Journal of AL-Qadisiyah for computer science and mathematics Vol.9 No.2 Year 2017
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

Comp Page 131 - 142 Dhyaa .S /Sinan .A

Design of Intelligent Agent Based management security system for E-government

Dhyaa Shaheed Al-Azzawy **Sinan Adnan Diwan**

College of Computer Sciences and Information Technology
Wasit University
dalazzawi@uowasit.edu.iq

Recived : 18\10\2017 **Revised : //** **Accepted : \?\2017**

Abstract :

E-Government delivers services into inhabitant electronically, action, and another government existence. This is analogous to document centric approach in traditional service delivery by the government. One of the most crucial factor regarding the reliability of government services is the security factor, which eventually leads to the social acceptance and satisfaction. E-Government is now a day is the response to the rapid development in the information technology especially in the automation of the process of service delivery. The model introduced by this paper is built over the social behavior of entities that shares the knowledge and provides decision-making baselines. Each entity is capturing its own knowledge and crystalize it with other entities within the communities. In this paper JAVA Agents where built to represent the individuals, which are attached to certain interaction points, for example each intelligent agent is attached to a web site representing the source of knowledge and behavior capture. Results proven that the social behavior of the software intelligent agent is a huge potential toward establishing social acceptance due to the smart behavior in collecting information regarding the utilization of the service, Three sites have been built along the implementation of paper to pursue its hypothesis; this is to represent government web sites deliver certain services and over which an intelligent agent is attached to capture the behavior of users and later on broadcast captured knowledge to other agents (i.e., the community is composed of four agents). The knowledge and expertise have been mutually exchanged and the overall knowledge has been proven to be converged toward the maximum experienced Agent.

Key Words : E-government , E-government security , Agent system , Intelligent JAVA system, Intelligent Systems.

1. Introduction

Currently the undertaking applications acquisition the most attention of the information investigators cause of the growing of modern conceptions in software technologies. These conceptions was applied to establish complicated distributed systems through the world. The software migration race was begun to emigrate SW modules to become complementary to the undertaking. This furnishes deliverable environment at view of SW provider. Thus, modern topical platforms was put in like E-Government, E-Learning, E-Commerce and etc [1]. In E-Government, citizen anticipates services to be submitted in the same limitations where services are submitted as paper action. People attend to confidence what they conventionally use to fulfill their sensitive missions such as missions of bank account, releasing personal documents, buying and selling estates, and etc.

Recently, security has become a key factor in any network and cross the Internet. It involves a lot of different areas such as on safeguarding individual users against attackers[2]. Safeguarding corporate systems overs on the damages and safeguarding data from attacks. This is lacking in most companies whereby the are also lacking in the government to safeguard from these attacks and unauthorized entry. Hence it is not possible to set a network truly safe, as there are a number of areas that have got protected. This research contains an evaluation of contemporary techniques solving security the problem, damages and prevent data from attacks.

Security has become a concern of networking applications, as the persistent existence of E-portals necessarily requires them to give easy access to network materials, while they have to make sure that data and materials are kept completely safe and secured. The famous security mechanisms like the intrusion, the firewalls, the detection systems (also called IDS), the anti-virus software and many more, play significant roles in the laying out of the security strategy, even though they do not promise the continuous in-line security over the sophisticated attacks of contemporary cyber-hackers [3].

These mechanisms appeared to be more advanced over the hackers through the closure of every loophole and the identification of signatures attached to malware and attacks, however they are surmounted in their effort to expose new threats. Therefore the security experts are determined to innovate a new kind of network security strategies which can perfectly safeguard the network that has many layers of security strategy exposing instant threats prior to them becoming more serious over the network [4]. The government has got many roles to demonstrate in these all since the implementation has to do with the gain to the people they rule. E-government is referred on how information technology is used to provide the people that government governs with information and services [5]. This contains of the sharing of information between business and between other government agencies. A perfect representation is when it contains government relationship with the people via Government and the Business (meaning G2B), the Government and the Government (meaning G2G) and the Government and the Employee (meaning G2E) [6]. Another security mechanism currently adopted by many of the advanced nations including the E-Governments is called the agent based system [7]. The agent means a computer system which is situated with and has interaction with its own surrounding. The two relationships of the agent and its surrounding involve a consequence and result relationship. As the agent is located in the environment, whatever step the agent makes closely affects the environment. When the agent takes a step from its domain location to another domain location, the consequence of this on the surrounding is that the prior domain location is over taken by the new domain location. Although less important as the analogy suggests, the environment made some alteration that can be felt by other different objects [8].

2. E-government Security

The term Security is certainly is very important elements of the E-Government system in every country. Regular security issues include confidence, authentication as well as access control [9]. Consumers demand a confident relationship along with the entity which provides the duty. On the other hand, all of information acquired in the service course supply would be worthless. At last, there are three main functions that were provided by E-Government services, the first one is to know the consumer that will receive the service from E-Government services, second, detect if the consumer has the accessibility to this service, and lastly, detect if the consumer will pay for this service or not. these concerns of security indicate how security is seriously necessary issue in E-Government services, each of those clients and governments, as well as that it should be taken in to consideration from the starting specification of the Communication Technology and Information [10].

In current moment networks the capability to protect information is very important to the being successful of government procedures in every country all over the world. In current time, the Government of lately developed countries realized the benefits of this work is started to develop abilities inside Ministries at countrywide level. The usage of specific helpful resources like risk assessments is surely a good example [11]. The Information assets this, since with other essential business assets, is important to a business of organization in the modern interconnected business environment. Because of the rising inter-connectivity, information is currently revealed to a quantity and wide range of vulnerabilities and risks. Information security is a safeguard of information beyond a wide range of risks like unauthorized accesses and virus attacks by the hackers and also crackers to make sure business continuity would decrease business risk, and also increase return on investment as well as business opportunity. Information security is obtained by implementing an appropriate set of controls, such as policies, procedures, processes, the structures of organization together with hardware and software functions. Those kinds of controls require being established, monitored, implemented, improved and reviewed.

To make sure security goals of government agency are realized. That ought to be done in association with additional business management procedures [12].

3. Agent System and Security

Nowadays, the emerging agent technologies and agent paradigm become the key for the flexible application and worldwide solutions with regard to open services market in the society of information. They become promising technologies for developing and designing complex software systems for example distributed systems and security [13]. The most broadly applied the intelligent agent definition was a system which entertains the following attributes Autonomy; agents run without direct involvement of human or others, also have several type of control through their internal state and actions. Public Ability; agents communicate with other agents through some type of agent interaction language. Agents understand their respond and environment in a time fashion to change it. Pro-activeness agent does not take action in response to the environment their ability to exhibit directed behavior goal by using the initiative.

The mobile agent is an object of software which is not certain to the system exactly where they begin performance; this has the sensible agent attributes beside the potential to migrate through one system within a network to a different network with their execution state and code. Multi-agent systems are system platforms that can control network of mobile and intelligent agents, which work with each other to solve a problem based on the agent knowledge in the network [14]. The intelligent agent has four main kinds they are: Straightforward response agents; acts just on the base of the recent precept. This function is depending on the Model-Based Agent condition : action; and handle partly noticeable environments. The current state is saved within the agent retaining for certain type of structure that explains the world part which are not able to be seen. This behavior needs information of how the world works and also behaves. Goal-Based agent; agent selects among multiple opportunities, choosing the one that gets to the target state.

Utility-Based agent; agent chooses the perfect action which achieves their targets. This measure may be achieved by the usage of a utility functionality which usually maps state in order to measure of the stated utility

4. Intelligent Agent based security policy Deploy (The proposal system)

Intelligent agent-based security policy developer referred to application of Web-Server, which has a high level of privacy for interactive with consumers like formal sites, banks and sites of government. This particular class of web software applications are controlling very sensible information related to the clients; therefore the confidence and trust is the essential factor to perform transactions through these types of applications web. The basic skeleton which the suggested system based at J2EE in which JSP is addressing the presentation layer, like it was mentioned in introduction section, these JSP-pages tend to be going to perform developing forms for interacting holding and clients codes to test session properties approved by business-logic. This business-logic was the processing where accomplished; business-logic could be Servlets, Java classes or EJBs. Figure (1) is showing the material components of the proposed system application.

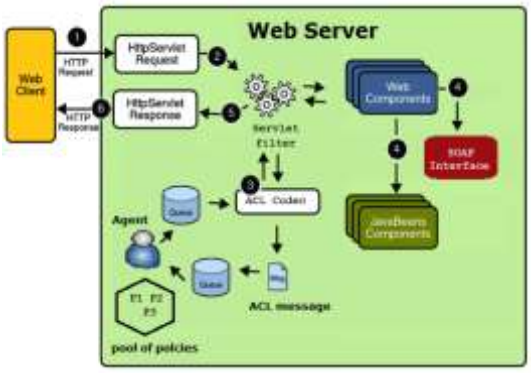

Figure (1) Components of the Autonomous Agent Security Policy Deploy System

The figure (1) promotes information inflow if clients react with the application; this means at this point the web applications which are under the checking of the current system, and below are the important components:

1. **Web-client**: this is an internet browser that utilized to explore with regard to the web application; each kind of internet explorer could be utilized likes Firefox, safari, internet explorer, or many other types.
2. **Web application server**: a program was utilized to host application of web; and the application must to collaborate with the application of web server to run smoothly, numerous applications are available like TomCat and Glassfish. This paper is using TomCat cause of its performance and light weight in spite of TomCat does not upholding EJB by default.
3. **Servlets**: real work logic to handle arriving demand (request) of client and reply to applications of clients. Servlets are implementing within servlet context that is the directory where the program of servlet is running.
4. **JSP pages**: frontal brim of the application of web which are accessed through the internet utilizing the software of web client. Every page is given a unique URI (Unified Resource Identifier) or URL (Unified Resource Locator).
5. **Http Servlet Request**: object in which client's information is encapsulated. Each data passed through client into server is packaged into Http Servlet Request object. It is the charge of programmer to protest this object and excavate passed parameters.
6. **Http Servlet Response**: object where the information is feedback to the client application.
7. **Web filter**: object which was installed to protest client demand before it gains to JSP and servlet; it is utilized to forward arriving traffic to Agent behaviors.

4.1 Dispatching Policy Agent behaviors

Effective job, an agent must carry out within behaviors which usually are run like a time frame bin in order to implement enclosed code. The mode of Agent should go to sleep whenever there is actually no behavior is scheduled to accomplish. Agent's behaviors are to wake up about to obtaining ACL message. Behaviors could engage concurrently. Within this suggested Policy Agent major behavior is activated with receiving the Request object of Http Servlet. Figure (2) provides the processing lifecycle of Http Servlet Request.

Journal of AL-Qadisiyah for computer science and mathematics Vol.9 No.2 Year 2017
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

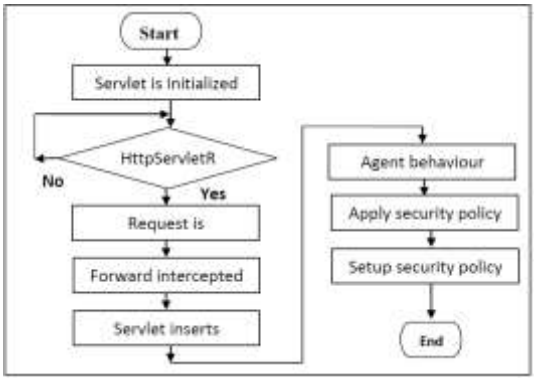

Figure (2) Http Servlet Request processing lifecycle in this proposal

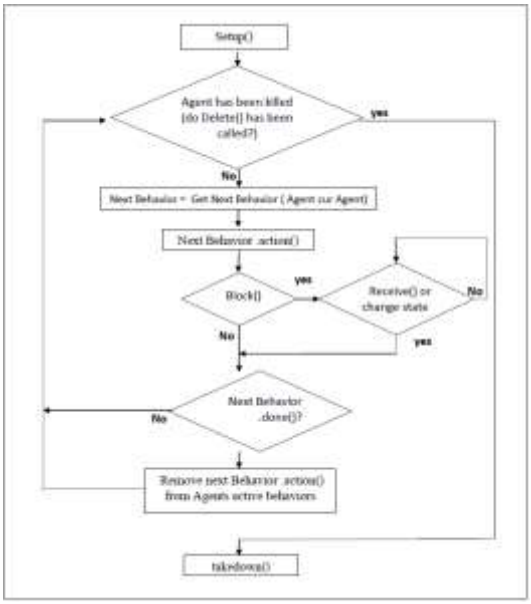

Figure (3) Highlights the behaviors' dispatching scheme utilized by Policy Agent where environmental situations stimulate behavior dispatching.

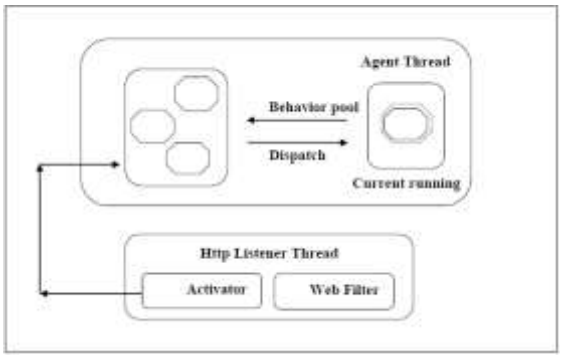

Figure (4) Behaviors are activated cause of environment change

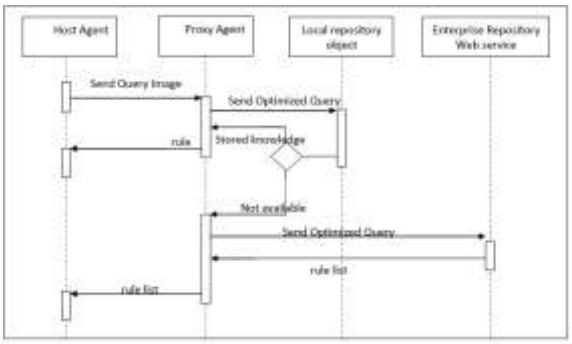

Figure (5) Sequence diagram of complete 2-tier knowledge transfer

Every security policy is used by separate behavior; hence dispatching behavior is dependent on the changing in the environment, to put it differently obtaining new Http Servlet Demand with different consumer information. Figure (3), (4) and (5) provides dispatching scenario which is used in this proposal just where web filter can be responsible regarding the activation of Agent thread right after receiving HTTP Request.

4.2 Mathematical Model

The mathematical model for the design of the according to the logical statement as in Figure (6). This statement was used to identify the user's behaviors pattern as they visit the Iraq government websites. This will make sure the patterns of the users can be identify to predict any attack online.

$$Interaction_a \cap Anno(Query_j) = S_a \quad \text{and} \quad = \sum_{i=1}^{K} weight(behavior)$$
$$Interaction_\theta \cap Anno(Query_j) = S_\theta \quad \text{and} \quad = \sum_{i=1}^{L} weight(behavior)$$
$$\vdots$$
$$Interaction_n \cap Anno(Query_j) = S_n \quad \text{and}$$
$$T.W_{Agent_{ij}}^{Interaction} = \sum_{i=1}^{M} weight(behavior)$$

$T.W_{Agent_{ij}}^{Interaction_i}$ is Total weight produced by $Agent_j$ for $interaction_i$

Figure (6) Mathematical Model

4.3 The Policy Agent protect Web application system

Probably the most interesting feature of Agent is the silent existing, which the agent SW module will not react users immediately; it operates on the part of the primary system, therefore its presence is simply not noticeable, for instance Latizia agent assists users to enhance inquiries gave to search engines. Considering this study is the web application back end as well as does not get involved in any way the web application business logic, a front end is actually required to illustrate Policy Agent in actions. Figure (7) provides an easy to customize web page released as a template with regard to front end web application system, this web page is re-designed and modified to fulfill the requirement of Policy Agent.

Figure (7) Servlet and JSP demo site for monitoring by security Agent

Policy Agent could be linked to almost any java based website (servlet and jsp); which is the web filter is employed to send traffic to the Agent module or maybe Policy Agent may setup http listener in order to capture http request. This study utilizes web filter to send the traffic of http session into the Agent. Figure (8) provides the form utilized to interact clients that are working with this web site, in the end the main aim at this point is a security policy, therefore the designated sites tend to be comprise exchanging critical information together with clients (such as, arriving personal information, bank accounts).

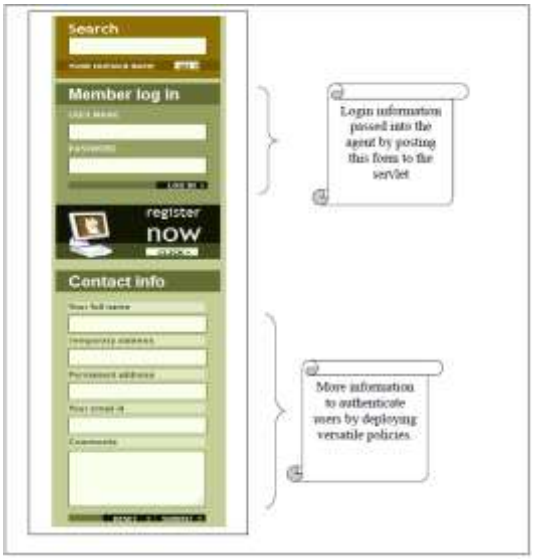

Figure (8) Client side form applied to interact the website

This particular implementation is showing of deploying the agent like automatical security deployer which is the data summarized with user call is to be extracted to produce more useful information. The discovered manner was coming from mining the demand will help Agent to consider credible decisions; this means that to pick appropriate security policy which will match with the situation. To illustrate aim Remote Agent Management (RMA) is appealed to reveal what will go under hood. Remote Agent Management is a strong Agent controlling appliance utilized to produce Agent application inside JADE. Figure (9) provides the RMA user interface appliance delivered with JADE package, also this interface offers numerous utilities to enable controlling Agent programs. Every application are devoted to single Agent or maybe to several Agents in several programs.

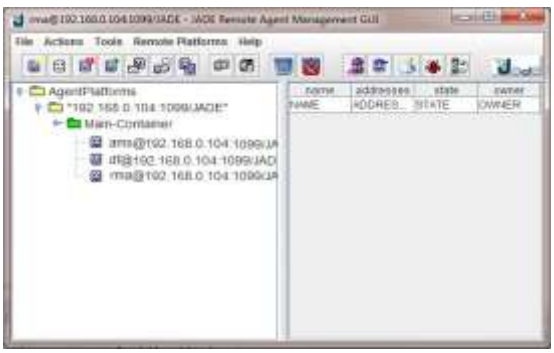

Figure (9) Start up window of the Remote Agent Management

There are three initialized agents when first invoking regarding RMA happened: (Remote Agent Management) RAM, (Directory Facility) DF, and (Agent Management System) AMS. Each one of them engages an essential task in the platform, 'RAM' is the main one which is very important to this research is that the Agent charge of administering remote Agents, therefore messages are ordered from the servlet in order to the make agent great influence of remote agents. Because Policy Agent is planned to deploy efficient security policies in order to dedicate web site, thereby a stub must be inserted in that application system to forward the traffic for the Agent. This is very possible to set up HTTP listener in order to detect HTTP sessions however would probably not avoid the traffic from being able to access the site business logic; this is a weakness that official sites cannot afford to have. Following an effective initialization with regard to the servlet the agent could be invoked for monitoring this session. Once the agent started, it will remain there till the application underlying. In this study TomCat server is utilized to host the application web because of the web application developing blocks (such as, java beans, servlet, java classes, and EJB). Figure (10) gives a screenshot of ram showing that Policy Agents was invoked and also initialized correctly inside a concentrated container known as 'Agent Policy Deplorer'.

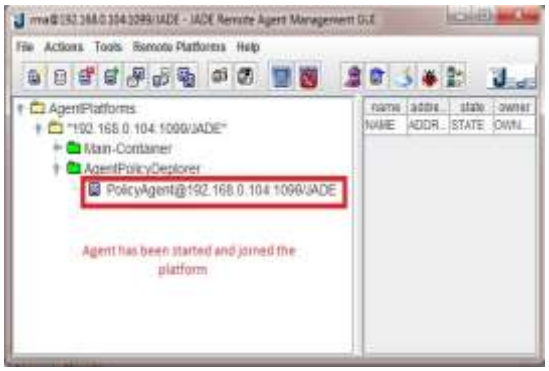

Figure (10) Poly Agent was launched and tied the platform

As mentioned before, the category of application which is proposed in this research is designated to the based web application of java (such as, Servlet web applications and JSP), therefore a filter stub could be installed to send the traffic as it is shown in figure (11).

```
public void doFilter(ServletRequest request, ServletResponse response,
        FilterChain chain) throws IOException, ServletException {
  // standard processing logic
  // code stub added to forward session HTTP traffic
RequestDispatcher rDisp = request.getRequestDispatcher("AgentRouter");
     rDisp.forward(request, response);
                                                                    }
```

Figure (11) Code stub established in web filter

RMA has a quite strong tool that makes it easy for Agent's developer to be captured all messages passing the system between Agents; this kind of tool is the agents sniffer, figure 12 highlights a sniffer Agent's GUI screen shot, that developer could select which Agent to display and monitor. This research has only single Agent that is Policy Agent, therefore the sniffers was installed to the Policy Agent as it is shown in figure (12).

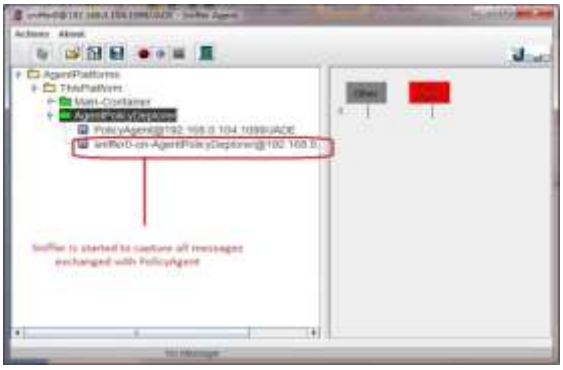

Figure (12) Using Agent Sniffer to monitor exchanged ACL Messages

Generally, Agent Communication Language (ACL) Messages are changed between Agents, however at this study; the messages would send through (web application filter) non-Agent module is in charge of forwarding arriving stream and marshaling to the servlet towards the Agent.

```
createNewAgent(String nickname, String className, Object [ ] args );
```

Figure (13) Create New Agent method prototype

Servlet is implementing Concurrent Linked Queue to contact with Agent, just where two situations pass into the Agents as arguments utilizing array of items to create New Agent() technique, and this technique has prototype demonstrated in figure (13). The 3rd parameter is the more critical parameter in develop New Agent() method because of its role in having Java objects array that could be approved to the Agent. To obtain approved array of objects get Arguments() API is employed as it is displayed in figure (14) using the

jade.core.Agent. The get Arguments() is obtainable only in setup part of the Agent code.

Figure (14) Retrieving the passed Arguments

4.4 Online Data

The online data obtain from the users activities online (This study involves 90 participants for three ministries of Iraq). Tables (1, 2, and 3) are the tables captured for 30 users who were trying to do true and false login on the three web sites. Obviously, presented table is capturing the quality of each agent to detect fraud users, for this purpose a list of users have been built and hosted in separate SQL server, each row of the three table is representing trials of user with certain user name, where TP, FP, TN, and represent True Password, False Password, True Name, and False Name respectively.

Table (1) Login of 30 users into Site One

Site 1				
Index	TP	FP	TN	Accuracy
1	0	1	2	0.666667
2	1	1	2	0.75
3	2	1	2	0.8
4	2	2	2	0.666667
5	3	2	2	0.714286
6	4	2	2	0.75
7	4	2	3	0.777778
8	4	2	4	0.8
9	4	2	4	0.8
10	5	2	4	0.818182
11	6	2	4	0.833333
12	7	2	4	0.846154
13	8	2	4	0.857143
14	9	2	4	0.866667
15	10	2	4	0.875
16	11	2	4	0.882353
17	12	2	4	0.888889
18	13	2	4	0.894737
19	14	2	4	0.9
20	15	2	4	0.904762
21	16	2	4	0.909091
22	17	2	4	0.913043
23	18	2	4	0.916667
24	19	2	4	0.92
25	20	2	4	0.923077
26	21	2	4	0.925926
27	22	2	4	0.928571
28	23	2	4	0.931034
29	24	2	4	0.933333
30	25	2	4	0.935484

Table (2) Login of 30 users into Site Two

	Site 2				
Index	TP	FP	TN	FN	Accuracy
1	0	1	2	0	0.666667
2	1	1	2	0	0.75
3	2	1	2	0	0.8
4	2	2	2	0	0.666667
5	3	2	2	0	0.714286
6	4	2	2	0	0.75
7	4	2	3	0	0.777778
8	4	2	4	0	0.8
9	4	2	4	0	0.8
10	5	2	4	0	0.818182
11	6	2	4	0	0.833333
12	7	2	4	0	0.846154
13	8	2	4	0	0.857143
14	9	2	4	0	0.866667
15	10	2	4	0	0.875
16	11	2	4	0	0.882353
17	12	2	4	0	0.888889
18	13	2	4	0	0.894737
19	14	2	4	0	0.9
20	15	2	4	0	0.904762
21	16	2	4	0	0.909091
22	17	2	4	0	0.913043
23	18	2	4	0	0.916667
24	19	2	4	0	0.92
25	20	2	4	0	0.923077
26	21	2	4	0	0.925926
27	22	2	4	0	0.928571
28	23	2	4	0	0.931034
29	24	2	4	0	0.933333
30	25	2	4	0	0.935484

Table (3) Login of 30 users into Site Three

	Site 3				
Index	TP	FP	TN	FN	Accuracy
1	1	1	5	0	0.857143
2	80	1	0	4	0.941176
3	60	1	1	6	0.897059
4	1	2	1	6	0.2
5	10	2	2	6	0.6
6	30	2	2	6	0.8
7	4	2	3	6	0.466667
8	4	2	4	6	0.5
9	4	2	1	7	0.357143
10	5	2	4	6	0.529412
11	6	2	4	6	0.555556
12	7	2	8	6	0.652174
13	8	2	4	6	0.6
14	9	2	4	6	0.619048
15	10	2	4	6	0.636364
16	11	2	4	6	0.652174
17	12	2	4	6	0.666667
18	13	0	4	6	0.73913
19	14	0	4	0	1
20	15	0	4	0	1
21	16	0	4	0	1
22	17	0	4	0	1
23	18	0	4	0	1
24	19	0	4	0	1
25	20	0	4	0	1
26	21	0	4	0	1
27	22	0	4	0	1
28	23	0	4	0	1
29	24	0	4	0	1
30	25	0	4	0	1

Amazingly, all sites showed convergence in their behavior to detect fraud and users by developing the knowledge for the entire system. Figure (15) shows very important behavior where at the starting phase of the smart site (i.e., smart site is the site that equipped with smart agent to monitor user behavior), the site doesn't have stable behavior due to the low level of knowledge developed by the smart agents, but as the progress of the monitoring is advanced and mutual exchange for the knowledge is conducted, the graph shows convergence toward stable area.

Figure (15) Agent's behavior at Site One converge to stability

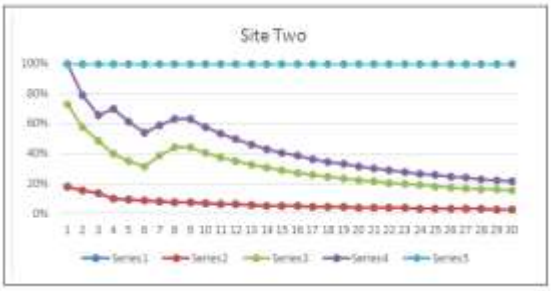

Figure (16) Site Two is affected by the Smart Agent at Site One

Figure (16) shows stability better than site one even from the early stages and this is due the knowledge exchange by Agent Detective-1, which is the agent in charge of monitoring Site One and revealing patterns and information for the entire system. From figure (17), the web site 2, and its smart agent, is capable on tuning up its behavior up to the information gathered by the system.

Figure (17) The accuracy in responding to login process is stabilized

Every agent is capable of using the knowledge in two modes: first mode which is the online mode, in this mode the agent counts on the central knowledge developed at the site of the administration, thus every query is to be sent to one central point which is producing a bottleneck when is system expands to high number of participants, while in mode two, every agent is developing its own knowledge, thus it is an offline mode. The most important issue faced the implementation is the synchronization of the knowledge in mode two where all agents have to hold the same knowledge; this has been achieved by creating version number that represents current version of the knowledge base, and broadcasting a query for all agents within the platform to respond with their version number, if one agent does not have the updated version, then an update process in forced over this agent.

In figure (18), the stability of the behavior for each smart site is presented where again the accuracy oscillates while the system is building the knowledge but after that, it is very clear that the accuracy is stabilized and keeps approaching an optimal point. Figure (19) shows the same behavior at site Three when the agent is not stable in identifying coming login at the first stage but when the system keeps going, the last section shows great stability. The most important behavior is introduced at site one where it does not hold any oscillation even at the first stage; this is due the knowledge built within the system is delivered to the new comer as an inheritance rather than start from scratch again.

Figure (18) Site Three is introducing great stability

Figure (19) Site One Stability

Login process was the use cased exploited to present the proof of concept where the proposed system by this thesis stated the theory of utilizing socialization approach to develop trust and confidence for societies who are recently faces the deploying of the new technologies, but this case can be expanded easily to more advanced processes and gaining the same results. Social programming is the programming approach that has been utilized to implement the proposed system and the results proved that social approach is a very fruitful approach when it comes to most recently developed countries in term of enforcing the technology backbone. One last issue which is to be presented in this chapter is the authentication mechanism where a simple authentication procedure is implementing to discriminate administrators than the normal agents; this procedure is by having a special key which is defined at the initialization phase of the implementation.

5. Conclusions

This paper has been dedicated to investigate the exploiting of social behavior as a convenient approach to enforce the community's acceptance for new technologies; this is due to the nature of communities in recently developed countries tend to count on social behavior as the only mean to bring trust and confidence. To achieve this approach, an autonomous software modules have to be injected within the software technology; this is to promote the behavior of traditional software modules from the reactive mode (i.e., responding to events occurred within the environment) of the instruction base (sequential or parallel execution of series of instruction or commands) to the most prominent human behavior which is the pro-active (i.e., collecting information about the environment before the interaction).

This paper has deployed the Agent technology where software modules have the ability to perceive the environment and change its behavior according that perceiving. The main target of this thesis was the government web sites where people come to interact looking for electronic services released by the government entities, each site has been equipped with a middle layer through which the agent can hook itself into and mount one of its sensors, this is from a side and from another, it will listen to the environment (i.e., Agent communities within a platform) and gaining knowledge out of the conversation, agents were able to do the knowledge transfer and eventually achieve the target. Along the implementation of the proposal and after the discussion of the resultant data and numbers, many conclusions have been reached out: Social behavior has been proven to be a very effective methodology to enforce security; this is by identifying new malicious activities that violate security metrics even its signatures net yet identified. Social behavior of the software agent by monitoring system reaction to certain input (i.e., say for example user name and password) can be used as single point of allegation, but this allegation is to be crystalized by sustaining the allegation by other agents within the platform.

The deviation of behavior of human been in interacting web sites tend to be in repetitive pattern (e.g., error in interaction the web site due to mis-spelling or due mis-understanding to web site content and directions). This repetitive pattern will be recognized by the Agent community and crystalize it as artifacts. Human interaction with government web sites is monitored be software module that has the ability to introduce smart behavior in collecting information.

References

1- Aronson, J., Liang, T. & Turban, E. 2005. Decision support systems and intelligent systems. *Yoyakarta: Andi***,** 24.
2- Arachchilage, N. A. G. & Love, S. 2014. Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38**,** 304-312.
3- Sullivan, C. 2005. *Cisco Security Agent*, Cisco Press.
4- AP Test 2011. Types of Software Testing. *[Accessed on the 26th of March, 2012] Available at:* <*http://www.aptest.com/testtypes.html*>.
5- Almarabeh, T. & AbuAli, A. 2010. A general framework for e-government: definition maturity challenges, opportunities, and success. *European Journal of Scientific Research*, 39**,** 29-42.
6- Valentina, N. 2004. E – Government for Developing Countries: Opportunities and Challenges. *[Accessed on the 25th of February, 2012] Available at:* <*http://unpan1.un.org/intradoc/groups/public/documents/untc/unpan018634.pdf*>.
7- Chappin, E. J. & Dijkema, G. P. 2010. Agent-based modelling of energy infrastructure transitions. *International journal of critical infrastructures*, 6**,** 106-130.

8- Amani, S. E., Mohamed, S. & Ibrahim, E. 2009. A Multi Agent-Based Framework for Network Intelligence and Intrusion Prevention, Cairo. . *[Accessed on 12 May 2012], Available at: <http://www.dtic.mil/dtic/tr/fulltext/u2/a417590.pdf>*.
9- Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F. & Sommerlad, P. 2013. *Security Patterns: Integrating security and systems engineering*, John Wiley & Sons.
10- Public Management Service 2001. E-Government: Analysis framework and methodology, December 2001. *[Accessed on the 24th of February, 2012] Available at: http://www.olis.oecd.org/olis/2001doc.nsf/c5ce8ffa41835d64c125685d005300b0/0b677ed527d35bc0c1256b21004f4b6a/$FILE/JT00118445.PDF*.
11- Drennan, L. T., McConnell, A. & Stark, A. 2014. *Risk and crisis management in the public sector*, Routledge.
12- Ian, M., Mahmood, S. & Brian, G. 2015. Government Of Iraq Egovernment Strategy, USAID. *Funded Economic Governance II Project, US.*
13- Sharma, V. P., Trivedi, V. & LNCT, B. Year. SECURE MOBILE AGENTS ON AD HOC WIRELESS NETWORKS. *In:* National Conference on Security Issues in Network Technologies (NCSI-2012), 2012.
14- Roscia, M., Longo, M. & Lazaroiu, G. C. Year. Smart city by multi-agent systems. *In:* Renewable Energy Research and Applications (ICRERA), 2013 International Conference on, 2013. IEEE, 371-376.

تصميم نظام إدارة امني ذكي قائم على إدارة الحكومة الالكترونية

ضياء شهيد العزاوي سنان عدنان ديوان الشمري

كلية علوم الحاسوب وتكنولوجيا المعلومات
جامعة واسط

المستخلص :

ان الحكومة الالكترونية تقوم بإيصال خدماتها الى المواطنين والشركات بشكل الكتروني وهو الاختلاف الاساسي عن عملية توصيل الخدمات في الحكومة الاعتيادية وان اهم عامل يخص موثوقية خدمات الحكومة الالكترونية هو العامل الامني اي امنية المعلومات والذي يقود الى القبول والثقة والقناعة بهذه الخدمات الالكترونية من قبل المجتمع والمواطنين والشركات. ان الموديل المقدم في هذا البحث يقوم ببناء عملاء امنيين اذكياء يتشاركون المعرفة ولهم القدرة على تحليل ومراقبة سلوك مستخدمي المواقع الالكترونية الحكومية ولهم القدرة على اتخاذ القرارات والمشاركة في المعرفة ويتم بناء العملاء الاذكياء باستخدام لغة جافا. ويكون لكل موقع الكتروني حكومي مجموعة من العملاء الاذكياء الذين يقومون بمراقبة ودراسة سلوك مستخدمي هذا الموقع وتحديد الوثائق المزورة والمستخدمين السيئين ونقل هذه المعرفة الى العملاء الاذكياء الاخرين المسؤولين عن المواقع الالكترونية الحكومية الاخرى ، تم تنفيذ هذا البحث على ثلاث مواقع الكترونية حكومية لوزارات النفط والمالية والداخلية وتم دراسة سلوك مستخدمي هذه المواقع الالكترونية ، وتم تناقل المعرفة والمعلومات المكتسبة للعملاء الاذكياء في ما بينهم .