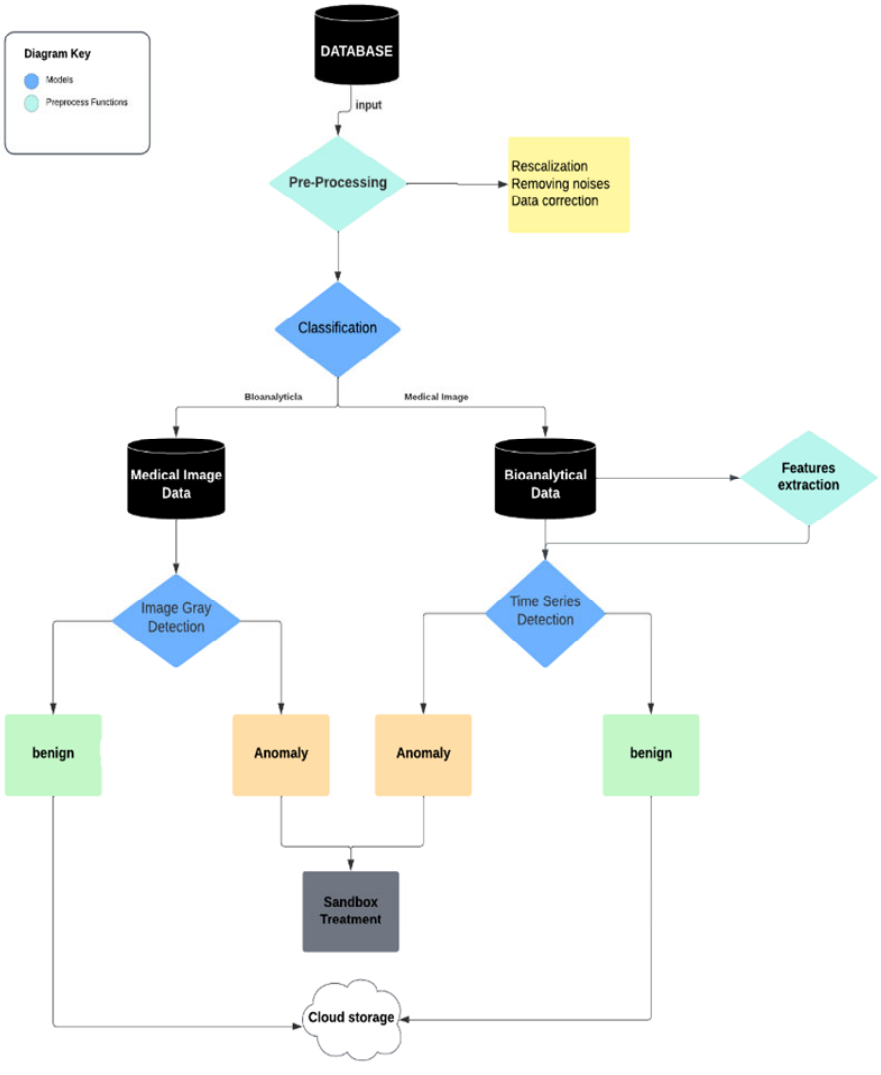
In electronic medical domains, anomaly detection applications handle data patient records which Consist of several data types and features (Chandola, 2009). It is considered a critical area that requires a high degree of accuracy. The challenging part in this field is that the cost of classifying an anomaly as normal might be very high. The hierarchical Federated Learning-based anomaly detection model was proposed to treat the privacy issues associated with the health data sent from IoMT to a centralised server, this proposition uses edge cloudlets to run the model locally without sharing the data to ensure the privacy-preserving, it demonstrates a high rate of accuracy, but there is indigency in the exact numbers of the measured results (Hasan et al., 2019). A graph neural network (GNN) model is used to detect malicious nodes by precisely managing the trust of users implementing, the detection accuracy of this proposed model is not much better than the traditional approaches due to the limited training dataset (Jmaiel et al., 2020). Also, an intrusion detection system (IDS) used for the rank attack against IoT networks based on support vector machines takes the smart hospitals as the use case to respond to multi challenges like sensitive information protection, assets service resilience ...etc. This IDS is evaluated using a simulator to figurate the high detection accuracy and small false-positive rates, even if their propositions prove their performance with all the tested data, we can not be sure if they treat all the data types circulated within a kind of network as an E-healthcare (Newaz et al., 2020). To detect events of interest for patients' health and environment there is a recently proposed anomaly detection system (ADS) that was dedicated to smart hospital IoT-based systems to figure out network intrusion. This approach applies a support vector machine as a single model to determine the ordinary behaviour repose on the baseline to identify anomaly, the result shows that this suggested model ensures low latency and the environment adaptation was more accurate with a high detection for the intrusion and the e-health-related event, but they did not specify exactly the rate results for the e-health-related events and also for the accuracy of detection IoMT network intrusions (Said et al., 2021). All these studies congregate in the missing proof of their performance on all the data types and categories of E-healthcare, we can not be sure that they can examine all the circulated data with its different natures and types inside the new e-healthcare networks of our days.

4.2 Proposed Anomaly detection architecture

Among the provided services of the fog layer highlighted by the previous Figure 1, there is an important zone responsible for data management where the collected data from sensors will be stored temporarily (Pudukotai Dinakarrao et al., 2019). And agreeing with the previous architecture proposed in Figure 2, the fog layer dynamically receives a huge quantity of recorded data from the sensors every single time, it has the main role of controlling the incoming data to give a fast reaction to many users as well as the conditions required in these kinds of the network (Ud Din et al., 2019). As known in healthcare scenarios any latency or uneasiness that takes place might cause incurable damage to the patient's life (Dash et al., 2019). This part of E-health architecture offers all the necessary data resources that respond to detecting anomalies mechanism based on machine learning techniques beginning with the pre-processing and ending with the detection anomalies and it provides the option of taking reactions against them to protect the entire network's functions. Our proposed architecture relies on the benefits of the fog

layer to finance all the layers of detection as follows. Data pre-processing is a step to transform the raw data into an adequate format for machine learning models. It guarantees the quality of the data values before applying ML. For this kind of dataset, we transform all the categorical values into numerical ones and rescale their values by applying methods and predefined functions depending on the predefined medical standard posed by the monitor staff to restore the correlation of the normal collected data. After this phase, the collected data will be classified into two clusters using single model classifications, the medical analytics data which contains all the biomedical analytic data such as biomedical signals, biomedical literature, multi-level analytics ... etc. And the medical images encompass all the medical images as radiology images, MRI scanners…etc. As we mentioned previously, we will use Time series and ImageGray for the analysis of each cluster of the new divided database.

Figure 2 The proposed architecture's model (see online version for colours)



4.3 Algorithm of detection

Our proposed method for anomaly detection in E-health networks treats data separately after the pre-processing phase. Is directed to detect anomalies obtained from IoMT sensors with their different types of data points. The purpose of this proposition is to detect lightly all types of anomalies with the maximum possible accuracy and the lowest false positive rate. While the previous methods mentioned above in the related work section are often provided to detect anomalies for a specific type of data, some of them with a high rate of false positives. This proposed method converts almost of all the main data types circulated in our studied networks. The main steps of our approach are depicted in Figure 2.

4.3.1 Pre-processing

The pre-processing phase is an important step, essentially cleans the data forms of the dataset and removes the unnecessary attributes to reduce the complexity. It converts the data to an appropriate format adequate for the performed analysis, especially for those that are based on machine learning. To fit the ML model the data must be processed and organised to avoid any misunderstandings or unwanted results (Firdausi et al., 2010). Its main usefulness is reducing ambiguity and providing the exact information for the prediction phase. The pre-processing includes usually three sub-phases rescalisation, removing noises, and data correction (Maniriho et al., 2020). Data rescale is putting the numerical values on the same level by applying some methods and predefined functions to restore the correlation of the dataset. Removing noises, or removing unnecessary dimensions which may be added to the data responding to the transfer standards or the null data point. Also, it refers to removing the redundant and irrelevant features for the training phase. At this point, we should deal carefully and strictly to not reformulate the necessary structure of the data. And Data correction is the opposite process of removing, as explained before the nature of E-healthcare data can include some special features that cannot be removed even if they contain a null value, these need some correction depending on their situation inside the dataset. It is to deal with dimension values that cannot be rescaled or removed, by modifying their value adequately depending on their types without affecting the prediction result. As we know ML models can not accept the None values, then the pre-processing stage prevents their existence in such a database.

4.3.2 Classification

The classification phase classifies the databased on their proprieties in two main clusters the medical images and the bio-analytical data and each one of them has an analysis path to follow of course by exploring the benefit of machine learning. Several works use several machine learning models like logistic regression (LR), decision tree (DT), support vector machines (SVMs), random forest (RF), and neural network (NN), the results prove that RF, DT, and NN models performed better than other methods, achieving 99.4% of accuracy which can be as a reference of choosing the adequate ML model (Alhajri et al., 2019; Sen, 2020.). The most convenient model for this phase is the single one-learner. We need to separate the data into two clusters so that all the medical images data will be grouped and follow its analysis path as shown in Figure 2. We highly recommend implementing the support vector machine model thanks to its concept of drawing the

equidistant boundary at space data points to separate them using the hyperplane with the principle of structural risk minimisation. It is operative for high dimensional spaces, in cases where the data dimensions are more than the number of samples plus it is known by its faster speed if its hyperparameters are optimised and evaluated in a manner consistent with the efficiently classified models (Laref, 2018.).

4.3.3 Feature extraction

Feature extraction or feature selection is important to building a model for anomaly detection. As we propose previously, we will count in our method on time-series data analysis to detect the anomalies point for the bio-analytical data. So, we need to restrict the data dimension and select only the necessary features included for anomaly analysis (Hosseini and Borojeni, 2018).

5 Times series detection

Time series represents a record of data that contains the necessary pieces of information for making analytical guesses about what is reasonably expected in the future, which is also one of the data mining steps. Each data point typically must be presented as a pair of two items the time when it was measured, and its associated value. This technique is very effective to examine E-healthcare data breaches, forecasting, and their cost. It is hugely used to analyse biomedical data to predict patients' states (Cook et al., 2020). There is a great example that proposes a method of predicting mortality risk for patients by exploring it for e-health records analysis (Gupta et al., 2020). So many broad ranges of algorithms and approaches are presented to detect anomalies with time-series data (Gupta et al., 2020). To use this technique for anomaly detection there are three main approaches we can apply to our proposed architecture;

5.1 Predictive confidence

Recently ML is hugely being used to automate this analysis for anomaly detection by building a predictive model to estimate the old data and obtain a sense of seasonal, cyclic patterns, or overall common trends. Using the predictive model to forecast future values and based on the error rates which can be calculated using the Mean absolute percentage error equation, we deduce the confidence interval, or band for the predicted values and every data point which isn't beyond this confidence band is an anomaly. Regression and deep learning-based algorithms like long short-term memory (LSTM) are likely used effectively for these kinds of tasks (Gupta et al., 2020). Its main advantage is finding local outliers providing that we apply the efficiency predictive model.

5.2 The statistical profiling

Generating a statistical model or profile for a given data is the fastest approach. It is recommended to generate a controlled and explainable outcome. It works by calculating the statistical values like the mean or median moving average of historical data using standard deviation to extract a band that defines the uppermost and the lowermost bound. Anything falling outside of those ranges is identified as an anomaly.

5.3 Clustering based unsupervised

Is extremely useful to detect an anomaly, it didn't require any labelled input data (Bhatia et al., 2019). The density-based spatial clustering of applications with noise (DBSCAN) is the basic choice, thanks to its simplicity also it is fast and does not require any predefined number of clusters and has only two parameters to tune; the minimum number of points in clusters and the epsilon that represents the distance between clusters. Plus, it helps to map the new normal the thing that most of the other approaches fail. However, we should pay attention to some anomaly data points if it repeats several times in a sparse interval, they cannot be mapped as an anomaly in the next shots.

Whilst some other models combine some elements from multiple approaches to provide a wide solution for the more typical data may also be useful to add to our proposed approach such as: Pattern matching; this method uses direct modelling. In the supervised setting with known characteristics for expected anomalous sub-sequences, the detector will compare each new observation against a database of labelled anomaly events, and flag those which are most similar. In the case where there is the destitution of prior labelled anomalies, the detector learns the most common historic patterns within the normal data and alerts those novel sub-sequences, which do not match the historic corpus as anomalies. The distance-based; is a defined distance metric such that newly received observations can be compared against preceding ones, with the assumption that a lower distance that occurs from similar mechanisms would be reported as normal. Conversely, the larger distance indicates that the observation has been generated differently, so this observation will be flagged as anomalous. Clustering; in this approach, the data will be projected into a multidimensional space and applied to the density of the resulting clusters. Those observations which are close and within dense clusters are indicated as normal observations while the ones which looked further away or do not belong, these clusters are reported as anomalous. Predictive; is a regression model generated based upon the recent and longer-term trends of the system predicting to expect value. When a new observation is received it will be compared against what was predicted, of course, an assessment was made of how accurate the predictions were, if both values observed and the predicted vary greatly then this observation is indicated as anomalous. The ensemble approach; uses many different algorithms to observe each data point and some form of voting mechanism is employed over the outputs from each method. An ensemble can be constructed from a group of similar detectors, such as a range of predictive models, or a collection of dissimilar detectors, such as the combination of probabilistic, clustering, and statistical detectors. Often the use of ensemble techniques can improve the overall success of the detection set at the potential expense of increased setup complexity and computational time.

6 Image recognition detection

Or also grayscale image is a type of detection method using the image conversion strategy. It is an interesting and novel way of conducting malware classification specified to analyse malware images. It is used also for binary data; it reformats it into an 8-bit sequence and then converted it to the gray-scale image that has pixel values from 0 to 255 to can be fed as a final step into machine learning Image classification models. We propose to rely on this method to analyse the medical image data. There is a recently

proposed lightweight solution that enhances this detection technique by contributing a neural network model for detecting malware on IoT networks (Su et al., 2018). In the mentioned work authors suggest a light-weight detection for IoT environments that can be exanimated in our case with the medical images after rescaling them to the convenable measures knowing that this kind of data already has almost the same nature as the transformed data within the proposed work so we can use it with an added benefit of minimising the overloading of the analysis process. With such convention straight-forwards, the detection inside a smart hospital network will require only data re-organisation with no further pre-processing mechanism, for the real images only the corresponding vector that represents the image is needed to fit adequately. In this part, the model extracts malware and classifies their families. Its Experimental shows that the proposed system achieves 94.0% of accuracy for classifying benign data and anomalies, further 81.8% of accuracy for classifying normal data and two main malware families. We can explore this novation as an additional benefit for the fog layer to be the light parallel side of time series detection.

7 Results

The choice of any time series approach is highly dependent on several factors in the monitored data as well as the environment in which the anomaly detector will be deployed. Our proposed architecture does not exact or recommend one of these described approaches, we let the decision of choosing between them as flexible as possible, it will be made depending on the network workflow and the nature of the bioanalytical data that circulate the most inside the hospital network, as we know not all the smart hospitals have the same standards or all can support the resources required of these approaches. The main idea is to choose the adequate technique which is convenient with the data proprieties inside the wanted network without overwhelming the detection process and get the possible minimum false positive rate to put for the proposed detection architecture.

8 Conclusion and perspectives

Our proposed architecture of anomaly detection covers all the previously described data, moreover, it hinges on pre-processing phase to prepare the data and the feature extraction phases to not overload the analysis, both restricting the data features and adjusting the data correlation are likely recommended to enhance the machine learning algorithms' performance and avoid the overfitting. To model this entire anomaly detection architecture and evaluate deeply each mentioned approach of time series plus the combination of image gray classification, we need a reliable dataset that contains all the data stereotypes. The major problem that the IoMT security researchers are always in front of to provide exact and efficient studies is the scarcity of data sources, due to the sensitive pieces of information associated with confident data about patients' identities and status. Considering that any legal or illegal leakage is a breaking of security laws. In our next work, we will try to examine every part of the proposed method separately with some generated data sources, and inspect the likely models which provide the best rate of accuracy, with the lower rate of false-positive results to get the details and the exact

numbers with the real implementation. This comprehensive study is to survey the efficient techniques adequate with the nature of E-healthcare network data to enhance and improve the security insurance inside smart hospitals. To conclude anomaly detection is an interesting area in cybersecurity, especially in our days because the integration of IoT technologies into any IT network produces a large set of captured data, and then there is a necessity to verify, analyse, and endorse each data point to ensure network safety.

References

Ahmed, A. (2018) 'Malicious insiders attack in IoT based multi-cloud e-healthcare environment: a systematic literature review. A systematic literature review', *Multimed Tools Appl*., Vol. 77, pp.21947–21965, https://doi.org/10.1007/s11042-017-5540-x.

Alghanmi, N. (2022) 'Machine learning approaches for anomaly detection in IoT: an overview and future research directions', *Wireless Pers Commun*., Vol. 122, pp.2309–2324, https://doi.org/10.1007/s11277-021-08994-z.

Alhajri, R., Zagrouba, R. and Al-Haidari, F. (2019) 'survey for anomaly detection of iot botnets using machine learning auto-encoders', *International Journal of Applied Engineering Research*, Vol. 14, No. 10, pp.2417–2421, ISSN 0973-4562 © Research India Publications, http://www.ripublication.com.

Al-Issa, Y., Ottom, M.A. and Tamrawi, A. (2019) 'eHealth cloud security challenges: a survey', *Journal of Healthcare Engineering*, Vol. 2019, Article ID 7516035, 15pp, https://doi.org/10.1155/2019/7516035.

Asfaw, B., Bekele, D., Eshete, B., Villafiorita, A. and Weldemariam, K. (2010) 'Host-based anomaly detection for pervasive medical systems', in: Presented at the *2010 5th International Conference on Risk and Security of Internet and Systems (CRISIS)*, IEEE, Montreal, QC, Canada, pp.1–8, https://doi.org/10.1109/CRISIS.2010.5764923.

Azeez, N.A. and der Vyver, C.V. (2019) 'Security and privacy issues in e-health cloud-based system: a comprehensive content analysis', *Egyptian Informatics Journal*, Vol. 20, pp.97–108, https://doi.org/10.1016/j.eij.2018.12.001.

Bhatia, R., Benno, S., Esteban, J., Lakshman, T.V. and Grogan, J. (2019) 'Unsupervised machine learning for network-centric anomaly detection in IoT', in *Proceedings of the 3rd ACM CoNEXT Workshop on Big DAta, Machine Learning and Artificial Intelligence for Data Communication Networks. Presented at the CoNEXT '19: The 15th International Conference on emerging Networking EXperiments and Technologies*, ACM, Orlando FL USA, pp.42–48, https://doi.org/10.1145/3359992.3366641.

Bonetto, R., Bui, N., Lakkundi, V., Olivereau, A., Serbanati, A. and Rossi, M. (2012) 'Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples', in *2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM). Presented at the 2012 IEEE Thirteenth International Symposium on 'A World of Wireless, Mobile and Multimedia Networks' (WoWMoM),* IEEE, San Francisco, CA, USA, pp.1–7, https://doi.org/10.1109/WoWMoM.2012.6263790.

Canedo, J. and Skjellum, A. (2016) 'Using machine learning to secure IoT systems', *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, Auckland, New Zealand, pp.219–222, doi: 10.1109/PST.2016.7906930.

Chandola, V. (2009) 'Anomaly detection: a survey', *ACM Computing Surveys*, Vol. 41, No. 3, Article No. 15, pp.1–58, https://doi.org/10.1145/1541880.1541882.

Cook, A.A., Misirli, G. and Fan, Z. (2020) 'Anomaly detection for IoT time-series data: a Survey. IEEE internet things J', Vol. 7, pp.6481–6494, https://doi.org/10.1109/JIOT.2019.2958185.

Costin, A., Zaddach, J. and Antipolis, S. (2018) 'IoT malware: comprehensive survey, analysis framework and case studies', *BlackHat USA*, Vol. 1, No. 1, pp.1–9.

Dash, S., Biswas, S. and Banerjee, D. (2019) 'Edge and fog computing in healthcare – a review', *Scalable Computing: Practice and Experience*, Vol. 20, No. 2, pp.191–206.

Diro, A., Chilamkurti, N., Nguyen, V-D. and Heyne, W. (2021) 'A comprehensive study of anomaly detection schemes in IoT networks using machine learning algorithms', *Sensors*, Vol. 21, p.8320, https://doi.org/10.3390/s21248320.

Firdausi, I., Lim, C., Erwin, A. and Nugroho, A.S. (2010) 'Analysis of machine learning techniques used in behavior-based malware detection', *2010 Second International Conference on Advances in Computing, Control, and Telecommunication Technologies*, pp.201–203, IEEE.

Gupta, A., Liu, T. and Crick, C. (2020) 'Utilizing time series data embedded in electronic health records to develop continuous mortality risk prediction models using hidden Markov models: a sepsis case study', *Statistical Methods in Medical Research*, Vol. 29, No. 11, pp.3409–3423, doi:10.1177/0962280220929045.

Hady, A.A., Ghubaish, A., Salman, T., Unal, D. and Jain, R. (2020) 'Intrusion detection system for healthcare systems using medical and network data: a comparison study', *IEEE Access*, Vol. 8, pp.106576–106584, https://doi.org/10.1109/ACCESS.2020.3000421.

Haji, S.H. and Ameen, S.Y. (2021) 'Attack and anomaly detection in IoT networks using machine learning techniques: a review', *Asian Journal of Research in Computer Science*, DOI:10.9734/AJRCOS/2021/V9I230218.

Hameed, R.T., Mohamad, O.A., Hamid, O.T. and Tapus, N. (2015) 'Design of e-healthcare management system based on cloud and service oriented architecture', *E-Health and Bioengineering Conference (EHB)*, Iasi, Romania, pp.1–4, doi: 10.1109/EHB.2015.7391393.

Hasan, M., Islam, Md.M., Zarif, M.I.I. and Hashem, M.M.A. (2019) 'Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches', *Internet of Things*, Vol. 7, p.100059, https://doi.org/10.1016/j.iot.2019.100059.

Hosseini, M. and Borojeni, H.R.S. (2018) 'A hybrid approach for anomaly detection in the internet of things', in: *Proceedings of the International Conference on Smart Cities and Internet of Things - SCIOT '18. Presented at the International Conference*, ACM Press, Mashhad, Iran, pp.1–6, https://doi.org/10.1145/3269961.3269975.

Jmaiel, M., Mokhtari, M., Abdulrazak, B., Aloulou, H. and Kallel, S. (Eds.) (2020) 'The impact of digital technologies on public health in developed and developing countries', *18th International Conference, ICOST 2020*, Hammamet, Tunisia, Proceedings, Lecture Notes in Computer Science. Springer International Publishing, Cham, June 24–26, https://doi.org/10.1007/978-3-030-51517-1

Laref, R. (2018) *On the Optimization of the Support Vector Machine Regression Hyperparameters Setting For Gas Sensors Array Applications*, Vol. 184, pp.22–27, ISSN 0169-7439, https://doi.org/10.1016/j.chemolab.2018.11.011.

Maniriho, P., Niyigaba, E., Bizimana, Z., Twiringiyimana, V., Mahoro, L.J. and Ahmad, T. (2020) 'Anomaly-based intrusion detection approach for IoT networks using machine learning', in *2020 International Conference on Computer Engineering, Network, and Intelligent Multimedia (CENIM). Presented at the 2020 International Conference on Computer Engineering, Network, and Intelligent Multimedia (CENIM)*, IEEE, Surabaya, Indonesia, pp.303–308, https://doi.org/10.1109/CENIM51130.2020.9297958.

Monteiro, K., Rocha, E., Silva, E., Santos, G.L., Santos, W. and Endo, P.T. (2018) 'Developing an e-health system based on IoT, fog and cloud computing', in *2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion). Presented at the 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion)*, IEEE, Zurich, pp.17–18, https://doi.org/10.1109/UCC-Companion.2018.00024.

Newaz, A.I., Sikder, A.K., Babun, L. and Uluagac, A.S. (2020) 'HEKA: a novel intrusion detection system for attacks to personal medical devices', in *2020 IEEE Conference on Communications and Network Security (CNS). Presented at the 2020 IEEE Conference on Communications and Network Security (CNS)*, IEEE, Avignon, France, pp.1–9, https://doi.org/10.1109/CNS48642.2020.9162311.

Pramanik, P.K.D., Nayyar, A. and Pareek, G. (2019) 'WBAN: driving e-healthcare beyond telemedicine to remote health monitoring', in: *Telemedicine Technologies*, Elsevier, pp.89–119. https://doi.org/10.1016/B978-0-12-816948-3.00007-6.

Pudukotai Dinakarrao, S.M., Sayadi, H., Makrani, H.M., Nowzari, C., Rafatirad, S. and Homayoun, H. (2019) 'Lightweight node-level malware detection and network-level malware confinement in IoT networks', in *2019 Design, Automation and Test in Europe Conference & Exhibition (DATE). Presented at the 2019 Design, Automation and Test in Europe Conference and Exhibition (DATE)*, IEEE, Florence, Italy, pp.776–781, https://doi.org/10.23919/DATE.2019.8715057.

Rahmani, A.M., Gia, T.N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M. and Liljeberg, P. (2018) 'Exploiting smart e-Health gateways at the edge of healthcare internet-of-things: a fog computing approach', *Future Generation Computer Systems*, Vol. 78, Part 2, pp.641–658, ISSN0167-739X, https://doi.org/10.1016/j.future.2017.02.

Rodrigues, J.J.P.C., Sendra Compte, S. and de la Torra Diez, I. (2016) *Electronic Medical Records and Their Standards, in: E-Health Systems*, Elsevier, pp.3–19. https://doi.org/10.1016/B978-1-78548-091-1.50001-4

Said, A.M., Yahyaoui, A. and Abdellatif, T. (2021) 'Efficient anomaly detection for smart hospital IoT systems', *Sensors*, Vol. 21, No. 4, p.1026, https://doi.org/10.3390/s21041026.

Seh, A.H., Zarour, M., Alenezi, M., Sarkar, A.K., Agrawal, A., Kumar, R. and Khan, R.A. (2020) 'Healthcare data breaches: insights and implications', *Healthcare*, Vol. 8, No. 2, p.133, MDPI, doi: 10.3390/healthcare8020133.

Sen, P.C. (2020) 'Supervised classification algorithms in machine learning: a survey and review', in Mandal, J. and Bhattacharya, D. (Eds.): *Emerging Technology in Modelling and Graphics. Advances in Intelligent Systems and Computing*, Vol. 937, Springer, Singapore, https://doi.org/10.1007/978-981-13-7403-6_11.

Su, J., Danilo Vasconcellos, V., Prasad, S., Daniele, S., Feng, Y. and Sakurai, K. (2018) 'Lightweight classification of IoT malware based on image recognition', in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). Presented at the 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, IEEE, Tokyo, Japan, pp.664–669, https://doi.org/10.1109/COMPSAC.2018.10315.

Talaminos-Barroso, A. (2016) 'A machine-to-machine protocol benchmark for eHealth applications – use case: respiratory rehabilitation', *Computer Method Sand Programs in Biomedicine*, Vol. 129, pp.1–11, ISSN 0169-2607, https://doi.org/10.1016/j.cmpb.2016.03.004.

Ud Din, I., Guizani, M., Hassan, S., Kim, B-S., Khurram Khan, M., Atiquzzaman, M. and Ahmed, S.H. (2019) 'The internet of things: a review of enabled technologies and future challenges', *IEEE Access*, Vol. 7, pp.7606–7640, https://doi.org/10.1109/ACCESS.2018.2886601.

Ukil, A., Bandyoapdhyay, S., Puri, C. and Pal, A. (2016) 'IoT healthcare analytics: the importance of anomaly detection', *IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, Crans-Montana, Switzerland, pp.994–997, doi: 10.1109/AINA.2016.158.