A Novel Methodology for Providing Security in Electronic Health Record Using Fuzzy Based Multi Agent System

https://doi.org/10.3991/ijoe.v17i11.25347

Mohammed Ateeq Alanezi
University of Hafr Al Batin, Hafr Al Batin, Saudi Arabia
alanezi.mohd@uhb.edu.sa

Abstract—Privacy and security are crucial when it comes to the implementation of Electronic Healthcare Records (HER). Whenever a patient visits a doctor, their health records are updated since it consists of vital information on the patient's health and well-being. It also comprises of description about the previous and current treatment quality. Multi-Agent Systems can support E-Healthcare applications for improving quality of life. The availability and use of extensive systems for EHR has increased dramatically. The EHR technology currently available consists of health information of various patients which helps those people to monitor their health. These information should be protected from being altered or mishandled. Various studies have been conducted in the past literature to improve the protection and privacy requirements in E-health services. Despite this, it hasn't been entirely improved. This article proposes a Fuzzy based multi-agent system architecture that uses agents and fuzzy logic to monitor the flow and access of the EHR record using fuzzy logic and multi agents. Architecture comprises of multi agent and fuzzy systems are proposed. In this system, we have employed Action/ Computation (Interface) agent, communication interface agent and verification agent and Communication Module Agent. These agents collaboratively worked one another in order to obtain the desired output. These agent based e-health system can increase the accuracy of data transfer by providing additional security in selecting the user who handles the data. It also monitors the communication between different medical units in the health system.

Keywords—information security, electronic health records, agents, fuzzy logic, security model, health information

1 Introduction

Digital Transformation has created and compiled a variety of electronic health information from different sources, including medical science labs, clinics, and health-care companies. As a result, a new term known as electronic health was created. This could be described as the use of IT-based technology and e-commerce activities to facilitate the distribution and analysis of health data. The EHR is the name given to this

data. Sensor-based clinical systems can be operated by a variety of controls, allowing for continuous recording of the patient during the diagnostic establishment. As a result, consumers such as medical personnel can view such stored medical information, which contain the majority of private and sensitive health information. Various methodologies for protecting the privacy and protection of the EHR [1, 2] have been suggested previously. However, in order to transmit health data, these approaches need more protection. E-healthcare services are authentic and provide patient data in clinical format. Licensed individuals keep these up to date. These data sets were generated by combining information from a variety of patients. The approved individuals in these EHRs may be patients or physicians. The information stored on the databases can be personal or cloud-based, and it can be used to store and analyze health information [3]. The elements used in systems can act as an interlink between staff and hospital personnel, allowing for better data transmission and transmission [4]. However these technologies offer many advantages, they also have more drawbacks in terms of data protection and privacy. Because of their nature, these security issues exist [18].

These risks can be divided into several categories, including data collection, delivery, and storage, which are discussed in greater detail in section 3. Some users are hesitant to use these applications because of the risks to the security and privacy of EHR data. As a result, it is critical to ensure that users are ready to apply the system. As a result, it's critical to propose a framework for ensuring the privacy and protection of EHR data. A comprehensive survey is conducted in this paper to analyse the protection and privacy risks that exist in the healthcare system. Then, a novel agent-based framework for ensuring EHR data protection and privacy is suggested. The agent-based framework comprises a set of smart objects with unique and efficient working functions, such as the control system agent, authorization agent, link organization agent, and regulatory management agent. These expert systems make access among healthcare professionals and E-service providers as simple and efficient. The agent-based framework performed tasks such as application design, sign up, access controls, link creation, and interface maintenance. The following is the rest of the document. Section II discusses the different forms of attacks and the strategies for avoiding them that were originally suggested by previous researchers along with the motivation of the proposed work. Section 3 proposes the agent based systems along with the intelligent agents and the suggested agent-based approach for ensuring privacy and protection in E-healthcare systems. Section 4 depicts the conclusions and future enhancements of the proposed system.

2 Literature review

An E-healthcare technology incorporates modern technology, intelligent wearable devices, and sensors based on multi-agent in Smart cities' order to support intelligent applications of e-healthcare that can help to create an intelligent healthcare city. Residents, healthcare professionals, medicinal businesses, health professionals, academics, and metropolitan administrators are all collaborating into a unified Internet of Things (IoT) framework to provide better healthcare services to the underprivileged.

By (i) providing emergency assistance with a rapid onset of action in the healthcare field, (ii) provide treatment via online, (iii) engage with the city's hospitals and clinics and (iv) preserve effort, resources, and lifestyles of people in the long run.

Various techniques for ensuring the safety and confidentiality of electronic health records (EHR) have proposed previously [5-7]. However, in order to transfer data sets related to health, these systems require enhanced security. E-healthcare frameworks operate in real time and save the patient data in electronic medium. Authorized individuals keep these in good working order. These sets of data were created by combining information from a variety of patients. The allowed individuals in such EHRs can be patients as clients or the physicians. The data on the systems can be accessed locally or via the cloud, that archives and analyzes the health care information. The features included in networking can act as an interface among patients and doctors, allowing for better data transmission and distribution. Nevertheless, there are numerous advantages to such systems: there are serious issues to the safety and confidentiality of the users stored on them. Such potential risks are built into the architecture of the system. These risks can be divided into several subcategories, including level of data gathering [8–10], level of transmission level [11–14], and level of storage [15,16], all of which are discussed in greater detail in Section 3. Some consumers are hesitant to use such technologies because of the concerns to the confidentiality and protection of EHR data. As a result, it is critical to ensure that consumers are prepared to apply the system without any reluctance. As a result, it's critical to provide a mechanism for protecting the reliability of EHR data.

The authors of [3] presented a multi-agent based intelligent method for controlling the health status of older peoples. In recent decades, multi-agent networks have been a prominent issue [2, 10]. It is being designed and analysed since it has a significant impact on society. In order to be effective, continuous supervision should have spontaneous interconnections between diverse clinical units. The suggested system, which employs a multi-agent structure, comprised of a network of agents who share knowledge and data together to fulfil the goal of geriatric and patient supervision. Agents in the created system will be provided with an artificial policy maker which provide the users with rule-based capabilities in order to help them make early conclusions about patients' and older people's health conditions.

Confidentiality support is a key feature of E-health systems [11], since it preserves the security and integrity of patients' personal data from unwanted access. An intruder must examine the communications transferred between smartphone physicians while they are exchanging their personal medical records (PHI) or collaborating to forward PHI these records in order to gain the patient's private identification and information about the location. As a result, non-shared symptom features must be safeguarded from unauthorized access because they can reveal the patient's personal health information. Moreover, the opponent must be kept in the dark about the identification of the origin and intermediary users who make and share the patients' health records. The opponent must also be safeguarded from the authenticated information about the location, since such data might be used to deduce the patient's traveling routines or lifestyle habits, which can subsequently be utilized for odds or even physical assault [12].

Authors in [20] suggested a Scalable and Privacy-Preserving Opportunistic Computation (SPOC) paradigm for m-Healthcare emergencies. By the use of preemptive computational architectures, the suggested methodology guarantees that confidentiality is preserved in the event of an m-Healthcare emergency. A standard patient information data is sent to a patient's regional healthcare facility every 5 minutes for routine remote access and monitoring. A specified method that must be performed in order to manage an urgent situation is split into many independent units using opportunistic information technology, such that no single element of the initial process exhausts the low computational facilities allocated to a resources restricted computing node like a motion sensor. Attacks on the cloud platform that are based on system access can be dangerous. It has the ability to alter health care information as well as the general design of a system or systems used for surveillance. These assaults can come in the form of interfering with a patient data, obtaining a patient's health information against their permission, and so on. It could be performed at the personal health data at customer's premises. Several concerns relating to the operating systems used to keep a people's clinical data can result in medical system interference. It's also likely that numerous forms of dangers, like malware, Trojan, and adware, can readily get access to public health system. The researchers of [2] presented a better access control mechanism and its application. The primary objective of this strategy is to make accessing private data relatively protected. It is made up of six key elements such as subject characteristics, object characteristics, entitlements, approvals, duties, and circumstances. Approvals, responsibilities, and restrictions are elements of usage policy narratives in such characteristics, which are then used to evaluate if a user is permitted to process the information or not. The availability of other characteristics opens the door to addressing some of the flaws that have plagued access restrictions in the past. The biggest limitation of this approach is that it serves as an initial stage in the authorization process.

2.1 Motivation of the proposed works

The following are some of the difficulties that traditional learning strategies face:

- Several strategies for improving the EHR have been suggested previously. The amount of EHR systems is already in the works, but they are inaccurate.
- Artificial Intelligence (AI) automated system approaches were used to improve the EHR model's accuracy. While it was infinitely performing, the accuracy of the model was limited.
- Subsequently on, fuzzy systems-based approaches for medical information were suggested. The mistakes were assessed. The approach was more effective and stable, but the reliability was low.

The following framework is developed in order to address the shortcomings of existing technology.

3 Agent based systems

An agent is a self-contained, versatile computer system which can take input and output from its surroundings. The agents have a slew of other benefits. Agents, is shown in Figure 1 for instance, can be taught to perform unique tasks, communicate with one another, and be extended, all of which are extremely useful when designing stable systems. An agent will act in the place of a consumer and complete work on their behalf. Furthermore, agent structures are naturally extensible. While modifying the overall structure, a new agent may be generated and attached to the current architecture to reflect an user account, including a network management agent.

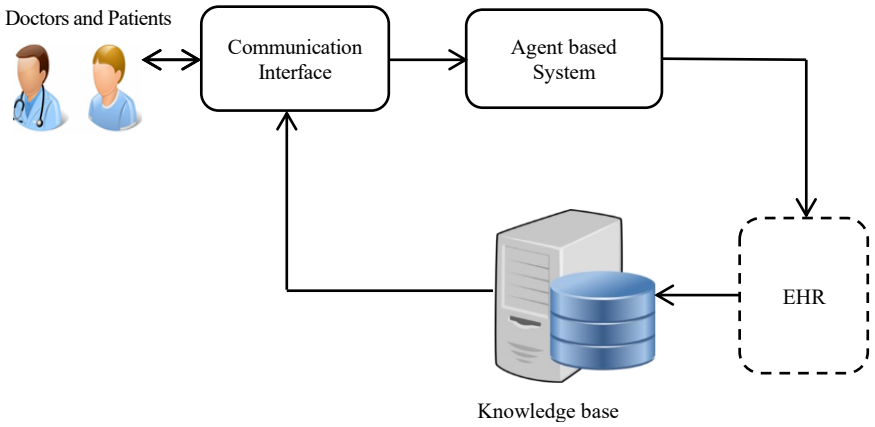

Fig. 1. Architecture if an intelligent agent

3.1 Proposed model

This section proposes a Multi-Agent Architecture for offering efficient and reliable E Health security services. Figure 2 depicts the architecture of the Intelligent-based Authentication management that uses agent-based technologies to improve the effectiveness of healthcare systems. The multi-agent system suggested in this paper is made up of a number of expert systems, each with its own set of functions and capabilities, such as the user interaction agent, verification agent, connection setup agent, and connection management agent. These expert systems make the conversation between healthcare professionals, patients and E-service organizations simple and successful. The multi-agent based system performed several functions such as constructing the interface, registering the user, authenticating the user, initiating the connection, and preserving the connection. It also makes use of a database to save and access medical data in the form of an EHR.

Domain/ Information phase, Action/ Computational agent, Customer phase, Operative phase, and Communication phase are the four primary phases of the proposed approach. All users who interact with this system are included in the customer phase. Physicians, consumers, and authorized professionals can only use the system to handle

medical records for further analysis. The agent phase is made up of multiple agents that are in charge of protecting the reliability of medical information access. The user interface agent established the policy and procedures. A healthcare database is used to keep all of the login credentials that patients, doctors, and other authorized individuals submit and utilize to retrieve and analyze data. The user is validated using an user identification agent. It is also utilized to verify the healthcare database's login credentials. The authorized connection is established using a data transmission agent and a connection management agent.

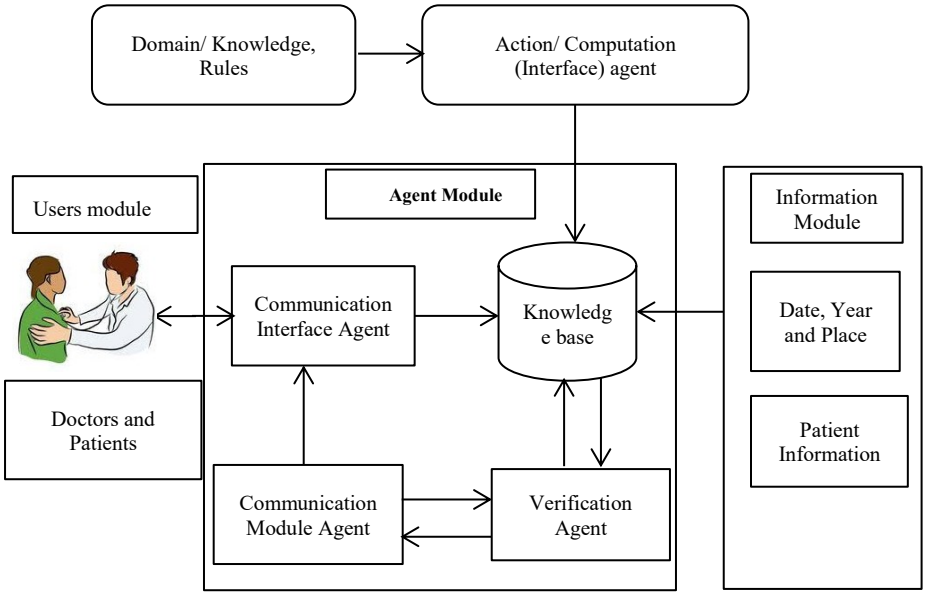

Fig. 2. Architecture of the Proposed Model

3.2 Working principle

Through the user interface agent, the suggested System acknowledges the user's request. Users' usernames and passwords are accepted. A website or a smartphone application connects the User interface agent. The validation agent verifies the user's account and credentials the connection establishment agent establishes an interface between the client and the server when the user has been authenticated. This lays the groundwork for efficient and secure access of EHR data. The details about the formed connection will be saved in the database as well, so it can be referred to in the future. The authentication agent allows users authorization to view the identities of the individual who sought the information after the connection is established.

The fundamental and all relevant facts and data about the individual are contained in the information phase of the health database. It includes information on the client's circumstances, such as his or her geo-location, the timestamp the data was obtained. Database includes details such as the patient's age, condition, blood type, height,

weight, and BGM. The present health information field contained recent health information such as pulse rate, hypertension, blood sugar, and surgery background, among other things. The health database also stores all of the login credentials issued and used by users, doctors, and other authorized individuals for retrieving and processing data. The following is a quick summary of numerous agents and their functions:

Fuzzification. Fixing the values of one set of crisp value to a different fuzzy set of qualitative illustration is termed as Fuzzification. In several Fuzzy strategies such as Fuzzy based process, Fuzzy C-means and Fuzzy based reasoning, intensity transformation of values towards various numerals are processed within the initial stage. In this proposed work, the Fuzzification method is similar the searching of user weather he/she is a valid user or not.

Fuzzy rules for user authentication. User authentication is a process that allows a device to verify the identity of someone who connects to a network resource. There were five Common types of user authentication:

- Password-based authentication.
- Multi-factor authentication.
- Certificate-based authentication.
- Biometric authentication.
- Token-based authentication

In this method, the token based authentication mechanism is employed using the fuzzy logic [17]. The tokens were generated by the user module which is responsible for identifying the valid user. The fuzzy rule shown below checks for the valid user Q from the user set QE. If the token T is equal to the user in Q, the user is a valid one. IF it is not equal to the user in Q, then the user is not a valid one.

Fuzzy rules for user authentication:

```
Rule-1: for every user Q in the user set UE
if( T ∈ Q )
then,
Valid User;
else
Invalid User;
End if,
End for
```

Action/ Computation (Interface) agent. The motivating concept behind the action/ computation agents is to allow the user to access the computation agent assistant. These agents follow this direction, scheduling and rescheduling user interaction, user authentication, validating the user and restricting the invalidated user. Main goal is to reduce the workload of users by creating personalized agents to which interface can be delegated.

Algorithm. Because there are so many actors in health systems, accessibility protocols are hard. The health-care system will be able to accommodate a large number

of users, responsibilities, documents, and privileges to explore the information of the health database. The technique for authenticating, maintaining the communication among users and the system, and granting authorized users access to files is provided in this section.

— Connection-establishing algorithm:

For every user Q in the user set UE

```
if (UN ∈ Q) and
User = <Valid User>
then,
Establish connection;
else
No connection;
End if,
End for
```

— Algorithm for accessing the files:

For every UE in Q, Compute the authentication policy

```
if (AP = FALSE)
Break;
end if;
if (AP = TRUE), then;
if FA = <Q, M, FI, FS>
then,
Access the files along with all the fields;
end if;
end if
end for
```

3.3 Research findings

— The proposed architecture, which is based on an agent-based system, can provide E-Health security services that are both efficient and reliable.
— The user, who is a critical component of the E-health system, is in charge of this structure.
— The connection establishment agent is responsible for connection establishment between the users and the agents.
— The 2 categories of expert systems, such as the user interaction agent and the authorization agent, make it easy to use and communicate with E-service operators.
— The control system agent is linked to a portal or a mobile-based device to make it easier for users to employ.

4 Conclusion and future works

The EHR enables communications between patients, doctors and the medical service providers thus enabling communications of health information anytime and anywhere. These information about patients must be kept safe on databases such that health professionals and physicians can view and use it during diagnosis. This paper proposes a combination of fuzzy logic and agent-based system to ensure that these data is secure Attacks on these health data have the potential to change details, adjust total data, and add unauthorized access as users. Using the proposed methodology, the proposed architecture aims to prevent these types of attacks. The proposed model is made up of the combination of fuzzy logic and agents. Based on the agents' features, this approach is a simple and effective security method of control.

5 References

[1] M. Barua, (2011). PEACE:An efficient and secure patient-centric access control scheme for e-Health care system in Computer Communications, IEEE INFOCOM Conference,. https://doi.org/10.1109/infcomw.2011.5928953

[2] D. Sharma and F. Shadabi, (2014). The potential use of multi-agent and hybrid data mining approaches in social informatics for improving e-health services, Proceedings of Fourth IEEE International Conference on Big Data and Cloud Computing, 350-354. https://doi.org/10.1109/bdcloud.2014.25

[3] Ayman M. Mansour, (2018). Intelligent e-Health System for Patient and Elderly People Monitoring Using Multi Agents System, Jordan Journal of Electrical Engineering, 4:1.

[4] S.S. Shinde, And D. Patil, (2015) Review on Security and Privacy for Mobile Healthcare Networks: From A Quality of Protection Perspective, International Journal of Engineering Research, 3, 203-213.

[5] K. Habib, A. Torjusen, and W. Leister, (2015). Security analysis of a patient monitoring system for the Internet of Things in e-Health", in Proceedings of the International Conference on e-Health, Telemedicine, and Social Medicine (eTELEMED'15).

[6] Fernández-Alemán, J.L.; Señor, I.C.; Lozoya, P.; Ángel, O.; Toval, (2013). A. Security and Privacy in Electronic Health Records: A Systematic Literature Review", J. Biomed. Informatics, 46, 541–562, https://doi.org/10.1016/j.jbi.2012.12.003

[7] Abd-Elhafiez,W.M.; Reyad, O.; Mofaddel, (2019). M.A.; Fathy, M. Image Encryption Algorithm Methodology Based on Multi-Mapping Image Pixel. In Advances in Intelligent Systems and Computing; Springer Science and Business Media LLC: Berlin/Heidelberg, Germany, 645–655. https://doi.org/10.1007/978-3-030-14118-9_64

[8] Khan, F, (2019). Automated Segmentation of Lung Parenchyma Using Colour Based Fuzzy C-Means Clustering", J. Electr. Eng. Technol, vol. 14, pp. 2163–2169. https://doi.org/10.1007/s42835-019-00224-8

[9] Manirabona, A.; Fourati, L.C.; (2017). Boudjit, S. Investigation on Healthcare Monitoring Systems. Int. J. E-Health Med. Commun, 8: 1–18.

[10] Han, S.; Zhao, S.; Li, Q.; Ju, C.H.; Zhou, W, (2015). PPM-HDA: Privacy-Preserving and Multifunctional Health Data Aggregation with Fault Tolerance". IEEE Trans. Inf. Forensics Secur, 11: 1940–1955, https://doi.org/10.1109/tifs.2015.2472369

[11] Tang, J.; Liu, A.; Zhao, M.; Wang, T, (2018), An Aggregate Signature Based Trust Routing for Data Gathering in Sensor Networks. Secur. Commun. Netw, 1–30, https://doi.org/10.1155/2018/6328504

[12] *Evelyn Santana Mantuano, Washington Xavier Garcia-Quilachamin, Jorge Anchundia Santana,* A Systematic Review of Algorithms in People Images Detection Based on Artificial Vision Techniques for Energy Management in Air Conditioners, International journal of online and Biomedical Engineering, Vol 17, No 01, 2021. https://doi.org/10.3991/ijoe.v17i01.17899

[13] *Xianfeng Yang, Xiaojian Jia,* Multi-frame Image Processing Based on Wireless Sensor Networks, International journal of online and Biomedical Engineering, Vol 14, No 10, 2018.

[14] Bonab, T.H.; Masdari, M, (2015). Security attacks in wireless body area networks: Challenges and issues, Acad. R. Sci. Outre-Mer Bull. Seances, 4:100–107

[15] Azeez, N.A.; Oluwatosin, A, (2016). CyberProtector: Identifying Compromised URLs in Electronic Mails with Bayesian Classification. In Proceedings of the International Conference Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 15–17. https://doi.org/10.1109/csci.2016.0184

[16] *Abdul Khader Jilani Saudagar,* Biomedical Image Compression Techniques for Clinical Image Processing, International journal of online and Biomedical Engineering, Vol 16, No 12, 2020. https://doi.org/10.3991/ijoe.v16i12.17019

[17] Faizal Khan, Z & A. Kannan, (2014). Intelligent Approach for Segmenting CT Lung Images Using Fuzzy Logic with Bitplane, Journal of Electrical Engineering and Technology, 9: 742-752, https://doi.org/10.5370/jeet.2014.9.4.1426

[18] Zhi-guo Wang, Wei Wang, Baolin Su, Multi-sensor Image Fusion Algorithm Based on Multiresolution Analysis, International journal of online and Biomedical Engineering, Vol 14, No 06, 2018. https://doi.org/10.3991/ijoe.v14i06.8697

6 Author

Dr. Mohammed Alanezi is an Associate Professor in the Department of Computer Science and Engineering, University of Hafr Al-Batin. His research interests include E-Government, E-Services, E-Health, IOT and Knowledge Management. He has had contributions in developing systems and projects. Much of his work has been in embracing digital transformation and improving the current technology to solve challenges facing the University of Hafr Al-Batin.

Article submitted 2021-07-08. Resubmitted 2021-08-04. Final acceptance 2021-08-05. Final version published as submitted by the author.