International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 1, February 2019, pp. 621~628
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i1.pp621-628

A dashboard of intelligent transportation system (ITS) using mobile agents strategy on notification authentication process

Najia Allali, Zineb Chaouch, Mohammed Tamali
SimulIA Team/ENERGARID.Lab, Tahri Mohamed University, Algeria

Article Info

Article history:

Received Jan 1, 2018
Revised Jul 5, 2018
Accepted Jul 28, 2018

Keywords:

Authentication
ITS-dashboard
Mobile agent
Mobile device
Notification
Performance
Security

ABSTRACT

Extracting accurate information from huge Transportation Database need to build efficiency Intelligent Transportation Systems ITS-Dashboard that should allow making correct decisions. The quality of decision and the achievement of performance depend on the quality of the information supplied. This information must be reliable, complete, pertinent and more to care about external attacks. Distributed Mobile Agent consists of autonomy of entities with capacities of perception, cooperation and action on their own environment. One of Agent function is the security of Authentication process by activation of notification system on Mobile Device. The main purpose of this paper is to make it consisting of an Agent Based Framework. The strategy is to exploit Mobile Agent capabilities in a Strict Notification Process when user validates his authentication request.

Corresponding Author:

Najia Allali,
SimulIA Team/ENERGARID.Lab,
Tahri Mohamed University,
Street independence B.P. 417, Bechar, Algeria.
Email: allalinadjia@gmail.com

1. INTRODUCTION

Intelligent Transport Systems (ITS) contains an enormous volume of data about various activities management based on different accounts, due to the growing demand for transportation services, competitiveness, and technological development; Organizational management needs a decision support tools, such as Dashboards. The ITS Dashboard is a set of pertinent data and indicators allowing a decision-making guidance to management in order to achieve the objectives [1], and to improve the quality of the service offered.

The usage of dashboard is limited not only to public information but also to confidential information, which has a value of confidentiality to certain parties so that it needs some security controls [2]. Password authentication is an important security tool because it allows organizations to secure their dashboard by allowing only authenticated users (or processes) to access its protected resources, which can include synthetic views of past, present, and therefore the future of the company.

Most computer systems, Internet-based environments, and networks use password authentication[3]. Once a Password (PW) or One Time Password (OTP) which is valid for the only certain amount of time or one session [4] has been entered, the system looks up it in the password hash. If the stored password matches the entered password for the specified username, the user is authenticated in that system. The adoption of the password in various formats [5], [6] without other operations is considered as a threat to the credibility of the systems and private information, because it is either simple or attacking quickly.

The proposed framework attempts to develop a system which automates the control of the Password authentication process. It uses agent technology to notify the owner for each authentication request.

When any user tries to log in on the Transportation dashboard trough desktop or mobile Authentication Interface, a remote user notification is launched. The framework will be adapting the notification mode according to the event context. This paper presents the new model based on realization of an Intelligent Agent to act as a Notification System to inform and alert the concerned admin or owner, when trying to authenticate or change the state of an account.

2. BACKGROUND

2.1. Mobile agent paradigm

Since the 1990s, with the development of computer network and computer communication technology, Mobile Agent technology is known as a high acceleration with various uses in many areas. So, it is a practical choice for many applications, for several reasons, including improvements in latency and bandwidth of client-server applications and reducing vulnerability to network disconnection [**7**]. Mobile Agent applied to mobile computation, M-commerce (especially mobile e-commerce) [8], [9], administration of networks, distributed information and so on. In computer science, the term agent can be associated with many different ideas: an agent is considered as a goal-oriented program with some learning ability [10], ability to move from machine to machine possibly in a heterogeneous network [11]. The program chooses when and where to migrate. It can suspend its execution at an arbitrary point, transport to another machine and resume execution on the new machine. It can dynamically adapt to individual users and can perform specific tasks autonomously in an environment. Thus, agent and its environment must come in a parallel for each taken action by the agent that would affect its environment and vice versa.

The advantages of using mobile agent paradigms have been proposed by [12]. These advantages include: Overcoming Network Latency (ONL), Reducing Network Load (RNL), executing asynchronously and autonomously, adapting dynamically, operating in heterogeneous environments, and having robust and fault tolerant behavior.

In the Notification Authentication Environment for the Agent, Agents represent owner or user how trying to login. When there is a new authentication request or new announcements available, Agents will react to its environmental changes, by sending the notification to authority-receptor (owner, administrator of the system, security partner) about every authentication request to access his account.

2.2. Literature review

In the literature, Agent-oriented programming is emerging as a popular programming paradigm for large and complicated system [13], [14]. An agent can learn from its interactions, or negotiation with other agents, and therefore exploit this information to notify for any new announcements made available. The Notification service offers the tool to enable the delivery of information about next events. The authors in paper [15] define a notification as a visual message, audible signal, or alert generated by an application or service that relays information to a user. More researches were being interested in agent notification. As [16] has proposed an Agent-Based monitoring and notification system in the wireless sensor network (WSN), where agents representing WSN nodes can report and send notification messages for critical events and vulnerabilities. Agent-Based approach explored by [17] to notify the smart grid about a change in air condition that affect load of a house. In [18] Alert Notification Service (ANS) represents a web service that automatically visits all requested websites selected by a specific user and alerts the user when a particular keyword phrase is changed. This action saves users' time and effort by reducing the repeatedly visiting multiple websites looking for some specific information or keywords.

The use of mobile devices (voice calls, video calls, text messaging (SMS), and multimedia messaging (MMS)) on notification system is a result of inventing more advanced mobile devices and the rapid evolution in wireless network infrastructure [19],[20]. Mobile devices are used in many important activities of the agent system, because of its many properties of flexibility, mobility, and adaptability through small and light, and movable devices.

2.3. Mobile notification in authentication process

Notification service offers the means to enable the delivery of information about immediate events. Define a notification as a visual or auditory signal [15]. There are a variety of means that are used for sending data. Free services like Google Alerts [21] allow sending of emails when an interesting event of user appears.

In mobile phones, notifications play an even more central role to “notify” users of new messages, events or actions. These are typically delivered instantly. For proper operation of the notifications, it is imperative to have a powerful mechanism for handling notifications. When a user is trying to authenticate, this action has triggered an event that requires notification by sending E-mail, SMS (phone), or Call Alerts the problem is that users exist in different timeframes. Within these different timeframes, some trying

authentication might be done, without the user is being notified early. An asynchronous communication must be enabled to delivering notification when the user is not connected to the system. The mobile notification system is one of the best selected methods. The decision to send notifications will be taken in the context of monitoring and authentication control and host control.

3. PROBLEM STATEMENT

There are several security levels which concerns in authentication like password schemes. Users have a tendency to use easy-to-remember passwords [22], [23], use the similar password for different accounts [3], and store these passwords on their systems insecurely, even if the case of strong password. This user may be vulnerable to threats especially family; thus forcing him to give the password to the enemy. The use of a simple notification system (SNS) on the login process requires an open connection without interruption. This is not economically and technically feasible. Add to this, SNS is limited when login on the device that we do not usually use, the notification mail about the login is sent to the registered address.

The ability of agent technology to react dynamically in unfavorable situations and events facilitates the construction of distributed robust notification systems and insensitive to failures. If a host is stopped (failure connection), all agents running on they are alerted to move and continue their operation to another host. The agents become independent of the process that created them and can work asynchronously or even autonomously.

4. MOBILE AGENT-BASED MODEL AND ITS IMPLEMENTATION

Our company information system allows networking with different services administration. Those interconnections create vulnerabilities for control of the authentication process and the follow-up of traces in the case of threats.

4.1. Authentication mobile agent

An Authentication Mobile Agent (AMA) is an agent that can move from machine to machine in the agent-enabled network [7] in the distributed system. The use of authentication process is to verify the identity of a user, server, and so on. Before a service will be accessible, the service must learn the user's identity. However, the authentication service needs a sophisticated notification system that keeps track of each successful or failed authentication attempt as shown in Figure 1.

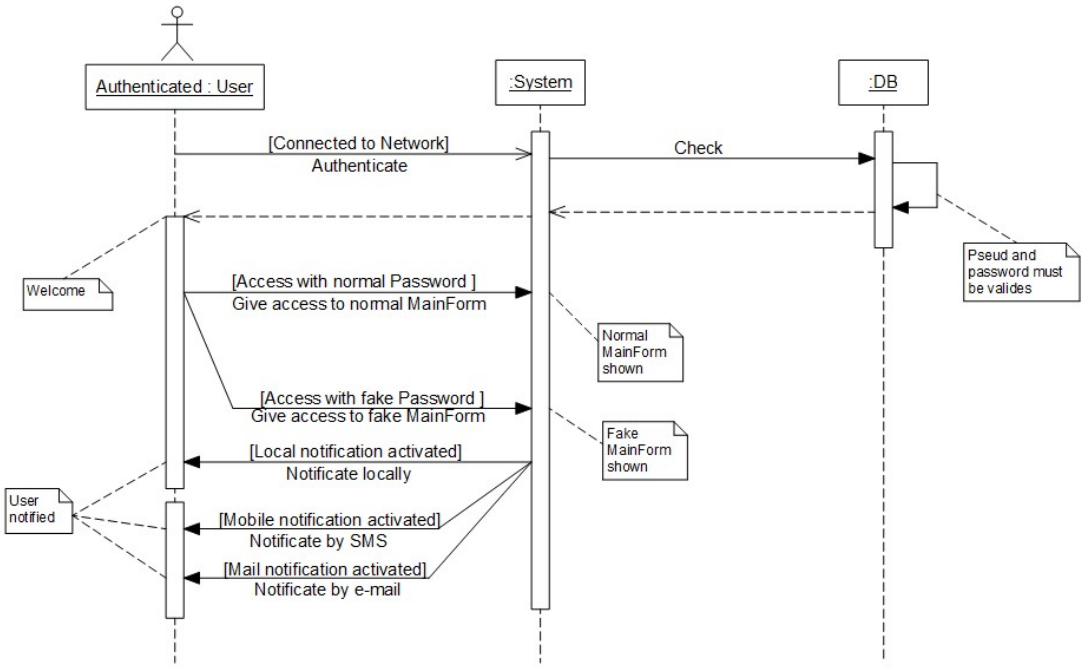


Figure 1. Sequence diagram authenticated

4.2. The proposed system

Notification of Authentication is carried out by different types of agents that perform specific function. Our proposed Architecture of Agent Notification System on Authentication Process (ANSAP) as shown in Figure 2 is a Mobile Agent based Notification System enables to verify the identity of the users connecting to system. When the user launches an authentication request, a Mobile Agent can wander from machine to machine in the agent-enabled network, to execute the request. Whatever the result, ANSAP will be sending asynchronous notifications into the mobile device of owner, because some Authentications request might be done without the owner awareness.

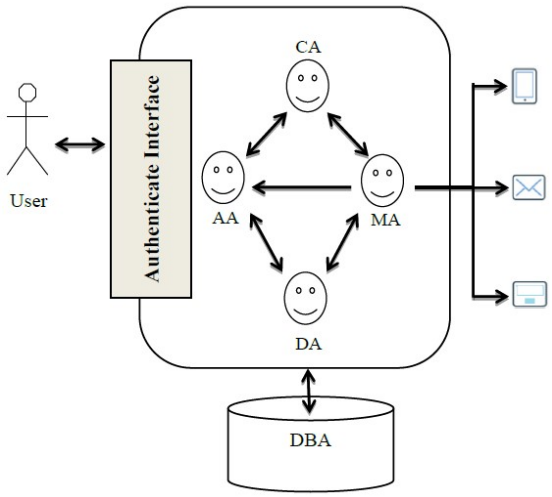


Figure 2. Architecture of agent notification system on authentication process

For having access to the resource, the entity should be adequately authenticated. There are three main authentication methods: Smart Card, Biometric Characteristics, and Password. Using any of these methods can help do the authentication. In our case, the classical method is chosen; when the password authentication process starts, an Authentication Agent (AA) is activated to collect the username followed by a password. This information (username, password) required to be stored in the Database server at registration phase. Authentication process consists of three phases: Registration Phase (RP), Login Phase (LP) and Verification Phase (VP) [24]. When the user enters the password on the displayed interface on the screen at (LP), the system verifies the entered password by comparing it with a content of the password generated during registration.

a. The ANSAP Framework: As mentioned before, an Asynchronous Communication Framework between the owner and the user who is trying to login. The idea is to provide this application on mobile device of owner to ensure his notification even as when moving. The model consists of the owner who receives notification, the user who tries to login and authentication request. When the user attempts to login on the Transportation System through desktop or mobile Authentication Interface, ANSAP receives Authentication Requests from login process through AA, stores them with GPS location and information about device used. After ANSAP executes the request by the strategy used, it will send notification according the obtained result to the owner through their Notification Agent (NAs). Our Framework performs all these functions through a set of autonomous agents: Detector Agent (DA) is a first agent that receives requests from the AA, sends it to Database Agent (DBA) to be stored in the database, and to Control Agent (CA). CA constructs a query and supplies DBA to retrieve the list of authorized-receptors of notification (Owner, Administrators, Security partner) if the case, and sends to Mediator Agent (MA). MA receives a list of receptors from the CA and deliver notifications to the NAs.
b. Mobile device: In the role of owner who is notified once he is registered in Transportation Database.
c. NAs: agent resides in the owner' mobile device. It has a role of displaying notification to owner.
d. Database server: Contains different pertinent data in concern of owner, owner account, mobile phone, and activities journal and so on. To interact with Database, DBA is an agent that resides in the database server. The DBA receives the various queries from the ANSAP agents: Insert, Select, and Update.

4.3. Demonstration

The user can login with the Username and Password. These details are compared with stored identity in Transportation Database server. There are three possible scenarios to describe the several actions of an agent within this Framework.

a. Scenario1: Successful Authentications

This scenario illustrates a sequence of activities that happened when the user succeed in authentication. The changes in its environment trigger the agent. The detector agent will receive any request of authentication newly from authentication agent. Once the authentication succeeds, the MA will interact with the NA to alert on this. At that time, the system provides access to the real platform, and different actions and communications of ANSAP agents are illustrated as shown in Figure 3. After authentication, the employee will receive notifications reminding him of meetings, scheduled tasks, etc. However, these types of notification events are outside this paper.

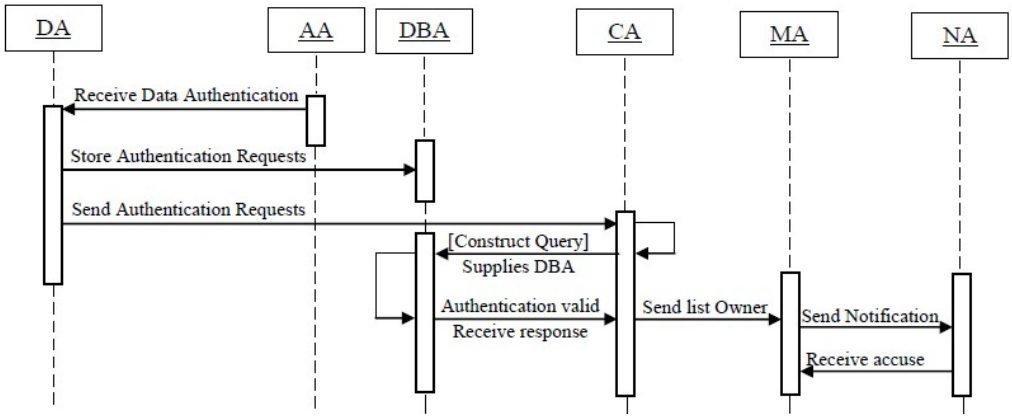


Figure 3. Successful authentications

b. Scenario 2: Falsification Test gives positive result

The first scenario is expanded to describe a situation in which a user uses a falsify password for authentication. With this new change, CA constructs a fake query for supplies DBA when test gives a positive result as shown in Figure 4. For security reasons, ANSAP will automatically block the relevant account, and allow the user authenticated to another fake platform. The MA will send an urgent alert to security partner and services.

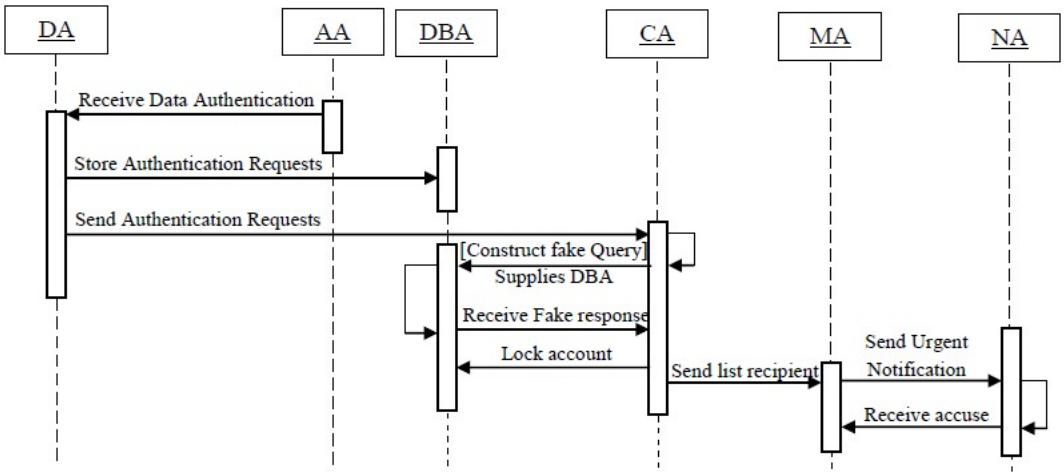


Figure 4. Falsification test gives a positive result

c. Scenario 3: Falsification Test gives an adverse result

When the test of fake query gives an adverse result and considering to the number of failed authentication attempts, (ANSAP) will notify owner in the first failed authentication attempt. Secondly, Administrator of the system and the owner will be warned. On the third failed attempts, the Administrator will be alerted so that this account will be automatically blocked owing to security policy measures as shown in Figure 5.

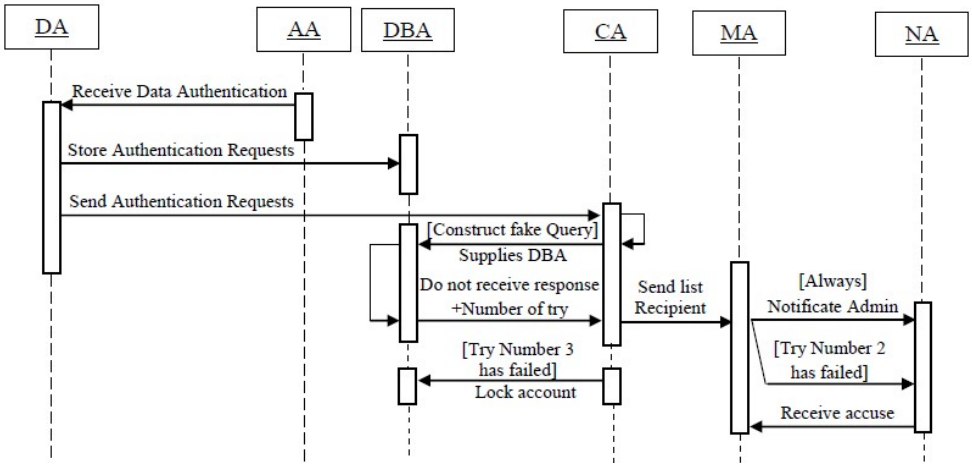
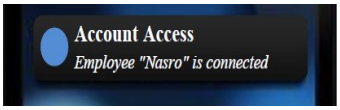
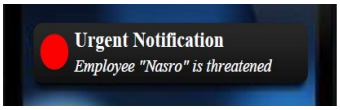
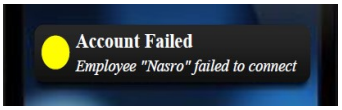


Figure 5. Falsification test gives a negative result

4.4. Implementation

To notify the user during an authentication process, anywhere and in real-time by auto-sending SMS notification is not always guaranteed. In wireless networks, disconnection and failure to deliver notification are possible. So, the MA is responsible for sending the notification to the NAs until ensuring that all authorized-receptors have received notification as show in Table 1.

Table 1. Result of Different Scenarios

Scenario 1	Scenario 2	Scenario 3
ANSAP sends notification "Account Accessed" automatically to the owner.	It is one of the most difficult situations, where the administrator receives "Urgent Notification" on the threat from ANSAP, which will help to move quickly to protect the person and the company	Depending on the number of failed tries, the administrator and the owner receive a notification "Account Failed"
		

5. DISCUSSION

The use of wireless and mobile devices in ANSAP allows providing users with efficient services and sharing information about their account, without need to use a specific mobile phone or a service. Hence, the system is widely adoptable without making big changes, and it is independent of any proprietary data format which makes it easy to be used by different grid management software. The objective is always how making it harder for the hacker and attacker to impersonate someone and login to his account. After using ANSAP, we noticed improvements in safety and speed in making the right decisions, to prevent many threats and trace their proportions and analyze their causes. As such, cannot overlook that one of the critical factors in a successful security strategy is user adherence to the procedure itself. Mobile technologies can be the best ally of any security strategy in identity protection and follow the authentication process addition the cost of notification via cellular network or Wi-Fi is almost zero and achieves a very high user satisfaction rate.

6. TOOLS USED

To use of mobile agent's techniques, the system must have a mobility framework for all of the agent modes, including the navigation model. For the lifecycle model, we need services to create, destroy, start, suspend, and stop, etc., agents [25].

JADE (Java Agent Development Environment) [26], [27] is a software Framework to be run under Java Environment with a flexible infrastructure. It is a middleware developed by TILAB that simplifies the development of agent based applications, where the agent platform can be distributed across several machines (Heterogeneous OS) and the configuration can be changed at run-time by moving agents from one machine to another one, as and when required. JADE is written entirely in Java [13], [27]. It publishes their services in DF-Agent-Description as defined by the FIPA specification [28]. A DF Agent-Description includes one or more service-descriptions, each one describing a service provided by the registering different agents used in ANSAP where MA match IDs of APs recipient using the DF. A service-description typically specifies, among others, one or more ontology that must be known to access the published service.

The FIPA Agent Communication Act uses a seven-layer model from the application layer of the classical OSI reference model. The sub-layers include, in ascending order; Transport, Encoding, Messaging, Ontology, Content Expression, Communication Act and Interaction Protocol (IP) [29]. The layered architecture is geared towards optimizing communication performance between agents in MAS [30]. The chosen platform for design and implementation is the JADE-LEAP [25], [31] framework because it enables developing agents on mobile device.

7. CONCLUSION

In this paper, we have proposed an agent Notification System to track the Authentication process in real time, to make it more flexible and reliable. The use of Agent technology is the next direction for computing, especially the mobile platform that has low resources and runs on ubiquitous wireless networks to help the system to reach owner. Agents have come to stay and to change the client-server approach, as mobile agents allow the processing of information to be done locally, instead of transmitting the data over a network thereby reducing the network overload.

REFERENCES

[1] Loredana Ciurlau, "Control Of The Company's Performance Through The Dashboard", *ACADEMIC BRÂNCUŞI*, ISSN 2344 – 3685/ISSN-L 1844 – 7007, Special Issue, volume II/2016.

[2] Teddy Mantoro, Andri Zakariya, "Securing E-Mail Communication Using Hybrid Cryptosystem on Android-based Mobile Devices ", *Telecommunication Computing Electronics an Control* (*TELKOMNIKA)*, Vol.10, No.4, pp. 827~834, ISSN: 2087-278X, August 2012.

[3] Touraj Khodadadi, A. K. M. Muzahidul Islam, Sabariah Baharun, Shozo Komaki, "Evaluation of Recognition-Based Graphical Password Schemes regarding Usability and Security Attributes," *International Journal of Electrical and Computer Engineering (IJECE),* Vol. 6, No. 6, pp. 2939~2948, December 2016.

[4] Seetha Ranganathan, R. Saravanan, «Password Authentication for Multicast Host Using Zero Knowledge Proof," *International Journal of Electrical and Computer Engineering (IJECE),* Vol. 5, No. 6, pp. 1468~1471, , December 2015.

[5] Kameswara Rao, Sushma Yalamanchili, "Novel Shoulder Surfing Resistant Authentication Schemes using Text Graphical Passwords," *International Journal of Information and Network Security (IJINS),* Vol. 1, No. 3, pp163-170, 2012.

[6] Hang Tu, "A Security Enhanced Password Authentication and Update Scheme Based on Elliptic Curve Cryptography," *TELKOMNIKA Indonesian Journal of Electrical Engineering and Computer Science (IJEECS),* Vol. 12, No. 10, pp. 7353-7360,2014, ISSN: 2302-4046.

[7] Dilli Prasad Sharma, "Mobile Agent-Based Authentication: A Model for User Authentication in a Distributed System," *International Journal of Computer Applications* (0975 – 8887), Volume 112 – No 13, February 2015.

[8] D. Liu, B. Yang, and K. Yang, "Migration Strategies Of Mobile Agent Based On The Itinerary Graph," *Journal of Computer Research and Development*, China, 838-845. 2003

[9] L. Xue, Z. Zhou and Q. Liu, "A Novel Communication Mechanism of Mobile Agent System," *International Workshop on Education Technology and Training & International Workshop on Geoscience and Remote Sensing*. 2008.

[10] T. Hsieh-Chang, and H. Jieh, "An Architecture And Category Knowledge For Intelligent Information Retrieval Agents" *Decision Support Systems*, 255-268. May 2000.

[11] R. Gary, D Kotz, G. Cybenko, D. Rus, "D'Agents: Security In A Multiple Languages, Mobile-Agent System," In G.Vigna, editor, Mobile agent and security, volume 1419 of LNCS. *Springer* 1998.

[12] David Chess, Colin Harrison, and Aaron Kershenbaum, "Mobile Agents: Are They are a Good Idea?", IBM Research Report.

[13] F. Bellifamine, G. Caire, and D. Greenwood, "Developing The Multi-Agent System With JADE," England: John Wiley & Sons Ltd. 2007.

[14] M. R. Genesereth and S.p. Ketchpel, " Software Agent," *Communications of ACM*, vol. 37(7), 1994, pp48-53.
[15] Iqbal S, & Bailey, B. P, "Effects Of Acute Notification Management On Users And Their Tasks." *CHI'08 Proceedings of the SIGCHI Conference on Human Factors*. 2008.
[16] Ala' Khalifeh, Salem Al-Stash, Rabi Tanash, Mahmoud AlQudah, " Deploying Agents for Monitoring and Notification of Wireless Sensor Networks," *IEEE 28th International Conference on Tools with Artificial Intelligence,* 2375-0197/16 $31.00 © 2016 IEEE, DOI 10.1109/ICTAI.2016.115, 2016.
[17] Saqib Rehan Ayyubi, Taha Selim Ustun, Yuan Miao, "Grid Planning: Agent-Based Approach for Early Notification of Air Conditioning Loads to Smart Grid," *IEEE 10th Conference on Industrial Electronics and Applications (ICIEA),* 978-1-4799-8389-6/15/$31.00_c 2015 IEEE, 2015.
[18] Marjan Gusev, Sasko Ristov, "Alert Notification as a New Model of Internet-based Transactions," *22nd Telecommunications forum TELFOR*, 978-1-4799-6191-7/14/$31.00_c 2014 IEEE, 2014.
[19] A. Adi, Z. Denfgyin, L. Haibo, "M-Learning In Review: Technology, Standard And Evaluation," *Journal of Communication and Computer*, USA, Vol. 5, No. 11, pp. 1-6, Nov. 2008.
[20] A. Vochin, «History of Mobile phone," Retrieved from http://gadgets.softpedia.com/newsPDF/History-of-Mobile-Phones-3578.pdf.
[21] Google Alerts. http://www.google.com/alerts
[22] N. Wright etal, "Do You See Your Password? Applying Recognition To Textual Passwords ", *in Proceedings of the Eighth Symposium on Usable Privacy and Security*, pp. 8, 2012.
[23] R. Biddle, etal, "Graphical passwords: Learning from the first twelve years," *ACM Computing Surveys (CSUR),* vol. 44, pp. 19, 2012.
[24] M. Sreelatha, M. Shashi, M. Anirudh, Md. Sultan Ahamer, V. Manoj Kumar, "*Authentication Schemes for Session Passwords using Color and Images," International Journal of Network Security & Its Applications (IJNSA),* Vol.3, No.3, pp 111-119, May 2011.
[25] Z. Chaouch, & M. Tamali, "A Mobile Agent-Based Technique for Medical Monitoring (Supports of Patients with Diabetes)," *International Journal of Computational Models and Algorithms in Medicine*, 4(1), 17-32, 2014.
[26] S. Balakrishnan, & K. Shunmuganathan, "An Agent-Based Collaborative Spam Filtering Assistance Using JADE," *International Journal of Applied Engineering Research*, ISSN 0973-4562, Volume 10, Number 21, 42476-42479, 2015.
[27] F. Bellifemine, F. Bergenti, G. Caire and A. Poggi, "Jade – A Java Agent Development Framework." *Springer,* 125–147, 2005.
[28] W. Gray, ORMLite. http://ormlite.com/javadoc/ormlite-core/doc-files/ormlite.html.2016.
[29] N. Collins, Udanor, and O. Oparaku, "A Model of Intelligent Mobile Learning System using Multi-Agent Systems," *Germany, Lambert Academic Publishing*, ISBN 978-3-659-44209-4, 93-106, 2013.
[30] S. Poslad, "Specifying Protocols For Multi-Agent System Interaction." ACM Trans. Autonom.2007.
[31] A. Moreno, A. Valls and A. Viejo, "Using JADE-LEAP to Implement Agents In Mobile Device." *TILAB "EXP in search of innovation*": http://jade.tilab.com/papers-exp.