Internet Of Things (IoT) in Healthcare System

Nadia Ayari [1] , Farah BARIKA KTATA[2], Souhir Gabsi[3], Belgacem Hamdi[3]

nadia.alayari@nbu.edu.sa ayarinadia13@yahoo.fr

[1]Faculty of Sciences and Arts, Turaif, Northern Border University, Arar 91431, Kingdom of Saudi Arabia

[2]Multimedia, InfoRmation Systems and Advanced Computing Laboratory, University of Sousse, Tunisia
[3]Electronic and Micro-electronic Laboratory, University of Monastir, Tunisia

Summary

In recent decades, Healthcare faces different challenges due to the increasing cost of care, population growth and lack of caregivers. This situation was more serious and critical, last recent years when the world has witnessed a major spread of the new corona virus (COVID-19), which has arisen, among others, many issues related to exchanges and Medical Data Management. A healthcare system consist mainly on collaboration between hospital wards, elaborations of medical diagnostics, coordination among medical entities and the collection of information about and from patients directly or via a set of connected devises and sensors. For that, cooperation in the Agent Technology can provide better healthcare than the established medical system. In fact, Intelligent Agents properties (sociability, proactivity, autonomy) and the features of Multi Agent Systems (management of distributed information, communication and cooperation between different entities) are a good option to solve several problems in the hospital organization. On the other hand, information and communication technologies (ICT) are widely used in e-health to deliver services. In medical centers such hospitals and other laboratories where more health data sets were formed during the treatment process. In order to enhance the standard of the services provided in healthcare, these records where shared and can be used by various users depends on their requirements. As a result, notable issues in the security and privacy where obtained which should be monitored and removed in order to make the use of Electronic Health Record (EHR) more effectively. Various researches have been done in the past literature for improving the standards of the security and privacy in E-health systems. The threats put the patient's privacy at risk. Therefore, it is important to make sure that security technologies can cater for the privacy and security needs, whenever communications occur through the Internet. This paper presents a security framework that allows the enhancement of the security level for e-health services. In this paper, we propose a new security framework based on a security model. This model is described using MA-UML notations. It defines permissions for users to treat individual and collaborative attacks. The proposed security framework uses the security model allowing administrator to define a strict and fine-grained authorization policies. Authorization enforcement on the proposed framework is also; dynamic that is the authorization decisions are based upon runtime parameters.

Keywords:
E-health, Framework, Multi-agent, IoT, security, MA-UML.

1. Introduction

An electronic health record (EHR) is a digital version of a patient's manuscript chart. EHRs are real-time, patient-centered records that make information available instantly and securely to authorized users. While an EHR does contain the medical and treatment histories of patients, an EHR system is built to go beyond standard clinical data collected in a provider's office and can be inclusive of a broader view of a patient's care

One of the key features of an EHR is that health information can be created and managed by authorized providers in a digital format capable of being shared with other providers across more than one health care organization such as laboratories, specialists, medical imaging facilities, pharmacies, emergency facilities, and school and workplace clinics.

The effect of Internet of Thing (IoT) has induced and combined numerous electronic health information from various places such as laboratories of medical research, hospitals and health care firms [1,2].

This led to the formation of a novel concept called Electronic health (E-health). This can be defined as the application of IT based technologies and the practices of E-commerce for the entire sharing and processing, of the health information. As a result, users such as medical personnel can access these acquired health records, which contain the majority of secret and sensitive health information. Various techniques for ensuring the privacy and security of EHRs have been offered previously. [3,4]. However, in order to distribute health data, these systems require extra security. E-healthcare systems are real-time and have digitally stored patient information.

Manuscript received May 5, 2022
Manuscript revised May 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.5.104

The data saved on the servers might be local or cloud-based, and it can store and analyze health data [5].The components included in networks can act as an interconnector between patients and medical personnel, boosting data transmission and distribution [6].

Though these systems offer numerous advantages, they also have additional drawbacks in terms of data security and privacy. These security risks are due to its design [17]. These dangers can be categorized into several groups.

Due to these threats in security and privacy of the EHR data. As a result, mobile agent technology offers various benefits for software development, including less network traffic, lower communication costs, and detached operations, all of which can result in a safe and private E-health system. Many studies have been conducted to address mobile agent's systems security issues by focusing on the theoretical aspect of the problem and essentially on individual attacks. Security mechanisms provided by the mobile agent platforms and by the literature present a lack of establishment of security aspects and of the mobility-related permissions [19] [15]. Also, they do not address all the security criteria, and they are not satisfactory to construct a system that defends against all possible attacks [4]. Hence, it becomes necessary to narrow the gap between theory and practice, and to improve the security mechanisms in mobile agent platforms to fully exploit the benefits of mobile agent technology. One of the principal issues that make the security question more sensitive on mobile agents systems than on the conventional systems is the fact that mobile agents move to the target platform and more precisely to the target place then it uses directly the resources (CPU, files). So, mobile agents can affect the place availability. That is why it is necessary to define the permissions and to control the actions that are running on a place. On the other hand, a successful mission of a mobile agent depends on how much the visited places contribute to achieving the goal of the mobile agent by providing a secure execution. The characteristics of systems of mobile agents require supplementary concepts (in addition to the one defined in conventional systems) to be considered when defining a security solution. Systems of mobile agents require a flexible security frame- work to permit the dynamic control of both places and agent behavior depending on application-specific requirements and peculiarities. Also, the security framework of a place should not be considered as an add-on feature but should be integrated into the place since the very first phases of the design [18]. The security framework must include agents' police as a component of the place. This police force should observe the activities on the place and intervene if an attack is detected [9]. The impact of an attack is aggravated when it involves many attackers; it is to say when it is about a collaborative attack. In general collaborative attacks have reportedly caused the most serious losses in recent years. Most of the modern sophisticated attacks are con- ducted collaboratively [12]. Collaborative attacks are characterized by the prevalence of coordination between the attacker entities. The collaboration in the mobile agent system can be between attacker users from the same platform or many platforms. The treatment of this type of attack is still an open question. Our goal in this paper is to propose a security framework that can protect the place and the mobile agents from various security threats, including attacks against authentication, integrity, access control, authenticity, confidentiality, availability, and non-repudiation. The proposed framework is a policy-based approach. The new security model is based on new extensions, which we add on this paper; and on some extensions, that were defined in [20].

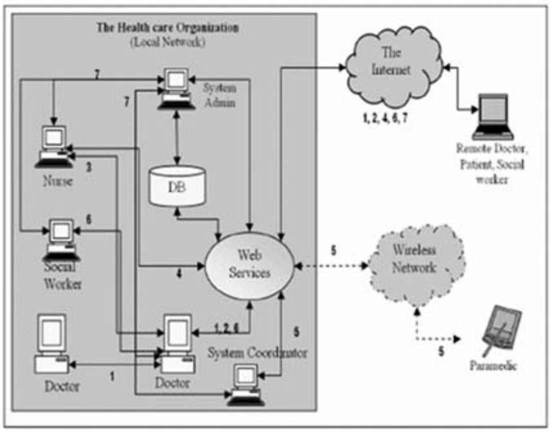
For this purpose, our work is organized as follows:
In section 2, we provide a background of e health services. A security in mobile agents systems that achieve a secure and private healthcare system was presented in section 3. Then in section 4, we propose the architecture of our security framework based method for providing the privacy and security in the E healthcare systems. Section5, presents the framework implementation and the obtained results in front of the executed in- dividable and collaborative attacks. Finally, section 6 concludes the paper and offers directions for future work.

2. E-Health Services

In the medical field, patients are integrating smart devices that offer health services the possibility to diagnose and determine if they are prone to certain pathologies. IoT and data sharing are also vectors of economic gains for hospitals (centralization and direct access to data via the cloud, continuous updating of medical information, etc.)

Moreover, in health care, IoT helps to deploy personal networks for monitoring and tracking clinical data, especially for the aged. It also enables to facilitate the monitoring of patients at home and to provide solutions to improve the autonomy for people with reduced mobility. Thus, with the ubiquity of communication systems that allow the doctor-patient relationship to be maintained remotely, smart homes are becoming an important part of the health care system and the hospital remains an essential specialized environment and the site of critical care. Additionally, the integration of IoT applications in healthcare allows a doctor in one hospital to use the internet to interact with a doctor in another hospital. As a further example, a paramedic at the scene of an accident can inform the hospital's system coordinator of a patient's current status using his or her personal data (PDA). The doctor, patient, nurse, social worker (SW), paramedic, system coordinator (SC), and system administrator (SA) are the roles or actors involved in the communications, designated from 1 to 7 in Figure 1.

The shaded area in Figure 1 represents communications internal to the enterprise. Communication can also take place between internal and external networks, including remote users such as patients and FTs at home, physicians at another hospital, or paramedics at an accident scene. Information from the rescuer is relayed over the wireless network using a PDA and received by the hospital's SC so that the rescuer can take the necessary action. In the meantime, the SC can call for a medical team.



(1) Doctor-to-Doctor,
(2) Doctor-to-Patient,
(3) Doctor-to-Nurse,
(4) Nurse-to-Patient,
(5) Paramedic-to- SC,
(6) Social workers-to-Doctor (Doctor, Nurse, Patient, SC, SW, and Paramedic) and
(7) SA to (Doctor, Nurse, Patient, SC, SW, and Paramedic).

Fig.1: Depicts the actors and communications in the e-health field.

3. Security in Mobile Agents Systems

3.1. Mobile Agents System

A mobile agents system is composed of one or more platforms. There are different types of mobile agent platforms (Aglet, Jade, etc.). A mobile agent platform or agent execution environment or agent development tool is a middleware that provides the appropriate functionalities for mobile agents to authenticate execute, communicate If a doctor wants to send a message to a nurse, for example, the Doctor-agent understands how to handle communication processes and establish communication with the Nurse-agent. The Doctor-agent can work with the Encryption agent to ensure that the communication is encrypted and digitally signed before delivering it to the Nurse-agent because the information is sensitive. If the Doctor-agent discovers that the Nurse-agent is unavailable after the message has been delivered, the Doctor-agent will either store the message or try to send it again later, or delete it within a given time frame. This shows that the agent is autonomous and it does not need user's intervention and can do tasks on its own. In addition, agent systems are extendible. A new agent can be created instantly and added to the existing system to represent a new user such as a researcher, without reconfiguring the whole system

A mobile agent platform's primary purpose is to provide a high-level abstraction framework for the development, execution, and management of multi-agent systems [8]. One or more places can be found on a platform. The source and destination locations may be on the same platform or on separate platforms. It is possible for a platform to be single-user or multi-user. Agents and locations can be owned by a user. Only one user can have access to a location. An agent is in the same boat. In a single location, one or more agents can run. The location is the platform's executing context for agents, which provides unique services and serves as a meeting point for agents.

3.2. The Security Criteria On Mobile Agents Systems

These criteria are necessary in order to ensure the privacy of patients during and after communications in which data must be kept secure. The level of obedience to the security requirements determines the security performance of a mobile agent system. Based on [19][16][10], the security criteria for mobile agent systems are as follows:

- *Authentication*: This is the ability to verify the identity of the two interacting entities that they are what they claim to be.
- *Integrity:* The communicating entities and the exchanged messages must be protected from unauthorized changes.
- *Authenticity:* The identity verification and at the same time the authentication of the communicating parties and integrity of the transmitted message or agent.
- *Confidentiality:* All private data exchanged, stored on a platform or carried by an agent must remain accessible only to authorized entities.
- *Access Control:* This is the definition of authorizations that specify who is allowed to do what, how and under what condition.
- *Non-repudiation:* The technique of non-repudiation is to eliminate the risk that an agent or a place may deny sending the data or perform an action.
- *Availability:* The places and the agents must be available to ensure the usability of data and services to local and remote agents.

3.3. Individual Attacks: In Mobile Agents Systems

Individual attacks are launched by one user account. Based on the literature [19][20], [16], [10] and [14], there are four categories of individual attacks in mobile agents based systems (figure 2).

3.3.1. Attacks Of An Agent(S) To Another

This class presents attacks that a user can carry out on an agent using one or sev- eral agents. Mobile agent attacks can take different forms. In the literature, there are mainly three types of attacks:

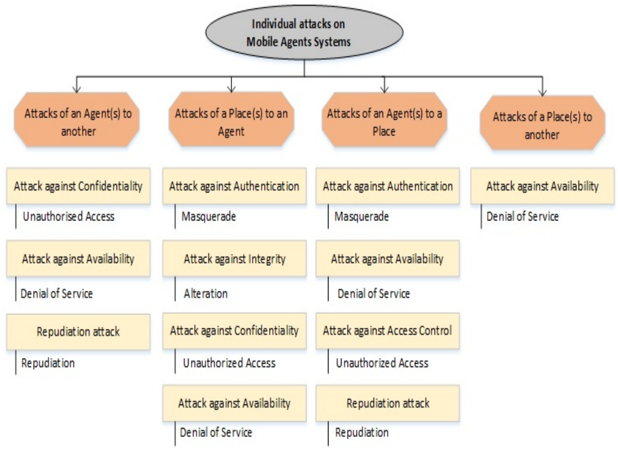

Individual attacks on Mobile Agents Systems
Attacks of an Agent(s) to another
Attacks of a Place(s) to an Agent
Attacks of an Agent(s) to a Place
Attacks of a Place(s) to another
Attack against Confidentiality
Unauthorised Access
Attack against Availability
Denial of Service
Repudiation attack
Repudiation
Attack against Authentication
Masquerade
Attack against Integrity
Alteration
Attack against Confidentiality
Unauthorized Access
Attack against Availability
Denial of Service
Attack against Authentication
Masquerade
Attack against Availability
Denial of Service
Attack against Access Control
Unauthorized Access
Repudiation attack
Repudiation
Attack against Availability
Denial of Service

Fig.2: Individual Attacks in Mobile Agents Systems

a) The Attack against the Confidentiality

- *Unauthorized access:* it occurs when an agent is able to access the information about the activity of another agent. This may allow a malicious agent to use this information to his own interest.

b) The Attack against the Availability

- *Delay of Service:* A delay of service attack can be launched against a victim agent by one or several agents when it provides an answer to a request after a long period that engenders the disruption of the mission of the agent. Also, the malicious agent can distribute false or useless information to prevent the other agent from completing its tasks properly or within the fixed time frame.
- *Denial of Service (DoS):* A denial of service may occur when one or several agents repeatedly or overwhelmingly send messages to another agent that can harm the message management process of the receiver agent. So, the availability of the agent will be affected and it can go up to harming the availability of the execution place too.

c) The Attack against the Non-Repudiation

- *Repudiation:* The repudiation occurs when an agent denies the fact that he having interacted or having provided results to another agent.

3.3.2. Attacks Of A Place(S) To An Agent

To run an agent, the place must have access to its code, its state, and its data. There- fore, an agent that runs on a place is exposed to security threats that can affect its authentication integrity, confidentiality. Also a place can launch an attack against the availability of an agent.

a) The Attack against the Authentication

- *Masquerade:* it occurs when a malicious place uses the identity of another place to trick visitor agents.

b) The Attack against the Integrity

- *Alteration:* it occurs when a malicious place is able to modify the code, the state of execution or the produced data of a visitor agent.

c) The Attack against the Confidentiality

- *Unauthorized access*: It is an attack that happens when a place gets access to parts of the agent for which it is not authorized to access.

d) The Attack against the Availability

- *Denial of Service (DoS):* it occurs when one or several places communicate via its own agents with the victim mobile agent excessively to degrade its performance (its response time).

3.3.3. Attacks Of An Agent(S) To A Place

This category presents attacks carried on by one or several malicious agents to disturb the victim place and it may take advantage of the security failures of the place.

a) The Attack against the Authentication

- *Masquerade:* An agent needs to authenticate before it is instantiated in the visited place. A malicious agent can attack a place using the identity of another agent to access services and resources for which it does not have the right to access.

b) The Attack against the Availability

- *Denial of services (DoS) :* one or several malicious mobile agents from the same place can launch denial of service attacks by excessively consuming the resources, by cloning themselves indefinitely or unending migrating. These DoS attacks can be launched to exploit the vulnerabilities of the system, to disrupt the services offered by the place or to degrade its performance. Ensuring the availability of a place includes ensuring the availability of the agents on it.

c) The Attack against the Access Control

- *Unauthorized access*: Every agent which visits a place must respect its security policy. An agent which has access to a place and its services without proper authorization may harm its performance. A place that hosts agents representing different users must ensure that the agents do not have access to services and resources for which they have no authorization.

d) The Attack against the Non-Repudiation

- *Repudiation:* occurs when an agent can deny performing an action. For example, an agent belies the fact that it visited a place and used resources.

3.3.4. Attacks Of A Place(S) To Another

a) The Attack against the Availability

- *Denial of services:* The denial of service against a place can be launched following an agreement between several agents coming from several places. The attacker agents are executed around the same time on the victim place.

3.4. Collaborative Attacks In Mobile Agents Systems

A collaborative attack is launched by human attackers or criminal organizations using multiple user accounts. Collaboration can be between accounts of users from the same platform or from multi-platforms. Collaborative attacks are more powerful than individual attacks because collaborative attacks can generate more serious impacts in a shorter time. The bigger the number is the faster the attack is, it can go up to a fairly fast attack in a way that even the defense system can’t stop the attack or even mitigates it. A collaborative attack can launch an undetectable attack, due to the fact that the involved parties do not violate the security policy, but because of their number, they are able to generate a rate of activity on the target entity in a manner to provoke a security gap. Another type is where the involved parties can be in collusion together to fallacy the target entity. In this paper, besides the individual attacks, we are interested essentially in the first type of collaborative attacks where the collaborators are able to harm the target entity using scenarios executed by complicit parties that can engender a security gap against the availability of an agent and/or a place. Such attacks target at eliminating a service’s availability by exhausting there sources of the service’s host entity, like memory or processing resources. We are interested essentially in the category of Denial-of-Service attacks which is called resource exhaustion [21] [22] by consuming the place computing resources (non-blocking behaviors or sending too many messages) or overloading the place with too many agents or too many services request [9].

4. The Multi-agent Based Security Framework

4.1. Our Framework: Architecture Overview

Our security framework is composed of five sort of communication necessitates a distinct level of security protection due to the sensitivity of the material. We classify communication levels in this study so that different security methods can be used to secure different levels of communication. We also plan to demonstrate the system's flexibility to adapt to a wide range of user requirements. Figure 3 describes the process of integrating our security framework into an e-marketplace system. In addition, low-processing-power devices (such as PDAs and smart phones) can benefit from suitable security protection. The following is an example of a classification:

- Level 1: Communication that is extremely sensitive. This type of communication is extremely sensitive, and the highest level of security must be maintained to protect the privacy, confidentiality, and integrity of the medical information sent, such as patient information (Figure 4). Information about one's personal life and health. Doctor is one of the people who have communicated with us. The communications include Doctor to Doctor, Doctor to Patient, Nurse to Doctor and Nurse to Patient.
- Level 2: Communication that is extremely sensitive. Because it incorporates wireless communication, SC to paramedic communication is classified as Level 2. The mobile service was chosen because it offers a larger breadth of coverage. The information transferred is related to current patient’s condition and considered as highly sensitive and therefore the privacy of the information must be protected events, it consults the policy database extract the visit rights (according to the role) of the user owner of the coming agent and of its originator platform. Then the Visit Sensor Analyzer Agent compares the visit right values with the current values related to the treated visit. If the comparison indicates that the related user or platform is making an abnormal activity and a deliberate attempt to violate the security policy then the Visit Sensor Analyzer Agent kills the malicious agent. The administrator can be stricter and choose to not accept more agents from the malicious user.
- Level 3: Medium Sensitive Communication Social Workers to Doctors are examples of Level 3 communication. There is only generic information involved, and medium security protection is required.
- Level 4: Low Sensitive Communication the SA to all other users are involved in Level 4 communication. Because these communications are considered low-risk, low-security protection is required. The SA communicates with other users about the highly confidential user account and password. The SA can phone or email the users, using an unsecured email program, to request that they pick up their Id and password at the office. Alternatively, the information can be sent by encrypted email by the system administrator that comes from the malicious user.
- Level 5: The general public. This form of communication is available to the whole population. This communication channel is typically used by the organization to disseminate important announcements as well as to educate the public. This classification can be used to determine the level of security processes for each level. In addition, with this classification the organization can save CPU processing power and

increase system performance, because only the most sensitive information requires the highest security processes.

5. Implementation and Test Results

For the implementation, we have used the Jade platform [13] and especially the Jade Security add-on [15] and the jade PKI add-on [11]. This choice is not arbitrary; it is made based on the comparative study of mobile agent platforms established in [19] which concludes that Jade is among the most secured platforms of mobile agents. The PKI add-on provides the Jade platform with the possibility of using the digital signature of the home container which is very useful for the verification of authentication and integrity criteria. Using the PKI add-on, the platform provides a key distribution which allows avoiding a considerable administrative burden and making the system less susceptible to several attacks such as masquerade. We implement our Framework using Sun's Java Development Kit version 1.8.0 and the Netbeans 8.2. All the experiments were conducted on our security Framework that we implement as a security layer on an e-health. We focus on the availability criterion on the execution place. To evaluate the performance of our model, we made DoS and DDoS tests to check if malicious agents are able to disturb the place or even prevent it from fulfilling its regular tasks (e.g. executing other test agents). To quantify the test results, we measured the time required for the test agent to perform a cycle of a cyclic behavior. This was done by recording each time when the test agent triggers the execution of a cycle of a cyclic behavior, and when it ends. The more the place of execution was affected by an attack, the more time it took for the test agent to complete the execution of a behavior cycle, and the lower is the frequency of the execution of a behavior cycle.

Thus, the time to complete a test agent behavior cycle and its frequency of execution are simple indicators of the effectiveness of an attack and its impact on the victim place. The following DoS and DDoS tests were implemented:

– Overloading the place with too many agents with a non-blocking behavior which are coming from the same user account.

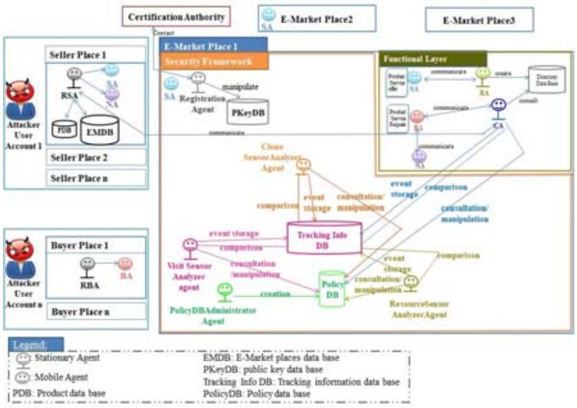


Fig.3: Our Security Framework Integrated on a System of e-Market Places

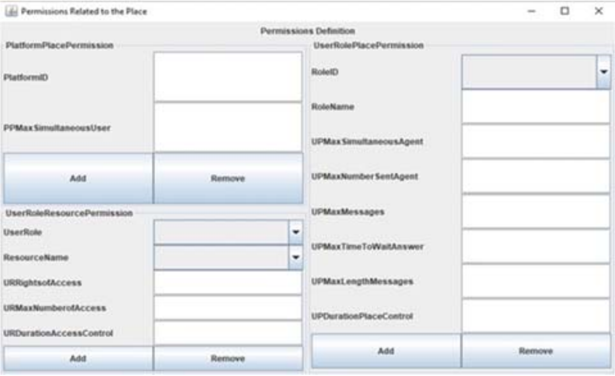


Fig4: The architecture of the e-health services security framework.

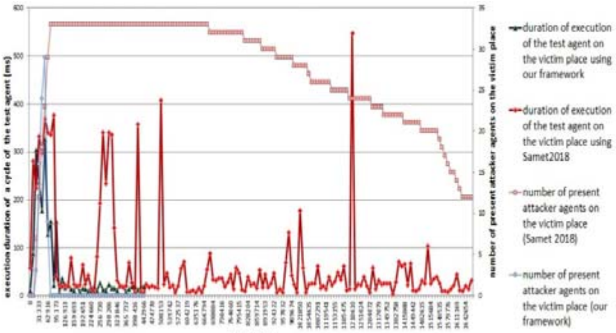


FIGURE 5: Overloading the place with too many agents with a non-blocking behavior which are coming from the same.

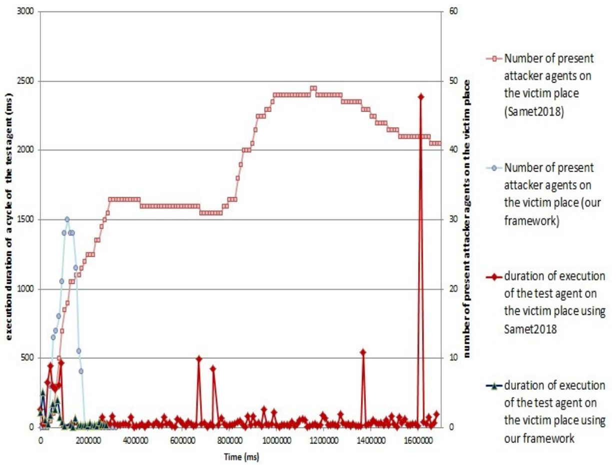


Fig.6: Overloading the place with too many agents with a non-blocking behavior which are coming from several users accounts

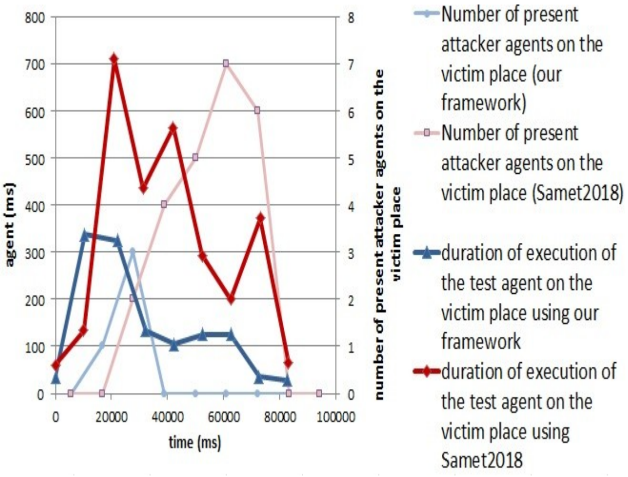


Fig.7: Consuming the place's computing resources by sending too many messages to an agent at the same time (one attacker user account)

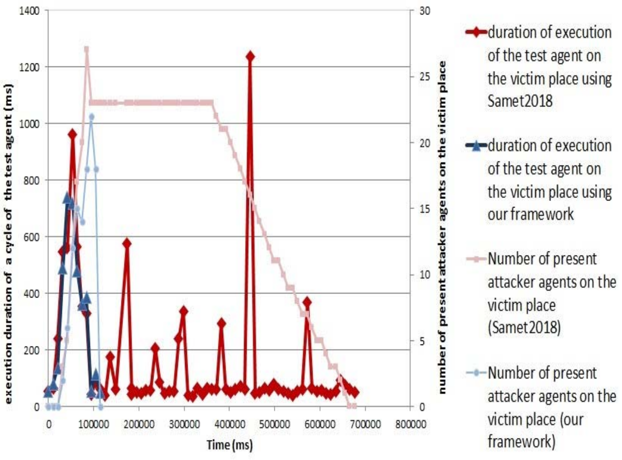


Fig.8: Consuming the place's computing resources by sending too many messages to an agent at the same time (several attackers users accounts)

– Overloading the place with too many agents with a non-blocking behavior which are coming from several users accounts.

– Consuming the place's computing resources by sending too many messages to an agent at the same time. The sent messages are from agents belonging to the same user account.

– Consuming the place's computing resources by sending too many messages to an agent at the same time. The sent messages are from agents belonging to several users' accounts.

We implement and compare two versions of the security framework: one which is implemented using the security model which is defined on [20] and another which is implemented using the security model defined in this paper. It is to be noted that the security policy is set up, as it is defined, according to users roles on our framework and according to places and agents roles on the case of the framework using the model of [20]. The figures 5, 6, 7 and 8 plot the measurement results. On the x-axis the time x = 0 indicates the start of the attack and the time x = t indicates the time of the end of the execution of a behavior cycle of the test agent. On the y-axis the time y = d indicates the duration of execution of a test agent behavior cycle. Throughout the attack, we calculate the execution duration of a behavior cycle of the test agent which is localized on the victim place. We calculate also the number of malicious agents that remain alive in the victim place during the attack. In the test we choose the more critical strategy where we adopt a tolerable security policy: the security framework kills only the attacker agents; whereas we were able to choose to not accept more agents from a malicious user account or a malicious platform.

- Overloading the place with too many agents with a non-blocking behavior:

We launched an attack where the e-health place is overloaded with agents from different places. The attacker user sends, in a short window of time, a set of agents that execute non-blocking behaviors in the victim e-health places. Figure 5 plot the measurement results in the case that the attacker places belonging to the same user account and Figure 6 plot the measurement results in the case that the attacker places belonging to different users accounts. As the figures show, our frame- work is faster to cope with the attack in the case of the individual attack as well as in the case of the cooperative attack. Using the model defined in [20] it takes a lot of time to execute the test behavior since the attack has taken more influence and the number of the attacker places cannot be limited.

- Consuming the place's computing resources by sending too many messages to an agent at the same time

We launched an attack where many agents (Social workers) send messages to the recorder agent (Doctor or nurse or Sc or SA) on the victim e-health. Figure 7 plots the measurement results in the case that the attacker agents belonging to the same user account and Figure 8 plots the measurement results in the case that the attacker agents belonging to different users ac- counts. As the chart shows, using our model the framework shows very interesting results. The victim place was only slightly affected and was able to return to its nor- mal function in a short time compared to the results obtained when using the model defined in [20], where the duration of execution of the test behavior was remarkably affected in the case of the individual attack as well as in the case of the cooperative attack.

6. Discussion and Future Work

The benefit of this framework is that it provides an alternate way to protect e-health user communication by enabling multi-level communications and a secure environment in which to communicate. In order to earn users' trust and confidence in communicating private data over the network, a multi-level communications method is proposed to provide for different levels of users while also being flexible enough to accommodate different sorts of user needs. For future work, the framework will be built using a multi-agent approach in order to investigate the agents' ability to coordinate and collaborate in order to improve the security processes' performance.

7. Conclusion

We created a security framework for mobile agent systems based on a standard security model that enables for the identification and prevention of a variety of individual and cooperative threats. Because the size of the policy database is not large, this model makes it simple to set up a security policy and exhibits a time performance. We get the expected results from the implementation. The suggested security architecture was able to detect the simulated attacks and eliminate the attacker agents. This fact is meant to demonstrate that the proposed security model and security framework may be used to secure mobile agent systems in practice. We will study how adding a trust layer to the proposed framework will improve the performance of our framework in future work.

Acknowledgments

The authors gratefully acknowledge the approval and support of this research study by the grant **No SAT-2019-1-10-F- 8342** from the Deanship of Scientific Research at Northern Border University, Arar, K.S.A.

References

[1] M. Barua et al., PEACE: An efficient and secure patientcentric access control scheme for eHealth care system, IEEE Conference on Computer Communications Workshops (INFOCOMWKSHPS), 970–975 (2011).

[2] M. A. Khfagy, O. Reyad, Y. AbdelSatar and N. F Omran, Multi-filter score-level fusion for fingerprint verification, In A. E. Hassanien et al. (Eds.): AMLTA 2018, AISC 723, Springer Cham, 624–633 (2018).

[3] J. L. Fernandez-Aleman et al., Security and privacy in electronic health records: A systematic literature review, J. of Biomedical Informatics 46, 541–562 (2013).

[4] W. M. Abd-Elhafiez, O. Reyad, M. A. Mofaddel and M. Fathy, Image Encryption Algorithm Methodology Based on Multi-mapping Image Pixel, In: A. Hassanien, et al. (eds.): AMLTA 2019. AISC 921, Springer Cham, 645–655 (2020).

[5] Z. F. Khan, Automated Segmentation of Lung Parenchyma using Colour based Fuzzy C-Means Clustering, Springer J. of Electrical Engineering and Technology 14, 2163–2169(2019).

[6] S. S. Shinde and D. Patil, Review on Security and Privacy For Mobile Healthcare Networks: From A Quality Of Protection Perspective, Int. J. of Engineering Research- Online Peer Reviewed International Journal, 3(6), (2015).

[7] Beydoun, G., Low, G.C., Mouratidis, H., Henderson-Sellers, B.: Modelling mas-specific security fea- tures (2007)

[8] Bhamra, G.S., Verma, A., Patel, R.: Intelligent software agent technology: an overview. International Journal of Computer Applications 89(2), 19–31 (2014)

[9] Bürkle, A., Hertel, A., Müller, W., Wieser, M.: Evaluating the security of mobile agent platforms. Autonomous Agents and Multi-Agent Systems 18(2), 295–311 (2009)

[10] Bellifemine, F., Caire, G., Poggi, A., Rimassa, G.: Jade: A software framework for developing multi- agent applications. lessons learned. Information and Software Technology 50(1-2), 10–21 (2008)

[11] lnowski ˙,A.P.Z.:JADE-PKI 1.0 Manual (2012). URL https://jade.tilab.com/doc/tutorials/PKI_Guide.pdf

[12] Feng, Y., Hori, Y., Sakurai, K.: A behavior-based online engine for detecting distributed cyber-attacks. In: International Workshop on Information Security Applications, pp. 79–89. Springer (2016)

[13] Bellifemine, F., Caire, G., Poggi, A., Rimassa, G.: Jade: A software framework for developing multi- agent applications. lessons learned. Information and Software Technology 50(1-2), 10–21 (2008)

[14] Hachicha, H., Samet, D., Ghedira, K.: A conceptual approach to place security in systems of mobile agents. In: German Conference on Multiagent System Technologies, pp. 154–170. Springer (2015)

[15] ADEBoard: Jade Security Guide (2005). URL https://jade.tilab.com/doc/tutorials/JADE_Security.pdf

[16] Jansen, W., Karygiannis, T.: Nist special publication 800-19– mobile agent security, national institute of standards and technology. URL http://csrc. ncsl. nist. gov/mobilesecurity/Publications/sp800-19. pdf (2000)

[17] T. MuthamilSelvan, B. Balamurugan, Comparative Performance Analysis of Various Classifiers for Cloud E-Health Users, Int. J. of E-Health and Medical Communications 10, 86–101 (2019).

[18] Montanari, R., Stefanelli, C., Dulay, N.: Flexible security policies for mobile agent systems. Micro- processors and Microsystems (2), 93–99 (2001)

[19] Samet, D., Ktata, F.B., Ghedira, K.: Security and trust on mobile agent platforms: A survey. In: G. Jezic, M. Kusek, Y.H.J. Chen-Burger, R.J. Howlett, L.C. Jain (eds.) Agent and Multi-Agent Systems: Technology and Applications, pp. 42–52. Springer International Publishing, Cham (2017)

[20] Samet, D., Ktata, F.B., Ghedira, K.: Securing mobile agents, stationary agents and places in mobile agents systems. In: KES International Symposium on Agent and Multi-Agent Systems: Technologies and Applications, pp. 97–109. Springer (2018)

[21] chäfer, G.: Sabotageangriffe auf kommunikationsinfrastrukturen: Angriffstechniken und ab- wehrmaßnahmen. Praxis der Informationsverarbeitung und Kommunikation 28(3), 130–139 (2005).

[22] Chen, X., Zhou, J., Shi, M., Chen, Y., & Wen, J. Distributed resilient control against denial of service attacks in DC microgrids with constant power load. Renewable and Sustainable Energy Reviews, 153, 111792. (2022).

Ayari Nadia was born in Tunisia. She received her PhD degrees 2015 in Electronics from Faculty of Sciences Tunis .She is Currently Assistant Professor in College of Science and arts at Northern border University ,KSA. She is a Researcher in the laboratory of electronics and microelectronics, Faculty of Sciences of Monastir in Tunisia. Her research interests are related to these topics: Electronics; RF, Analog, E-health, internet of things and Mixed microelectronic.

Farah BARIKA KTATA is currently associate professor of computer science at Higher Institute of Applied Sciences and Technology of Sousse (ISSAT of Sousse). Her research interests mainly include Artificial Intelligence, IT security and Database Management Systems. She is a senior researcher at MIRACL (Multimedia, InfoRmation Systems and Advanced Computing Laboratory). Actually she is Vice Director of ISSAT and President of ATIA (Tunisian Association of Artificial Intelligence).

Belgacem Hamdi Has a Ph.D. in Microelectronics Design from Institut National Polytechnique de Grenoble, France. He is currently a professor at the Higher Institute of Applied Science and Technology of Sousse (ISSATSo), Sousse, Tunisia. He is a Researcher and team leader in the laboratory of electronics and microelectronics. His research interests are related to these topics: Electronics Engineering; Digital, Analog, and Mixed microelectronic; Fault-Tolerant circuits.