Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 210 (2022) 149–156

Procedia Computer Science

www.elsevier.com/locate/procedia

The 12th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH 2022)
October 26-28, 2022, Leuven, Belgium

Swarm Intelligence Model for Securing Healthcare Ecosystem

Patrizia Ribino[a,*], Mario Ciampi[a], Shareeful Islam[b,d], Spyridon Papastergiou[c,d]

[a]*Institute for High Performance Computing and Networking, National Research Council of Italy*
[b]*School of Computing and Information Science, Anglia Ruskin University, United Kingdom*
[c]*Department of Informatics, University of Piraeus, Greece*
[d]*Focal Point , Belgium*

Abstract

The healthcare sector is constantly facing challenges in ensuring security due to the sophisticated attacks by the threat actor for acquiring sensitive patient data. An attack on the system can pose any potential risk to the business continuity. The increased use of information technology in the modern healthcare system makes medical devices and systems more vulnerable to exploitation and possible cyber-security attacks. This paper proposes a flexible and decentralized cyber-security model based on the integration of multi-agent systems and swarm intelligence for tackling the propagation of attacks inside interconnected healthcare organizations and ensuring the whole healthcare ecosystem's security and resilience. The proposed model is based on the collaboration between the agents with different functions and cognitive capabilities, named primary and supervisor agents. Primary agents are lightweight BDI (Belief-Desire-Intention) agents implementing a minimum set of capabilities for monitoring a specific area of the healthcare system; supervisor agents incorporate an extended version of the BDI reasoning to provide advanced capabilities for securing the overall healthcare system by enabling collective intelligence and overall cyber-security awareness. The preliminary experimental results show that the model is robust and responsive for securing the ecosystem.

Keywords: Healthcare Ecosystem; Cyber-Security; Swarm Intelligence; Multi-Agent Systems; Belief-Desire-Intention

1. Introduction

The increased use of information technology (IT) in the modern healthcare system leads medical devices to be more interfaced with other IT equipment, but these devices generally lack adequate security measures. Therefore, vulnerabilities of these devices can propagate to other parts of the network. Additionally, Health Care Information Infrastructure (HCII) contains a large number of legacy systems that attackers constantly explore for potential exploitation.

* Corresponding author. Tel.: +39 091 8031083
E-mail address: patrizia.ribino@icar.cnr.it

1877-0509
10.1016/j.procs.2022.10.131

In recent years, the value of personal medical data has increased on the black market. Credit card information and Personal Identifiable Information (PII) sell for USD 1-2, but Personal Health Information (PHI) can sell for as much as USD 363. Nearly 90% of healthcare organizations experienced risk from a data breach in 2018 [21]. A report by KPMG highlights that the healthcare industry is behind other industries in protecting its infrastructure and data [3]. Cyber threats are a significant challenge for the healthcare domain, and it is necessary to protect from these threats and related risks and ensure resilience for the overall healthcare system [14].

The distributed and heterogeneous nature of the healthcare domain poses new challenges for securing the healthcare ecosystem. Flexible and decentralized cyber-security models are required for tackling the propagation of the attacks inside interconnected healthcare organizations. Swarm Intelligence (SI) [4] is a collection of bio-inspired approaches where a group of autonomous entities, without central control, exhibit a collective behaviour by interacting with the environment to solve a distributed problem. On the other hand, multi-agent systems are among the most representative artificial systems dealing with complexity and distribution [25], making them a natural choice for realizing swarm intelligence approaches [12, 8]. The major strength of such systems is the ability to reach optimized decisions based on the actions taken by individual agents.

In this paper, we propose a novel model to bring cyber-security to the overall healthcare ecosystem that considers the healthcare domain's peculiarities by exploiting the features of multi-agent and swarm intelligence systems. The proposed model is based on the collaboration between two kinds of intelligent agents, named primary and supervisor agents, endowed with different functions and cognitive capabilities based on the Belief-Desire-Intention (BDI) paradigm [10, 7]. Mainly, primary agents are basic BDI agents implementing a minimum set of capabilities for monitoring a set of assets of the healthcare system by performing individual tasks. Conversely, supervisor agents incorporate an extended version of the BDI reasoning to provide advanced capabilities for tackling the risks within the healthcare system by enabling collective intelligence and overall cyber-security awareness. The resulting multi-agent system exhibits self-organising and swarm-inspired coordination capabilities obtained by the direct collaboration between primary agents that, acting locally, provide the supervisor agent with local information and by indirect collaboration between supervisor agents by exchanging stigmergic information through the environment that allows each supervisor agent to make a collective informed decision. Adopting the proposed model allows for achieving higher-order intelligence that cannot be obtained by single agents and provides several advantages such as robustness, resilience and adaptation. The main contributions of this paper are: (i) a novel swarm intelligence model for dealing with security issues for the overall healthcare system; and (ii) an algorithm that extends the BDI reasoning by introducing stigmergic events and situation awareness by enabling indirect collaboration between supervisor agents of interconnected healthcare organizations.

The rest of the paper is organized as follows. Section 2 shows the related literature. Section 3 introduces the proposed model. Finally, in Section 4 conclusions are presented.

2. Related works

Numerous solutions have been proposed in the literature to protect information systems from unauthorized access and use. These methods usually employ security mechanisms such as password protection, firewall, access control, and encryption. However, these techniques have become ineffective against increasingly sophisticated cyber attacks due to the exponential growth of ubiquitous devices and the widespread adoption of IoT across multiple domains. Additionally, current cyber defence solutions involve humans at multiple levels causing slow and asynchronous information flow. Therefore, more advanced techniques have been proposed to deal with cyber attacks. One such technique includes swarm intelligence (SI) due to the flexibility provided and the learning ability that improve the performance of cyber protection systems. The adoption of SI approaches in security mainly focuses on anomaly or intrusion detection in computer networks. A recent review study [20] provided an exhaustive overview of SI approaches in intrusion detection systems identifying four main categories. The first category consists of studies that use SI-based approaches to solve classification problems. These models use SI algorithms to inspect network packets for anomaly detection directly. To cite a few, Boughanci et al. [6] presented a Fuzzy PSO-based classification model where PSO optimizes the fuzzy rules to achieve better performance. Kolias et al. [15] combined classification rule with ACO to devise a distributed intrusion detection solution for wireless networks. In the second category are classified methods that employ SI algorithms to optimize Machine learning-based classifiers and provide an automated way of selecting weights

to enhance the classification performance of these ML-based classification models. Among them, Shi et al. [23] presented a hybrid model with a support vector machine (SVM) classifier, whose parameters are optimized with PSO. Enache and Patriciu [9] implemented an SVM-based classifier whose parameters are optimized by PSO and ABC approaches with Information Gain (IG) as a feature selection approach to attain high detection and low false alarm rates than traditional SVMs. The third category consists of works that adopt SI for data dimensionality reduction. Among them, Malik et al. [18] implement a feature selection approach for classifying probe attacks. Cordero and Guha [17] presented a distributed cooperative approach, i.e. BPSO, for selecting a small set of features and filtering out most of the noise from data. Finally, the fourth category consists of approaches that simultaneously employ SI algorithms for feature selection and optimization of ML-based classifiers. To cite one, in [24] Jooghi and Mirvaziri presented an ANN-based intrusion detection model whose weights and biases are optimized by PSO to reduce the training complexity. Another recent survey presented in [19] provides an overview of the SI algorithms applied in anomaly detection. Ant Colony Optimisation (ACO) is one of the most used techniques to solve feature selection problems because of its simplicity and quick convergence. In [1] Aghdam and Kabiri designed a new heuristic function based on the length of the selected feature vector. The ACO-based clustering method is used to detect the outliers. Particle swarm optimization (PSO) is widely used in anomaly detection due to its low computational complexity. Lima et al. [16] presented the signature-based approach to profile the normal network traffic behaviour in a realistic traffic environment. Finally, firefly algorithms are efficacious approaches to mathematical optimization and engineering problems inspired by the flashing behaviour of some insects. In [22] authors present a model to identify anomalous network traffic based on traffic characterization, which uses the Firefly and Genetic Algorithms to classify network flows.

Although Swarm Intelligence approaches have received considerable attention in the context of cybersecurity [20, 19], to the best of our knowledge, no works address such problems in the context of the healthcare ecosystem focusing on cyber-security risks for the overall system resilience. This paper proposes a flexible and decentralized cyber-security model based on the integration of multi-agent systems and swarm intelligence for tackling the propagation of attacks inside interconnected healthcare organizations and ensuring the whole healthcare ecosystem security.

3. Swarm Intelligence Model for healthcare ecosystem

The proposed model consists of a population of agents interacting with each other and their surrounding environment to ensure the security of the overall healthcare ecosystem. These interactions apply bio-inspired techniques (such as firefly synchronization and stigmergy) to facilitate and ensure the efficient communications and management of large-scale, ad-hoc and distributed networks typical of large interconnected HCIIs. The main novelty of the proposed approach is the exploitation of swarm intelligence and multi-agent systems so that healthcare entities, i.e., system, practitioner, and other assets, can act as sole intelligence. Hence, the actions performed by the healthcare entities gradually accumulate to form intelligence of a higher level which does not exist in any of the individual members and drives the community towards making optimal decisions, such as choosing the proper control to mitigate the risk.

3.1. Heathcare domain description

Healthcare entities are the individual hospital, clinic, diagnostic centre, and other related stakeholders responsible for delivering healthcare services. They are responsible for performing specific actions relating to risk management based on security-related information. Such entities follow a hierarchical level of abstraction from healthcare information infrastructures to interdependent Healthcare Information Infrastructure. In particular, the Healthcare Information Infrastructure (HCII) implies the components of the overall IT infrastructure necessary to deliver healthcare services, including the patient healthcare devices, communication networks, information systems, and other relevant ICT infrastructure. HCII can also be considered systems that provide resources or services on which essential functions depend. Possible incapacitation or destruction would significantly affect society's economy, security and health. Such HCIIs are considered critical and sensitive due to their importance for people's well-being and safety.

Interdependent Healthcare Information Infrastructure (iHCII) connects the individual HCII to deliver supply chain healthcare services and composes the whole health ecosystem. The security of iHCII depends on HCIIs. The interdependency among the independent HCIIs is characterized by the distribution of services, data sharing, and collaboration among the activities for the informed decision-making relating to risk management and incident handling.

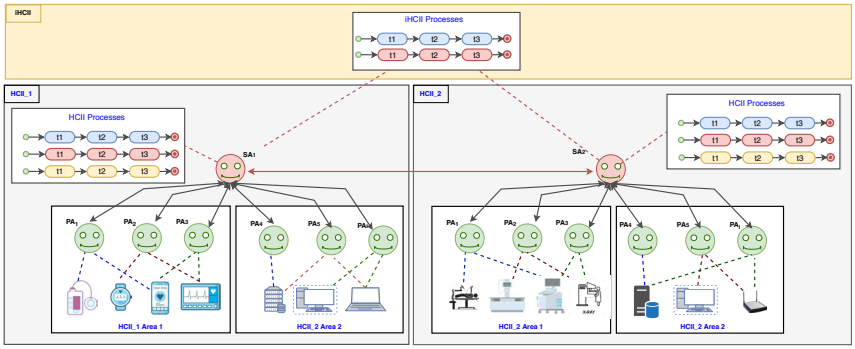


Fig. 1: Agents within the healthcare ecosystem.

3.2. Model abstractions

Agents are the main elements of the proposed self-organized swarm intelligence model. They are conceptual entities within the HCII who are autonomous and capable of effectively operating in dynamic and open healthcare environments. Agents interact with the environment and cooperate with other agents to come to a decision. A healthcare ecosystem is a dynamic and complex environment where agents must communicate and consider the current state of their dynamic environment with existing information. Following the conceptual healthcare hierarchy, the proposed model comprises two different agents, i.e., primary and supervisor agents, performing specific functionalities for mitigating risk and incidents in the overall healthcare ecosystem. Each agent plays a role described by the functions that it should perform. A role consists of permission, activities, and protocols. Permissions to resources are the rights associated with each role, mainly to access any resource such as inventory of assets, threat profile, and vulnerability information. The activities are actions carried out by the agent to support the role, such as risk identification and calculation of risk level. Finally, the protocol represents the communication model among the agents to interact with each other to achieve any security goal. Fig.1 shows the hierarchical organization of primary and supervisor agents within two interconnected HCII. Mainly, *Primary Agents*(PA) are active agents able to monitor and protect specific HCII areas. These agents collect and analyze information relating to risks (i.e., individual risk) and incidents about the assets they manage (e.g., medical and IoT devices, servers, databases). Such information will be communicated to the supervisor agent. *Supervisor Agents* (SA) are autonomous intelligence agents who undertake actionable decisions for tackling the risks and related incidents at a higher level. In particular, supervisor agents are responsible for the collective decision-making for managing risks by also looking at the healthcare processes within their HCII and the interdependent HCIIs. SA are swarm-inspired; they can correlate the data from the primary agents and other supervisor agents and analyze the data to identify the pattern for risk (i.e., cascading risk) and incident (i.e., attack path). SAs aim to ensure the cyber defence of the overall healthcare ecosystem. The SA receives the risk and incident-related data from the PA and correlates the data for decision-making. Therefore, specific swarm functionalities such as population-based approach and firefly synchronization are integrated into the SA for risk assessment and management.

3.3. Integrating Swarming and BDI Agents

As previously said, the proposed self-organized swarm intelligence model is based on the collaboration between primary and supervisor agents. Due to their different roles in the healthcare system, we model such agents with different cognitive capabilities by adopting the BDI paradigm. In particular, while primary agents rely on classical BDI reasoning, for the supervisor agents, we propose an extended BDI reasoning to integrate stigmergic events in the reasoning cycle that influence the supervisor agent's situation awareness and lead to cooperative decision-making. Stigmergy [11] is a mechanism of indirect coordination based on the principle that work performed by an agent leaves a trace in the environment that stimulates the performance of subsequent work of other agents. This mediation via the environment ensures that tasks are executed in the proper order, without any need for planning, control, or direct interaction between the agents. By exploiting stigmergic events, supervisor agents assess anomalous activity patterns.

Fig.2 shows a schematic representation of the supervisor agent model within the healthcare domain. According to the classical BDI paradigm, a supervisor agent has a set of beliefs representing its knowledge base, a set of desires

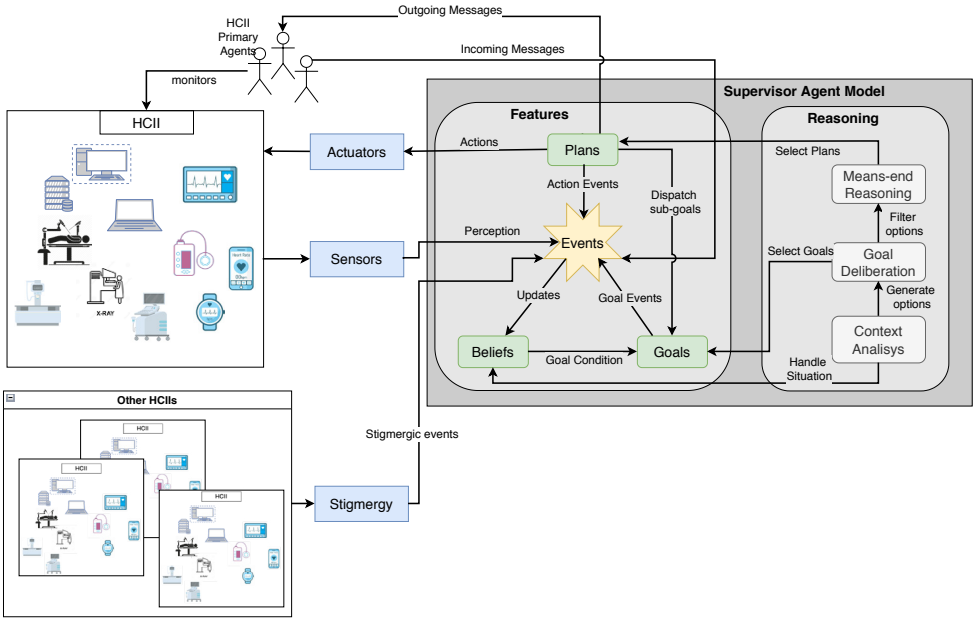


Fig. 2: BDI Architecture of Supervisor Agents.

representing its goals, and a set of intentions representing the commitment to specific courses of action to achieve particular desires. The plans' library describes the agent's concrete actions to reach its goals.

Differently to the classical BDI approach, in the proposed model, the supervisor agent manages three kinds of information coming from three different sources: direct messages exchanged with primary agents of the HCII monitored by the supervisor agent, individual perceptions coming from its sensors, and finally stigmergic events triggered by supervisor agents belonging to interdependent HCIIs. Moreover, the traditional practical reasoning is extended with a context-analysis module. Indeed, the common practical reasoning of BDI agents consists of two main activities: Goal Deliberation and Means-ends reasoning. Deliberation is concerned with determining what goals to pursue among several goals. In contrast, Means-ends reasoning allows the supervisor agent to determine how the goals can be achieved (thinking about suitable actions and resources) by choosing appropriate plans. In our model, we enable supervisor agents to develop situational awareness that improves the deliberation phase leading to a better decision-making process. Supervisor agents have context-aware capabilities to identify the nature of the problem from the environment, classify the contextual knowledge based on its belief set, and provide a set of options to be chosen. The supervisor agent determines the new situation by revising its belief set and selects the execution plan to attain its goal.

3.4. Supervisor Agent Reasoning Cycle

The reasoning cycle of the supervisor agent is essentially composed of three main phases (see Algorithm1), i.e., sensing, deliberation and acting phase, along with an initialization phase. During the sensing phase, a supervisory agent collects information by sensing the environment through direct communications with the primary agents and stigmergic communications with other supervisor agents belonging to the interdependent HCII. The supervisor agent uses these perceptions to update its knowledge. A supervisor agent's deliberation and acting phases are more demanding than the ones of a primary agent. Primary agents are lightweight agents with just a few goals and plans. Conversely, supervisory agents can exhibit more complex behaviour due to the several tasks they are engaged in (such as learning from the environment, collective intelligence decisions, risk mitigation and incident handling, etc.). Moreover, supervisory agents' plans are triggered not only by a single event but by a more complex situation it can infer from events. Thus, supervisory agents must apply rules for situation recognition to invoke a plan. The agent observes its environment detecting new events within the primary control loop. If the supervisor agent receives a message, it updates its knowledge base with the message's content and sender. If the event is a perception, the supervisor agent updates its belief base with the object of the perception (i.e., the percept). Finally, a supervisor agent may also perceive

a stigmergic event produced by a stigmergic communication of other supervisor agents. In this case, the belief base is updated with the outcome of stigmergic communication (e.g., STIX objects [2]). In order to start the deliberation process, the supervisor agent needs to understand the situation determined by the current knowledge. According to the new context, supervisor agents may reconsider their current intention. They will sort the set of 'suitable' intentions based on an evaluation function that will generate a ranking among the intentions, thus pursuing the one with the highest score. For example, the supervisor agent may suspend its current task to manage a more critical situation due to a high-level attack. Hence, the appropriate plan according to the new context is selected. If the supervisor's intention does not change during the action execution, it simply picks off each action from its plan and executes it until the plan is completed or the goal is fulfilled. Conversely, suppose after executing an action, the supervisor agent, observing its environment, perceives some beliefs that change its current intention. In that case, it drops to pursue the new intention and to return to continue the previous plan if all intentions are not reached.

Algorithm 1: Supervisor Agent Reasoning Cycle

Data: Instantiated model of Supervisory Agent
$< Sup\_Ag, B_0, D, I_0, Plans >\leftarrow$ Supervisory Agent;
$I_0 \leftarrow Monitoring\_HCII$;
`// Agent Initialization`
$R \leftarrow setInitialRules(R_0 \subset B_0)$;
$B \leftarrow setInitialBeliefs(B_0)$;
$I \leftarrow setInitialIntentions(I_0)$;
while *true* **do**
  `// Sensing`
  $\omega \leftarrow getEnvEvent()$;
  if $\omega \subset$ *a received message* Msg **then**
    $Msg_{content} \leftarrow$ getContent(Msg);
    $Msg_{source} \leftarrow$ getSource(Msg);
    $B' \leftarrow (Msg_{content} \wedge Msg_{source})$;
    $B \leftarrow update(B, B')$;
  if $\omega \subset$ *a perception event* **then**
    $\rho \leftarrow getPercept(\omega)$;
    $B \leftarrow update(B, \rho)$;
  if $\omega \subset$ *a stigmergic event* **then**
    $\sigma \leftarrow getStigmergicOutcome(\omega)$;
    $B \leftarrow update(B, \sigma)$;
  `// Deliberation`
  $Context \leftarrow understand\_Situation(B, R_0)$;
  if $reconsider(I, Context)$ **then**
    $D \leftarrow options(Context, I)$;
    $I \leftarrow evaluate(Context, D, I)$;
  `// Plan selection`
  $\pi \leftarrow selectPlan(Context, I, Plans)$;
  if $\neg achieved(I, B) \wedge \pi \neq \varnothing$ **then**
    $act \leftarrow head(\pi)$;
    $execute(act)$;
    $\pi \leftarrow tail(\pi)$;

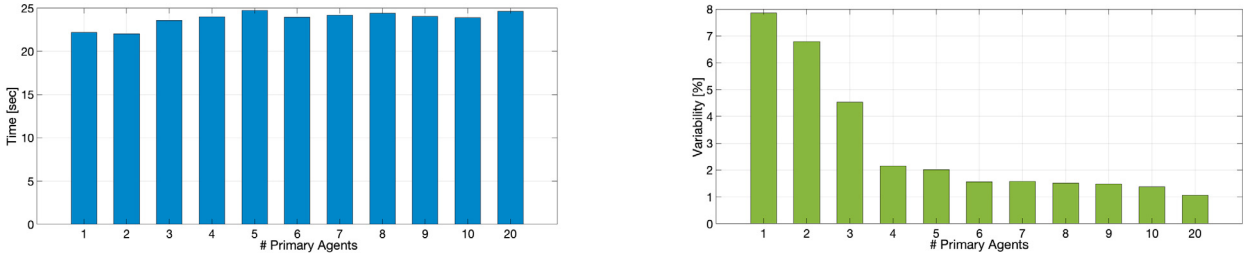
3.5. Preliminary evaluation

This section aims to evaluate the suitability of the proposed model for highly distributed and interconnected healthcare ecosystems. Please note that the model performance in terms of attack detection is beyond the scope of this study as it depends on the algorithm adopted by the agents discussed in [13].

The preliminary evaluation has been performed by considering three critical quality attributes for dealing with the healthcare ecosystem's security: Responsiveness, Robustness and Scalability. Regarding the first one, timely response is an essential requirement for protecting healthcare data and services in a healthcare scenario. We evaluated responsiveness by considering the time taken by a supervisor agent to get a response to several contemporary primary agents' requests. Regarding the second quality attribute, it is worth noting that several attacks can be performed on different assets of the same HCII simultaneously, producing numerous communications between primary and supervisor agents. Robustness measures the capacity of the model to manage several attacks in terms of agent communication failures. Finally, *Scalability* is the ability of the model to perform efficiently with healthcare organizations with large numbers of assets to be monitored.

In order to evaluate such quality attributes, we simulated a healthcare environment where several cyber-security attacks were simultaneously performed on different IoT devices that are interconnected for delivering a healthcare service (e.g. attacks to guess user credentials and to change devices configuration file). The model was implemented in Jason [5], an interpreter for an extended version of AgentSpeak, the most widely adopted BDI language. Several tests have been executed by increasing the number of primary agents controlled by a supervisor agent within the healthcare environment. Fig.3a reports the average times a supervisor agent takes to complete its reasoning cycle and get a response for security requests from primary agents. As we can see, despite the number of agents that simultaneously make requests to the supervisor agent increases, the time to response increases only by two seconds with four agents, and it remains almost stable with more agents. Moreover, the variation coefficient reported in fig.3b gives evidence that the model can ensure timely responses to several agents with a slight variation. In addition, by increasing the number of primary agents, we can see that the variation coefficient is very similar, ensuring that although the requests increase, the responses are provided within the same time interval. It is worth noting that the variation coefficient when adopting less than four agents is higher than the case with more agents because of fixed working time that gives more influence with fewer agents.

Regarding the scalability, we also stressed the system by considering an HCII area with a high number of assets requiring 20 primary agents. In such a case, we can also see that the system works properly, the significant communication flow does not create a bottleneck, and the response time is slightly increased compared to the case with 10 primary agents. Finally, as concerns the robustness, in this preliminary evaluation, by engaging 20 agents, no communication failures occurred.



(a) Response Times

(b) Normalized Variation Coefficient.

Fig. 3: Experimental results.

4. Conclusion

This paper proposes a swarm intelligence model for tackling the propagation of attacks inside interconnected healthcare organizations and ensuring the whole healthcare ecosystem's security and resilience. Although Swarm Intelligence approaches have received considerable attention in the context of cybersecurity, the works proposed in the literature focus on solving specific security problems; on the contrary, in this paper, the integration of multi agent system and SI is proposed as a scalable and lightweight model for the healthcare sector security and resilience. The proposed agent-based SI model utilizes multiple agents to achieve different security requirements depending on the healthcare detection component by adopting swarm intelligence mechanisms such as stigmergy. In particular, the hierarchical monitoring through primary and supervisor agents provides local and global knowledge about the attack. Indeed, for a HCII, primary agents are responsible for local monitoring of the lower-level healthcare assets. On the contrary, supervisor agents are responsible for global monitoring of the whole HCII. Primary Agents deal with issues on a local level and communicate directly with supervisor agents regarding asset states. Supervisor agents deal

with issues on an HCII level and, by adopting an indirect communication structure founded on the swarm intelligence paradigm, contribute to the overall resilience of the interconnected HCII of the whole healthcare ecosystem. The distributed collaboration among heterogeneous agents within and across interdependent Health Care Information Infrastructure contributes to better incident detection and prevention through threat knowledge sharing. Moreover, the proposed extension of supervisor agent reasoning with situational awareness allows for a better understanding of the environment and the cybersecurity threats and vulnerabilities and anticipating the potential consequences. Awareness enables supervisor agents to get a real-time view of cyber threats and respond appropriately to a security event.

Preliminary evaluation gives evidence about the proposed model's robustness, scalability and timely response.

Currently, we are working to implement the model into a real healthcare scenario. We are also focusing on the development of SI based platform for the healthcare sector.

Acknowledgements

This work was partially supported by the AI4HEALTHSEC EU project, funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273.

References

[1] Aghdam, M.H., Kabiri, P., et al., 2016. Feature selection for intrusion detection system using ant colony optimization. Int. J. Netw. Secur. 18.
[2] Barnum, S., 2012. Standardizing cyber threat intelligence information with the structured threat information expression (stix). Mitre Corp. 11.
[3] Bell, G., Ebert, M., 2015. Health care and cyber security: increasing threats require increased capabilities. KPMG .
[4] Bonabeau, E., Theraulaz, G., Dorigo, M., Theraulaz, G., Marco, D.d.R.D.F., et al., 1999. Swarm intelligence: from natural to artificial systems. 1, Oxford university press.
[5] Bordini, R.H., Hübner, J.F., Wooldridge, M., 2007. Programming multi-agent systems in AgentSpeak using Jason. John Wiley & Sons.
[6] Boughaci, D., Kadi, M.D.E., Kada, M., 2012. Fuzzy particle swarm optimization for intrusion detection, in: International Conference on Neural Information Processing, Springer. pp. 541–548.
[7] Bratman, M., 1987. Intentions, plans, and practical reason. csli publication.
[8] Duan, J., Zhu, Y.a., Huang, S., 2012. Stigmergy agent and swarm-intelligence-based multi-agent system, in: Proceedings of the 10th World Congress on Intelligent Control and Automation, IEEE. pp. 720–724.
[9] Enache, A.C., Patriciu, V.V., 2014. Intrusions detection based on support vector machine optimized with swarm intelligence, in: 2014 IEEE 9th IEEE international symposium on applied computational intelligence and informatics (SACI), IEEE. pp. 153–158.
[10] Georgeff, M., Pell, B., Pollack, M., Tambe, M., Wooldridge, M., 1998. The belief-desire-intention model of agency, in: International workshop on agent theories, architectures, and languages, Springer. pp. 1–10.
[11] Heylighen, F., 2016. Stigmergy as a universal coordination mechanism i: Definition and components. Cognitive Systems Research 38, 4–13.
[12] Ilie, S., Bădică, C., 2013. Multi-agent distributed framework for swarm intelligence. Procedia Computer Science 18, 611–620.
[13] Islam, S., Papastergiou, S., Kalogeraki, E.M., Kioskli, K., 2022. Cyberattack path generation and prioritisation for securing healthcare systems. Applied Sciences 12, 4443.
[14] Islam, S., Papastergiou, S., Mouratidis, H., 2021. A dynamic cyber security situational awareness framework for healthcare ict infrastructures, in: 25th Pan-Hellenic Conference on Informatics, pp. 334–339.
[15] Kolias, C., Kolias, V., Kambourakis, G., 2017. Termid: A distributed swarm intelligence-based approach for wireless intrusion detection. International Journal of Information Security 16, 401–416.
[16] Lima, M.F., Sampaio, L.D., Zarpelao, B.B., Rodrigues, J.J., Abrao, T., Proença, M.L., 2010. Networking anomaly detection using dsns and particle swarm optimization with re-clustering, in: 2010 IEEE global telecommunications conference GLOBECOM 2010, IEEE. pp. 1–6.
[17] Lugo-Cordero, H.M., Guha, R.K., 2013. What defines an intruder? an intelligent approach, in: 2013 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), IEEE. pp. 31–36.
[18] Malik, A.J., Shahzad, W., Khan, F.A., 2011. Binary pso and random forests algorithm for probe attacks detection in a network, in: 2011 IEEE Congress of Evolutionary Computation (CEC), IEEE. pp. 662–668.
[19] Mishra, S., Sagban, R., Yakoob, A., Gandhi, N., 2021. Swarm intelligence in anomaly detection systems: an overview. International Journal of Computers and Applications 43, 109–118.
[20] Nasir, M.H., Khan, S.A., Khan, M.M., Fatima, M., 2022. Swarm intelligence inspired intrusion detection systems—a systematic literature review. Computer Networks , 108708.
[21] Ponemon, I., 2016. Sixth annual benchmark study on privacy & security of healthcare data. Technical Report. Technical report.
[22] Salmen, F., Hernandes, P., Carvalho, L., Proenca, M., 2015. Using firefly and genetic metaheuristics for anomaly detection based on network flows, in: AICT: The Eleventh Advanced International Conference on Telecommunications.
[23] Shi, Y., Li, H., Bao, J., Yan, Z., Jiang, S., 2011. Research on the improved svm model for intrusion detection of transportation information security systems, in: 2011 Third Pacific-Asia Conference on Circuits, Communications and System (PACCS), IEEE. pp. 1–3.
[24] Shokoohsaljooghi, A., Mirvaziri, H., 2020. Performance improvement of intrusion detection system using neural networks and particle swarm optimization algorithms. International Journal of Information Technology 12, 849–860.
[25] Weiss, G., 1999. Multiagent systems: a modern approach to distributed artificial intelligence. MIT press.