Security Enhancement during Agents Communication in GNA Approach

Khudhair Abbas Mohammed
Mazlina Abdul Majid
Faculty of Computer Systems & Software Engineering,
University Malaysia Pahang,
26300 Kuantan, Pahang,
Malaysia

Mohd Sharifuddin Ahmad
College of Computer Science and Information Technology,
Universiti Tenaga Nasional,
43000 Kajang, Selangor, Malaysia

***Abstract*—In many dynamic environments, where humans and agents coexist, agents cooperate for internal and external resources to achieve their goals. Consequently, the agents are exposed to the risk of being attacked by malicious agents. Such situation, if not mitigated, risks the entire model and threatens its long-term performances. Due to uncertainties of an agent and its potential behavior, especially in human-agent collaboration systems, an agent might behave fraudulently to its partners (humans or agents). Therefore, security is a crucial aspect in the initial development of a collaborative human-agent system. However, many research envisages the security aspects only in the implementation stage. At this stage, a security model is strictly formulated based on the techniques and constraints among agents. Over the past decade, many researchers propose various security models with outstanding features. However, despite the features of the proposed security models, there is still a lack of research effort in security aspects for multi-agent systems, which is considered as a critical challenge. In this paper, we attempt to enhance the Generic Nodal Abstraction (GNA) approach with a security model applied among agents in their communication. The enhancements include authentication, message encryption and interaction constraints.**

Keywords—Security; human agent collaboration; malicious agent.

I. INTRODUCTION

Multi-agent systems (MAS) prevail in several areas of applications such as financial systems, industrial engineering, e-commerce, e-health, computer games, and many others [1] [2]. Unfortunately, many heterogeneous systems, in which MAS are applied, are unsafe and unreliable. In such systems, agents could be harmed via external accesses, which could compromise the data and information of the entire system. Therefore, security issues need to be properly and adequately addressed before multi-agent systems can be a viable solution for a wide range of applications. Specifically, collaborations involving humans and agents are jeopardized by attackers and criminals with malicious intents, consequently, causing financial losses and ruins to organizations' reputations and images.

Due to agents' decentralized and distributed architecture, global attackers with malicious intent yield negative consequences for the entire system. They may attack with different sly plans such as the man in the middle, replay attacks, modification and masquerade. In fact, integrating MAS with secure and safe techniques presents a prominent obstacle for researchers [3]. Consequently, several studies have been conducted by researchers proposing different methods to enhance MAS with security models. Authentication, confidentiality, and authorization are considered as the fundamental security systems requirements that should be implemented. Nevertheless, a number of research provides methods and techniques for constructing security models for multi-agent systems.

Ignoring security in collaborative systems increases the opportunities for criminals to expose its information, which is a crucial material for the collaborative system. Hackers exploit the system vulnerabilities to attack and harm its sensitive information. The level of attack becomes much risker in an open system especially when humans are involved [4]. Due to the architecture of Generic Nodal Abstraction (GNA) approach and the combination of human and agent, the level of attack would increase, which requires several phases of security as an imperative factor in the development lifecycle. Any weaknesses in these phases would open the gate for malicious users to access and steal sensitive information and use the GNA against the owners and users. Such risks cause serious damage to the GNA via affecting both sides of human and agents and threaten their availability of work.

Security issue in many software systems have been given a prominent attention due to the severe impacts on humans' organizations, including e-commerce, governmental, military, financial, health, telecom, and transport sectors [5]. Since security are not considered during the development process, a large number of these systems, unfortunately, remain susceptible and have vulnerabilities to attacks. Basically, there have only been few integrations made to enhance security aspect within the development stages of methodologies. Hence, a prime point in developing such aspects in our GNA approach is to reduce vulnerabilities, which are usually the results of

978-1-5386-7856-5/18/$31.00 ©2018 IEEE

defective design specifications, development process and implementation.

This paper proposes a security model for a GNA approach in agents' communications. The models are also discussed according to their features to enhance collaborative systems. The paper is structured as follows: Section 2 reviews the literature on security models and provides a comparison of different models. Section 3 shows the GNA approach presentation, Section 4 discusses security model integrated in the GNA stages and Section 5 summarizes and concludes the paper.

II. RELATED WORKS

Several attempts have been made to identify vulnerabilities in Multi-Agent Systems (MAS). Security in computing is a platform that provides solutions, which can contribute to resolving these vulnerabilities. Consequently, it is critical and important to protect data from tampering or hacking by malicious actions. The term computer security does not have a unique definition by researchers. Security in MAS is quite susceptible to threats compared with other systems that make use of centralized performance. Many components of MAS are decentralized and deployed in different areas [6]. Hence, it is essential to promote multi-agent systems deployed with security aspects.

Researchers have proposed diverse techniques and methods to ensure that multi-agent systems are safe from attackers. Yue et al. propose a security model to prevent a Colluded Truncation Attack, which focuses on a sent message and modifies it. This attack comprises of two malicious agents, which connect to a sender agent and conspire to change its message [7]. Becker [8] presents another technique which provides an inference system. The inference system tells the users about a malignant part that the whole system detects. Even though his system establishment is not for MAS, it applies to keeping MAS safe from malevolent parts. Backer provides his framework based on the secrecy of policy language analysis.

Rashvand et al. [9]made an overview of distributed security for MAS applications in different domains including military applications, e-business, e-commerce, e-health, network management, etc. Through a thorough scan of various domain literatures as the authors discuss the sophisticated progress followed by some observations, inferences and remarks for the researchers in the areas. Rashvand et al. [9] is a review into secure MAS, where it is an aim to seek new solutions for securing the general purpose MAS applications and security MAS, as a new overlay Security solution in which we propose distributed security models, to adopt MAS approach for securing distributed systems.

The security of multi-agent frameworks is an intriguing and vital issue. Multi-agent frameworks, similar to all vast scale spatially dispersed frameworks, are helpless against digital/cyber assaults in view of the improvement of system data and correspondence advancements. Ordinarily, there are two diverse attack situations in a multi-agent framework: assault on the changing conduct (or closed-circle flow) of the agents and attacks on the interchanges among the operators (humans and agents alike) (Feng, Hu, and Wen, 2016). These intrusions can significantly influence the accord features of the entire group of agents. In reality, a solitary agent whose deficiency in communicating to its fellow can cause the collapse of the whole system resulting in cascading damages. Clark et al. propose a framework for a particular Service Level Agreement (SLA) that involves methods to dynamically protect and maintain reliable violation monitoring policies. Clark uses a Web service for an SLA specification which he implements in AgentScape [10]. The reason for utilizing the Web services is to test and establish an agreement among participants in a centralized and decentralized monitoring. Clark framework offers usefulness of results with its use in decentralized systems.

Nowadays, many devices that use networks in joining and sharing data need smart utilization to prevail safely in several areas. Definitely, security perspective considers a smarter utilization due to software vulnerabilities that cause huge problems (e.g., e-commerce field). Security applications continuously improve systems' devices to be immune to data theft, invasion detection, fire detection, personal health protection, etc. Nevertheless, there are deficiencies in fully securing network devices and equipping them with flexibility to serve users. Therefore, several systems to enhance and construct security services by providing monitoring sensors, controlling parameters, and robots are proposals currently in motion. Moradian et al. in the paper entitled “Security of E- Commerce Software Systems” suggest using intelligent agents to develop business processes. The authors show the facilitation, implementation, and design of the agent technology to support engineers during the development process. The proposed system enacts various security services in an e-commerce system, which assist engineers to monitor decisions and activities; search for security measures and mechanisms; perform checks; and provide advice and feedbacks [11].

III. WHAT IS GENERIC NODAL ASTRACTION (GNA)?

The GNA approach operates based on collaborative nodes which consist of a model of a human's job position within an organization, a mediator agent, workflow, and resources. The collaborative nodes enactment architecture realizes the human position and its functions. Each function is modelled as an action with which a mediator agent, assisted by an agent or more, performs to support their human counterpart in cooperative processes (see Figure 1). Basically, the GNA approach is a model, established to expand the work done in 2012 [12] and claimed to be applicable in generic domains. The model is framed by nodal abstractions that are considered as intelligent entities that comprise of a human with agent(s) collaborated via a mediator agent.

In Node 1 of the figure, ϕ represents a human's set of functions and λ represents an agent's set of functions. Node 1 shows a human with only one assistant agent via a mediator agent, presumably to handle all the mundane tasks of its human counterpart. In Node 2, the human is assisted by three agents, the number of agents are selected according to the node mediator agent which handles one or more specific tasks forits human counterpart.

Even though the GNA provides flexible features between human and agents, and between agents the GNA approach still has some drawbacks and lacks security aspects. Additionally, the overall model vulnerability to several security attacks are deemed a prominent challenge. Thus, a security model is presented to integrate the GNA approach and increase the reliability and efficiency among its agents.

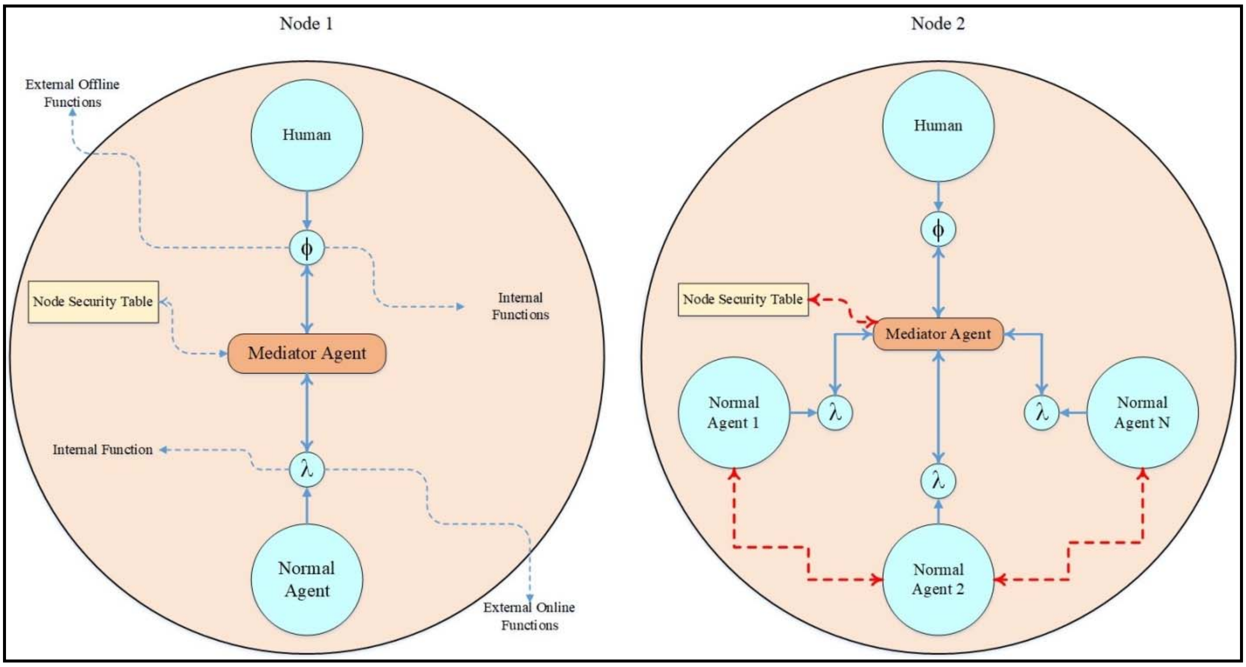


Figure 1 GNA concept

IV. SECURITY MODEL FOR GNA

Multi-agent systems are widely used in complex applications such as industrial, commercial, governmental, military, entertainment and healthcare applications. Each agent has special abilities to perform tasks and it is specialized with certain capabilities to assist humans in their daily work. An agent is beneficial to humans when the agent assists to reduce the task's complexity. In many circumstances, interfaces are provided to handle communication and tasks' exchanges between humans and agents. Agents are currently applied in both small applications, such as email filters and personal assistants, as well as open and complex applications, such as air traffic control, military demining, logistic planning, financial portfolio management, among others [13].

However, in order to develop multi-agent systems that use the Internet as a medium to interconnect the agents, security aspects should be implemented. MAS relies on collaboration between humans and agents, which makes it vulnerable to interact with strangers. Systems in heterogeneous environments in which agents reside are open to security threats. A multi-agent system is similar to other systems when using the network, threaten by malicious actions and other security problems. The security problems in these environments, which must not be neglected, include malicious actions, blocking of resources, breach of information integrity, and breach of private data.

Additionally, there are several vulnerabilities of MAS when connected to an open-network [14]. Malicious entities in the environment of open-network may cause problems by rendering agents to misbehave or vulnerable to attack. By exploiting an agent's social ability, these entities applied in heterogeneous systems could force the agent to misbehave and redirect its result to the attackers' destination.

One of the techniques that attackers use to deceive is to use a masquerade agent that acts similarly to a real agent in a certain environment and steal valuable data and perform malicious actions. Attackers can also persuade an agent to perform mischievous tasks by taking data that belongs to other agents. For example, in financial systems, in which MAS are used to support team decision-making, such systems may be inheritably unsafe. Such systems demonstrate failures to resolve security problems when a huge amount of data or online banking transactions are wrongly transferred by attackers. Furthermore, numerous insecure actions may occur and put the organization in a serious danger. In order to avoid these security threats, organizations (such as healthcare administration and e-business) that depend on MAS, must install and deploy security systems within their software systems.

Consequently, a strong and robust mechanism with which agents in our model (GNA) can secure and defend themselves against attackers from other agents and/or humans needs to be developed and integrated. Figure 2 depicts the general architecture of the security sub-model for the GNA. The main node creates the user name and initial password for the human node. Moreover, the security properties such as authentication, integration, cryptography, and interaction constraints are applied between the sub-nodes.

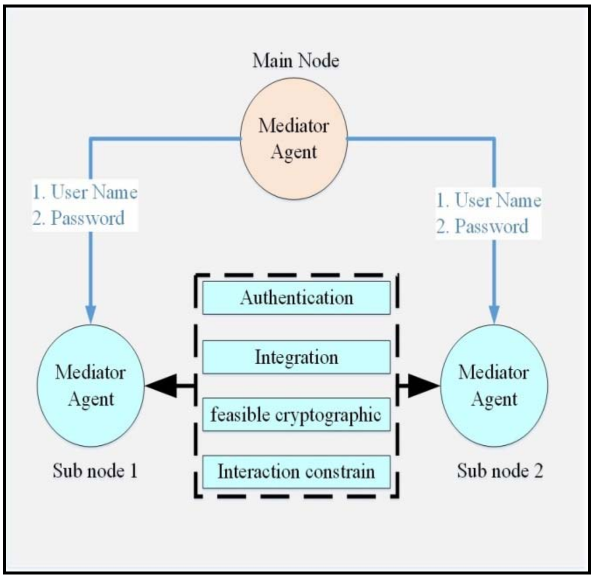
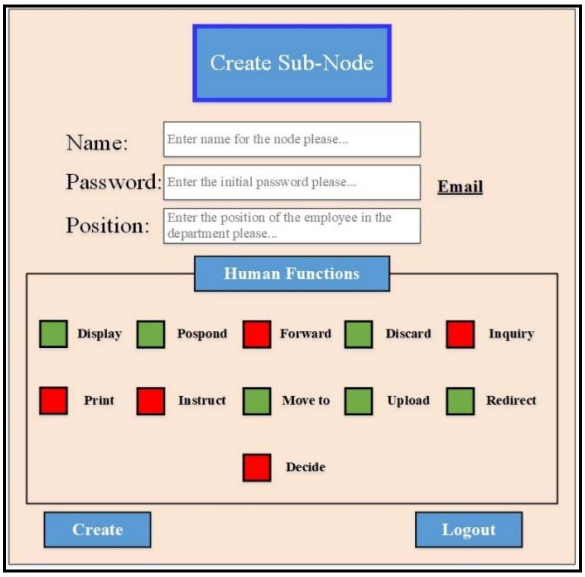


Figure 2 Security sub-model architecture for the GNA

Basically, the number of agents is restricted according to the assignment by the mediator agent and the delegated tasks that must be performed. The GNA is enhanced with security node authentication (Username and Password) for each node in the system. The main node has a table in its database that saves all the registered nodes with specific name and initial password. Additionally, a security table stores all the information about the nodes that include: Node name, Agent ID and a secret key, which play a role of verification and authentication when node interactions occur. Furthermore, a secure message exchange is another aim of our security sub-model, with which the agent in a certain node is able to implement a feasible cryptographic solution between nodes. Eventually, we restrict the interaction time and number between the nodes so that the nodes of the GNA are protected. The following points elaborate the security sub-model properties for the GNA nodes:

A. Node user name and password

When the internet service is provided, multi-agent system capabilities expanded because of the availability of wide area networks. Furthermore, agents in several systems are deployed to assist its human counterpart and improve the choice for establishing complex and collaborative applications. Agents and humans in distributed systems always collaborate in utilizing the data, information, and resources for tasks performances. These distribution and collaboration offer significant benefits, improve the work process, and share expertise. However, during these distribution and collaboration providing security of user name and password must be given high priority before any interaction occurs. Consequently, we integrate the GNA nodes with specific user name and password for each node in order to secure and protect them. Figure 3 illustrates a created sub-node which deploys private name and password. The created name and password are sent through the email to the representative human sub-node.



Name: Enter name for the node please...

Password: Enter the initial password please...

Position: Enter the position of the employee in the department please...

Human Functions

🟩 Display 🟩 Pospond 🟥 Forward 🟩 Discard 🟥 Inquiry

🟥 Print 🟥 Instruct 🟩 Move to 🟩 Upload 🟩 Redirect

🟥 Decide

Figure 3 Node user name and password

This property is a prime objective for the sub-nodes which is created by the main node in the system domain. When security exist, it eradicates impersonation of users by providing each node with a user name and password. Ensuing a successful login of the sub-node, the mediator agent of the main node is notified that a sub-node "N" is successfully registered, where N refers to the node's name. Creating strong user name and password mechanism is a significant requirement but need the high subtlety. It is important that each node of the GNA prevent soft authentication from being regenerated.

B. Message Encryption between nodes

Threats and attacks in multi-agent systems are widely spread and need to be remedied. Since the GNA utilizes MASs which are gradually implemented in many distributed nodes, it is imperative to establish confidentiality that implements a comprehensive protection and provides a solid security for the proposed model. For instance, the GNA data and information is considered a prime part and protecting them is highly recommended. The threats and attacks constitutes serious risks for the whole information of the GNA. Subsequently, the security aspect is extremely fundamental and should be integrated in the methodology phases of the GNA to defend the system against threats and attacks. Figure 4 illustrates the mechanism in which nodes are sending a secret message where a secret key is applied as well.

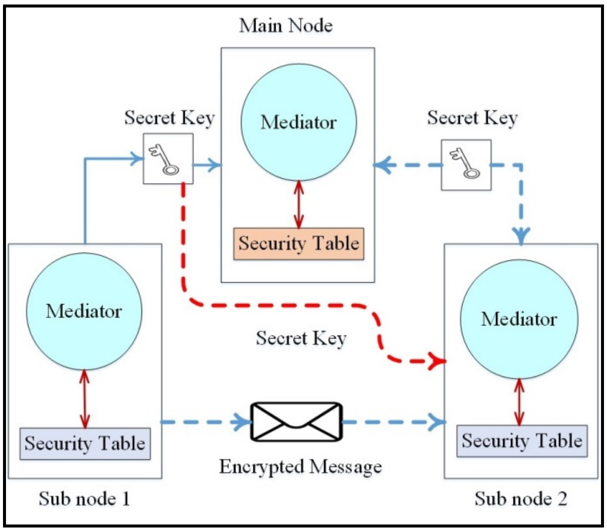


Figure 4 node secret message mechanism

The security sub-model for the GNA depicted in Figure 4 shows the secret message exchange between its nodes. Specifically, when sub-node 1 sends a secret message to sub-node 2 two scenarios occur before sub-node 2 is able open and read it. Firstly, sub-node 1 sends an encrypted message and to sub-node 2. Simultaneously, sub-node 1 also sends a random secret key to both sub-node 2 and the main node to be authenticated latter by sub-node 2. Note that, a sub-node means practically the mediator agent inside each node which has the capabilities and authorities to check and retrieve the information from the security table. Consequently, sub-node 2 need to send authentication to the main node including the sender's sub-node id and its secret key. The main node checks this information whether the secret key of sub-node 2 and sub-node 1 are matched, if so then an authentication is sent to sub-node 2 and now it is able to open and decrypt the received message.

C. Interaction constraints

During nodes' interactions in the system, agents communicate to execute their delegated tasks. Consequently, the behaviour of the agents in the node might change or attacked via a malicious agent. While the GNA nodes are collaborating with various other nodes' hosts in order to solve, assist, or reply to each other, a severe denial of service can occur via the malicious agent and then cause crucial problems to all the GNA nodes. Subsequently, the performance of the GNA nodes can be degraded and their code, data or information are disrupted.

To protect the GNA nodes from these types of attacks, the interactions between nodes have to be controlled and restricted with some constraints. The GNA environment identifies entities that constitute the components of a node (human, mediator agent, and normal agents). However, when the elements of the GNA model are interacting, they can neither implement interaction constraints on communication between nodes nor protect the model from denial of service. Thus, we establish a security sub-model that specifies the interaction constraints between nodes. This sub-model presents a set of properties and preferences that provides the privileges for nodes when interactions occur between them. The following sub-sections discuss the integrated security sub-model interaction constraints.

1) *Restricted time of interactions between nodes:*

This property is implemented via the mediator agent of the nodes, which provides the maximum time allowed (MaxTiAl) to a number of nodes (sender and receiver nodes) to collaborate with each other. This property assures availability by avoiding any denial of service. This restriction eliminates attacks from disgraceful behaviour and guarantees system reliability. Furthermore, the GNA receiver node guarantees that the sender node does not exploit more than the time of interaction being allowed.

2) *Restricted number of interactions between nodes:*

This property is also implemented via the mediator agent of the nodes, which stipulates the maximum number of interactions (MaxNoTAl) assigned to various nodes to collaborate with each other. This property guarantees availability by eliminating the denial of service. This restriction eliminates attacks from disgraceful behaviour and guarantees system reliability. Moreover, the GNA receiver node depends on the sender node not to exceed more than the number of interactions being allowed.

Figure 5 illustrates the nodes' interaction constraints in which collaboration, negotiation, and communication are allowed. When the mediator agent in a sender node wants to collaborate with another node (a receiver node), interaction constraints have to be specified via its human counterpart. The interaction constraints are identified via TNT authorized, which defines the maximum time and the number of times a sender is authorized to communicate with another node.

For example, the offline modes between the human operator nodes include phone calls, SMS, or discussions after they agree upon the interaction constraints (TNT authorized), sent to their mediator agents. To verify the sender node's confidentiality, the sender node should carry out the same number of interaction constraints that the receiver node obtained for its human counterpart.

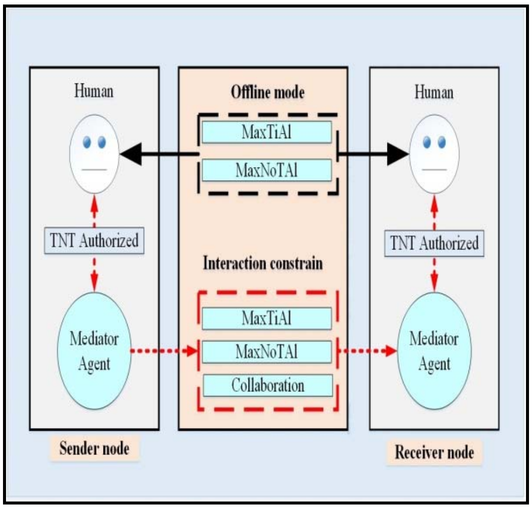


Figure 5 Nodes interaction constraints

Furthermore, the interaction constraints extend the GNA nodes security during their collaboration. The nodes are totally protected via identifying the maximum time allowed and maximum number of interactions allowed for collaboration, negotiation and communication. These restrictions secure the nodes and arrange the maximum time and number of interactions that the sender node should respect. In oursecurity sub-model, the interaction and collaboration between the nodes are stopped and refused if only if the time and number interactions from the sender node have exceeded their limited and predefined interaction constraints. Thus, such nodes are deduced and considered as fraudulent nodes. Subsequently, the GNA nodes are secured and safe from attacks by external entities.

V. CONCLUSIONS AND FUTURE WORK

This paper presents the security for the Generic Nodal Abstraction (GNA) approach that are built based on human and mediator agent with several normal agents' systems. The security mechanism that we have introduced attempts to integrate the GNA approach and assure to guarantee the system's functionality. The proposed model prevents attacks on the GNA and categorizes the kinds of threats for possible avoidance and protection. The integration of security model extends the confidentiality and effectiveness of the GNA.

In our future work, we shall attempt to test the integrated model in a simulation system involving two or more nodes.

ACKNOWLEDGEMENTS

This study is supported and financed under Postgraduate Research Scheme Grand (PGRS 160319) from University Malaysia Pahang (UMP).

REFERENCES

[1] W. S. Cheah, A. Bujang, E. M. Masli, and A. A. Halin, "Improved Two-Ways Classification for Agent Patterns," *Int. J. Softw. Eng. Comput. Syst.,* vol. 1, p. 53, 2010.

[2] M. Furmankiewicz, A. Sołtysik-Piorunkiewicz, and P. Ziuziański, "Artificial Intelligence and Multi-agent software for e-health Knowledge Management System," *Informatyka Ekonomiczna,* vol. 2, p. 32, 2014.

[3] Y. Hedin and E. Moradian, "Security in Multi-Agent Systems," *Procedia Computer Science,* vol. 60, pp. 1604-1612, 2015.

[4] S. Bijani and D. Robertson, "A review of attacks and security approaches in open multi-agent systems," *Artificial Intelligence Review,* vol. 42, pp. 607-636, 2014.

[5] N. H. A. Hamid, M. S. Ahmad, A. Ahmad, A. Mustapha, M. A. Mahmoud, and M. Z. M. Yusoff, "Trusting Norms: A Conceptual Norms' Trust Framework for Norms Adoption in Open Normative Multi-agent Systems," in *Distributed Computing and Artificial Intelligence, 12th International Conference*, 2015, pp. 149-157.

[6] F. D. Ahmed, M. A. Majid, M. Sharifuddin, and A. N. Jaber, "Software agent and cloud computing: A brief review," *Int. J. Softw. Eng. Comput. Syst.,* vol. 2, pp. 108-113, 2016.

[7] X. Yue, X. Qiu, Y. Ji, and C. Zhang, "P2P attack taxonomy and relationship analysis," in *2009 11th International Conference on Advanced Communication Technology*, 2009, pp. 1207-1210.

[8] C. Becker-Asano and I. Wachsmuth, "Affective computing with primary and secondary emotions in a virtual human," *Autonomous Agents and Multi-Agent Systems,* vol. 20, p. 32, 2010.

[9] H. F. Rashvand, K. Salah, J. M. A. Calero, and L. Harn, "Distributed security for multi-agent systems–review and applications," *IET information security,* vol. 4, pp. 188-201, 2010.

[10] K. P. Clark, M. Warnier, F. M. Brazier, and T. B. Quillinan, "Secure monitoring of service level agreements," in *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*, 2010, pp. 454-461.

[11] E. Moradian, "Security of E-Commerce Software Systems," in *Agent and Multi-Agent Systems in Distributed Systems - Digital Economy and E-Commerce*, A. Hakansson and R. Hartung, Eds., ed Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 95-103.

[12] K. A. Mohammed, M. S. Ahmad, S. A. Mostafa, and F. Sharifuddin, "A Nodal Approach to Modeling Human-Agents Collaboration," *International Journal of Computer Applications, Foundation of Computer Science,* vol. 43, pp. 33-40, 2012.

[13] D.-H. Shih, H.-S. Chiang, D. C. Yen, and S.-C. Huang, "An intelligent embedded system for malicious email filtering," *Computer Standards & Interfaces,* vol. 35, pp. 557-565, 9// 2013.

[14] S. Adameit, T. Betz, L. Cabac, F. Hars, M. Hewelt, M. Köhler-Bußmeier, *et al.*, "Modelling Distributed Network Security in a Petri Net- and Agent-Based Approach," in *Multiagent System Technologies: 8th German Conference, MATES 2010, Leipzig, Germany, September 27-29, 2010. Proceedings*, J. Dix and C. Witteveen, Eds., ed Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 209-220.