Multi-Agent Based Security Framework for E-Government in Recently technology Developed Countries

Dr. Enas Hadi Salih[1], Sinan Adnan Diwan[2], Ammar J. Fattah[3]

1 Software Engineering, Al-Rafidain University College, Baghdad, Iraq
2 Computer Science, Wasit University, Wasit, Iraq
2 Online Research Center, Science Gate Virtual University

*E-mail of the corresponding author: jabbara@sciencegate2all.com

Abstract

E-Government is an environment where government produces services to citizens electronically, this is beside services to other e-Governments, and one crucial factor regarding the reliability of accepting services provided by e-Government is the security factor.

This work is targeting Countries in their developing process that need to develop configurable management model, that capable of adapting security technologies to other factors revealed from the society. The configuration of this management model will be autonomously built up through the association of three domains presented by this proposal: policies, measures and infrastructure. Along this work; ontology will be built up to accommodate these domains and eventually to grant Agent software the ability to perceive the environment and configure the management model for deploying security technologies.

Keywords: Socio-Techno, Java Agent, Security policy, eGovernment, JADE, Ontology, knowledge development.

1. Introduction

E-government describes the use of technologies to facilitate the operation of government and the disbursement of government information and services. E-government, short for electronic government, deals heavily with Internet and non-internet applications to aid in governments. E-government includes the use of electronics in government as large-scale as the use of telephones and fax machines, as well as surveillance systems, tracking systems such as RFID tags, and even the use of television and radios to provide government-related information and services to the citizens.[WiKi]

Studies have shown that there is a link between security issues, e-government and management .[Dhillon, G. and Backhouse, J. (2001) , Dhillon, G. and Torkzadeh. (2006), Heeks, R. (2003), Heeks, R. (2006)., , M. T. and Oinas-Kukkonen, H. (2007)] Studies have also shown that non-technical issues are as important as technical issues in safeguarding an organization’s sensitive information.[Dhillon, G. and Backhouse, J. (2001), Heeks, R. (2006)] The importance of non-technical issues related to security management, however, is de-emphasized in many studies which tend to be quantitative by nature.[Heeks, R. (2006), Peter T. Knight (2007)] Particularly, with respect to developing countries, organizational culture, environment and level of awareness and how these factors relate to generic attitudes towards information security and its management.

On the highest level of abstraction, the very first step is to select the specific application domain and to determine, on a very coarse grained level, the key players within that domain (i.e. involved participants with their respective roles and responsibilities as well as strategic decisions and constraints having to be born in mind). In the next step, the respective underlying governmental and administrative model can be sketched. It is important to set up this general frame for the development of any e-Government system, because once (most reasonably at the beginning of the project) the underlying requirements and goals have to be made clear and visible to every party being somehow involved during the development process.[von Solms, B. (1999), Peter T. Knight (2007), Jonathan Sofian's (2011)]

E-Government strategy identifies interior's e-Government mission and vision, guiding principles, goals and objectives, and strategies. It also provides an overview of the strengthened governance structure and processes to manage the implementation of e-Government at the ministry level.[von Solms, B. (1999), Wimmer, M. & Bredow, B. (2002), Luis f, Luna-Reyes, Jing Zhang, J. Ramon Gil-Garcia and Anthony M. Cresswell]. The strategy also includes certain "enabling technologies"' in its definition of e-Government. These enabling technologies include, but are not limited to: the internet; personal digital assistants; handheld and remote wireless devices; integrated call centers; and machine-to-machine devices. [von Solms, B. (1999), Wimmer, M. & Bredow, B. (2002), Peter T. Knight (2007)]

2. Java Agent Development Framework (JADE)

JADE is the most widespread Agent-oriented middleware and it is a completely distributed middleware system with a flexible infrastructure allowing easy extension with add-on modules. The framework facilitates the development of complete Agent-based applications by means of a run-time environment implementing the life-cycle support features required by Agents, the core logic of Agents themselves, and of language features.[Wimmer, M. & Bredow, B. (2002)] figure (1) presents Agent Management reference model used by JADE environment

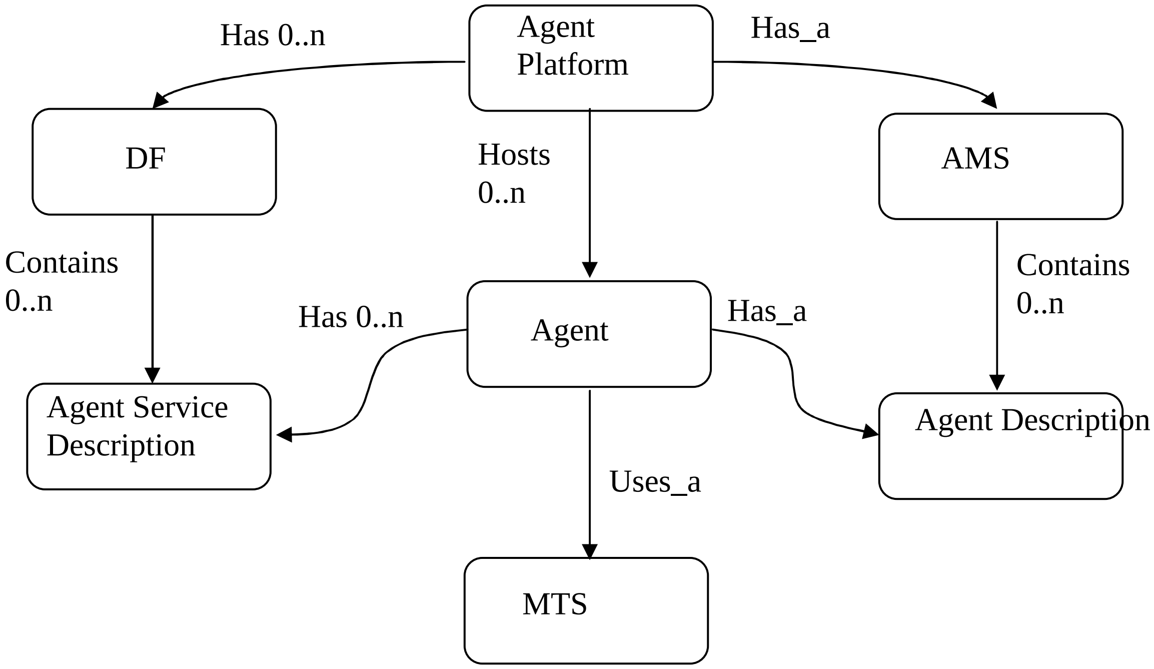


Figure 1 : Java Agent Development Platform Components

From figure(1) main components of the model can be briefly described as the following:

- Agent Platform (AP): Agent physical infrastructure in which Agents are deployed, this component includes machines, operating systems, FIPA agent management components, Agents.
- Agent: computational process that inhavits an AP and typically offers one or more computational services that can be published as a service description.
- Directory Facilitator (DF): the DF is an optional component of an AP providing yellow pages services to other agents. It maintains an accurate, complete and timely list of agents and must provide the most current information about agents in its directory on a non-discriminatory basis to all authorized agents. An AP may support any number of DFs which may register with one another to for federations. [R. Bordini, L. Braubach, M. Dastani, , J. Sanz, J. Leite, G. O'Hare, A. Pokahr, and A. Ricci, (2006), Wimmer, M. & Bredow, B. (2002)]

3. Proposed Multi-Agent Framework

This paper is introducing a framework for a multi-agent based eGovernment scheme in recently developed countries (i.e., countries that recently are deploying modern technologies). Figure (2) presents the conceptual diagram of the management model for security technologies, main components of this model is:

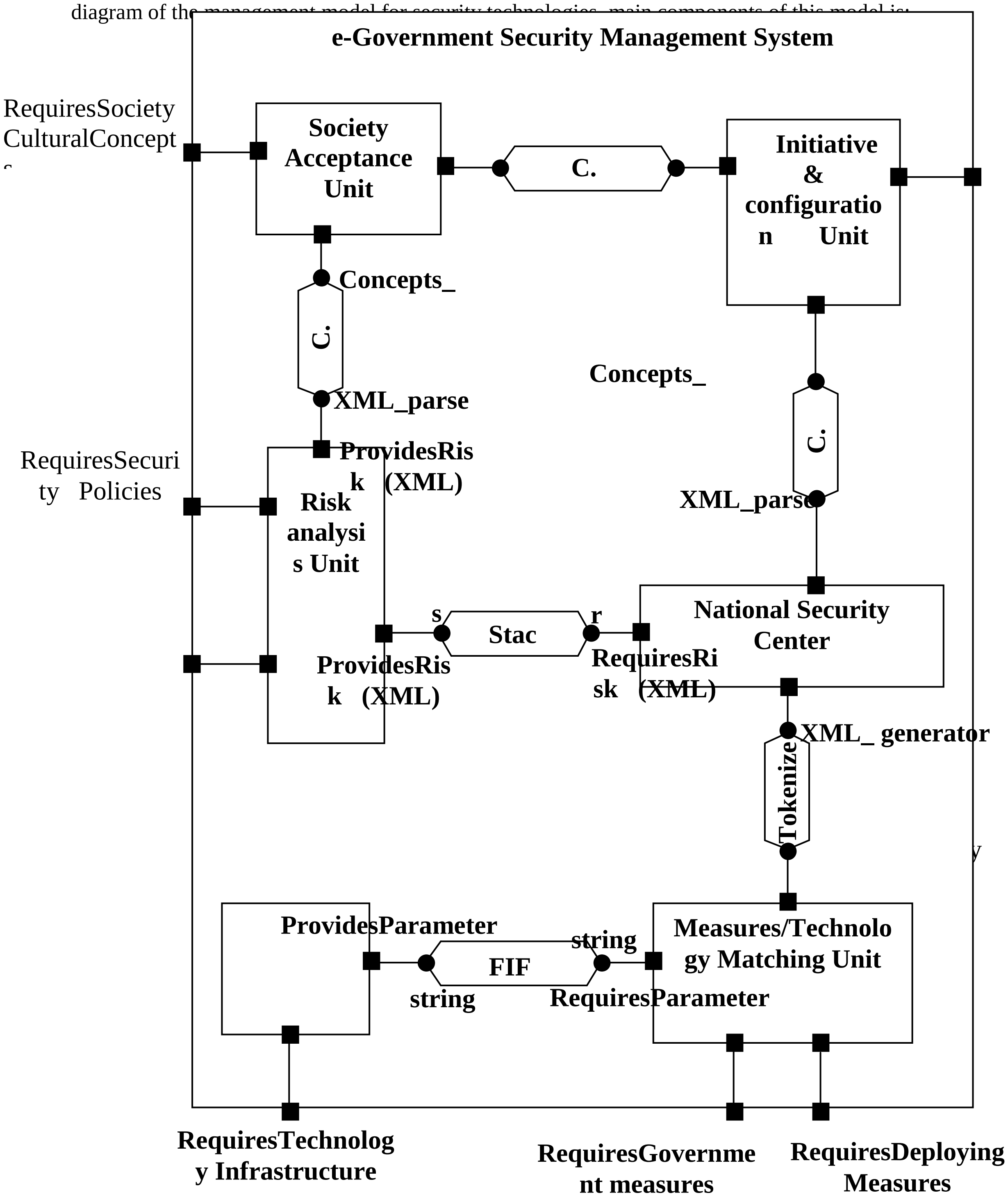

e-Government Security Management System
RequiresSociety CulturalConcepts
Society Acceptance Unit
C.
Initiative & configuration Unit
Concepts_
C.
XML_parse
Concepts_
C.
XML_parse
RequiresSecurity Policies
ProvidesRisk (XML)
Risk analysis Unit
s
Stac
r
National Security Center
ProvidesRisk (XML)
RequiresRisk (XML)
XML_ generator
Tokenize
y
ProvidesParameter
string
FIF
string
RequiresParameter
Measures/Technology Matching Unit
RequiresTechnology Infrastructure
RequiresGovernment measures
RequiresDeploying Measures

Figure 2 : Conceptual Architectural View to Multi-Agent Security scheme in eGovernment

1- **Social Acceptance unit:** this unit will consider the pairing security technology with society cultures (socio-technology). Ontology is designed and implemented to grant software agents' system the ability to perceive in this domain and eventually to make decisions (i.e., rating current deployed security policy). The ontology designed for the Multi-Agents in this scheme considers social factors and parameters revealed by the society expertise, sociological doctors and statistical analysis of population policies in their normal daily activities, and these social factors are involved closely in proper security policy deployment as figure (2) presents.

2- **Risk analysis Unit:** this unit is conceptualized security policies according to conceptualization model built upon ontology; this ontology is designed based on national and social concepts. Successful security policy is that one which brings citizens' trust to electronic government web sites; this is from a side and it should cope with security metrics on the other side.

3- **National security Unit:** ontology is designed over national security concepts of the country being developed, constitutional concepts and political concepts should be included, and other concepts will be added upon practical analysis to field data collected in deploying this framework.

4- **Technology Infrastructure Unit:** this unit is responsible on conceptualizing existing technology infrastructure, basically, this will include communication technology, government ministries technology, public sector technologies, software products , accounting systems and others.

5- **Measures / technology matching Unit:** this unit is considering ministries protocols and scenarios in providing services to each other (Ministry-to-Ministry) or services provided from the ministry to citizens (Ministry-to-Citizen)

4. Proposed Security Ontologies

1- Governmental web site authentication and counterfeit ontology
2- Session authorization and investigation ontology
3- Governmental security measures ontology
4- Technology social acceptance ontology
5- Third party technology complying and assessment ontology
6- Mobile investigators ontology

4.1 Governmental web site authentication and counterfeit ontology

- $\forall web\ \exists! agent\ \ (\ Request(web)\ \rightarrow\ Start(agent)\ AND\ Bind(web, agent)\ )$
- $\forall client\ \exists! token\ \ Register(client, token)$
- $\forall client\ \exists! token\ \exists\ key\ Encrypt(token, key)\ AND$
  $\exists address\ \ Private(client, address) \rightarrow Send(\ address, URL_{LINK})$.
- $\forall web\ \ \forall client\ \ \exists!\ token\ (\ \ Authenticate\ (client,\ token)\ AND\ Login(web, client)\ )$
- $\exists agent\ \forall x\ (\ Identify(agent, x)\ AND\ (x\ \in G\_AGENTS\ ) \rightarrow Authenticate(web))$

4.2 Session authorization and investigation ontology

- $\forall agent\ \exists\ token\ Bind(agent, token)$
- $\forall web\ \exists! token\ Bind(agent, token)\ AND\ Authorize(token) \rightarrow Authorize(\ agent)$
- $\forall agent\ (\ Active(agent)\ AND\ Social(agent)\ \rightarrow\ Knowledgeable(agent)\ AND\ Aware(agent)\ \ )$
  $\exists event\ \exists agent\ \ (Respond(event, agent)\ AND\ Aware(agent)) \rightarrow$
- $(event\ \in AUTHORIZATION - SET\ )\ \ )$

4.3 Governmental Security Measures ontology

- $\exists securityPolicy\ \exists agent\ \ \ (\ (\ Perceive(securityPolicy, Agent)\ AND$
- $Mobile(agent)\ ) \rightarrow Inspector(agent)\ )$
- $\forall agent\ (\ Active(agent)\ AND\ Social(agent)\ \rightarrow\ Knowledgeable(agent)\ AND\ Aware(agent)\ \ )$
  $\forall securityPolicy\ \exists agent\ (\ Aware(agent) AND\ Inspector(agent) \rightarrow$
- $Assess(securityPolicy, agent\ )$

5. The Proposed Agent, Knowledge Evolution and Sociality

The essential objective of software intelligent agent models is to establish computer based architecture through which agent properties are satisfied. In theory agent entity has significant properties such as autonomy, reactivity, sociality and pro-activeness and these properties impose utilizing more sophisticated concepts of knowledge evolution and ontological approach to interact the environment.

This paper focuses on the sociality property of intelligent agent due to the great effect reflected by this property on the knowledge development scheme. For an agent to be social it means its capability to take on roles, play roles, and locate in some society organization at all time. This paper abstract sociality in agent world as the ability to participate sessions where knowledge can be developed, as the following equation:

$$\forall i\, \exists j \begin{pmatrix} Social(agent_i , agent_j) \wedge (i \neq j) \rightarrow \forall event\ DevKnow(event, agent_i) \\ \wedge\, DevKnow(event, agent_j) \end{pmatrix} \qquad \text{Eq.1}$$

eq.1 satisfies if and only if the following constraint applied

constraint

$$\boxed{\forall event\ \exists agent\ \ Know(event, agent)\ \wedge (agent\ )}$$

if constraint.1 is not satisfied then a learning phase is requested to get knowledge about event failed to fulfill the constraint.

6. User Activities Interpretation

Let $c_{ref} = \sum_1^N e_i . x^i$, a vector of events that composed axiom concepts; these events are collected in ideal trusted session; or approved by the proposed system along

$c_{tst} = \sum_1^K e_i . x^i$, a vector of windows messages obtained during running session.

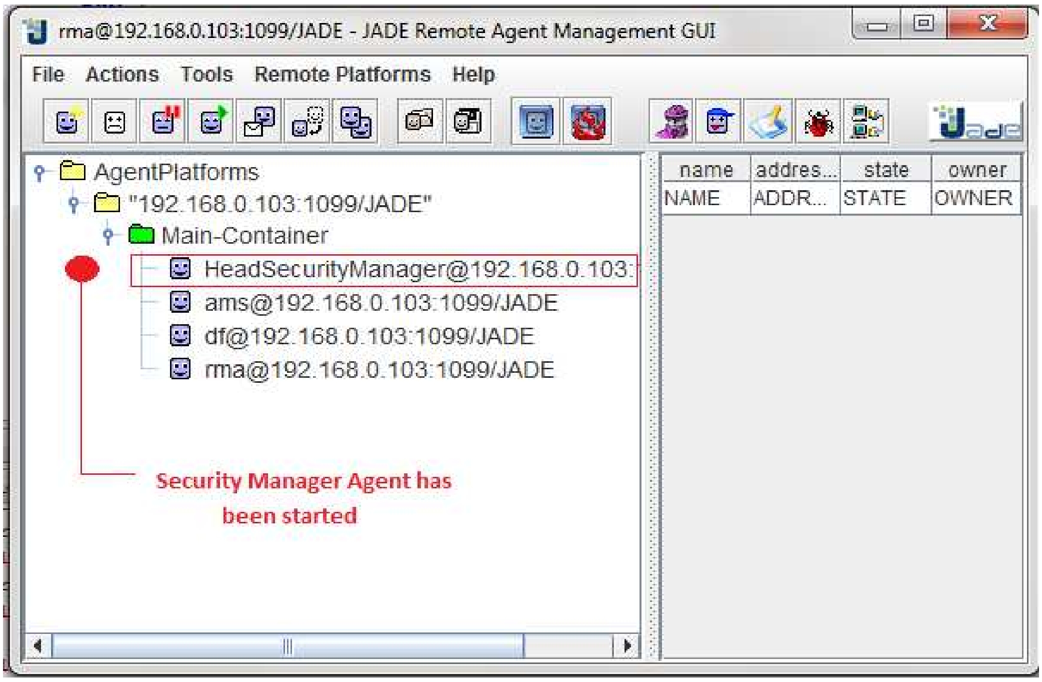
We define the following formulas:

- $\exists(c_{ref}, c_{tst})\ \boldsymbol{PerfectSimilar}(c_{ref}, c_{tst}) \leftrightarrow \big(Length(c_{ref}) == Length(c_{tst})\big) \wedge \forall(i \in Length)\ (c_{ref}^i == c_{tst}^i)$

- $\exists(c_{ref}, c_{tst})\ \boldsymbol{StructuralSimilar}(c_{ref}, c_{tst}) \leftrightarrow \forall(i \in S : S \subset c_{ref}, c_{tst})\ (c_{ref}^i == c_{tst}^i)$
- $\exists(c_{ref}, c_{tst})\ \big(\boldsymbol{Realize}(c_{ref}) \equiv \boldsymbol{Realize}(c_{tst})\big) \rightarrow \boldsymbol{FunctionalSimilar}(c_{ref}, c_{tst})$

7. Implementation Scenario

The first Agent to be fired up is in ‘National Security Center’ where the decisions to what security policy is deployed are taken. Figure (3) presents the JADE RMA agent starting window; in this figure four essential Agents have been started AMS, DF, RMA and the most important one is HeadSecurityManager Agent.


rma@192.168.0.103:1099/JADE - JADE Remote Agent Management GUI
File
Actions
Tools
Remote Platforms
Help

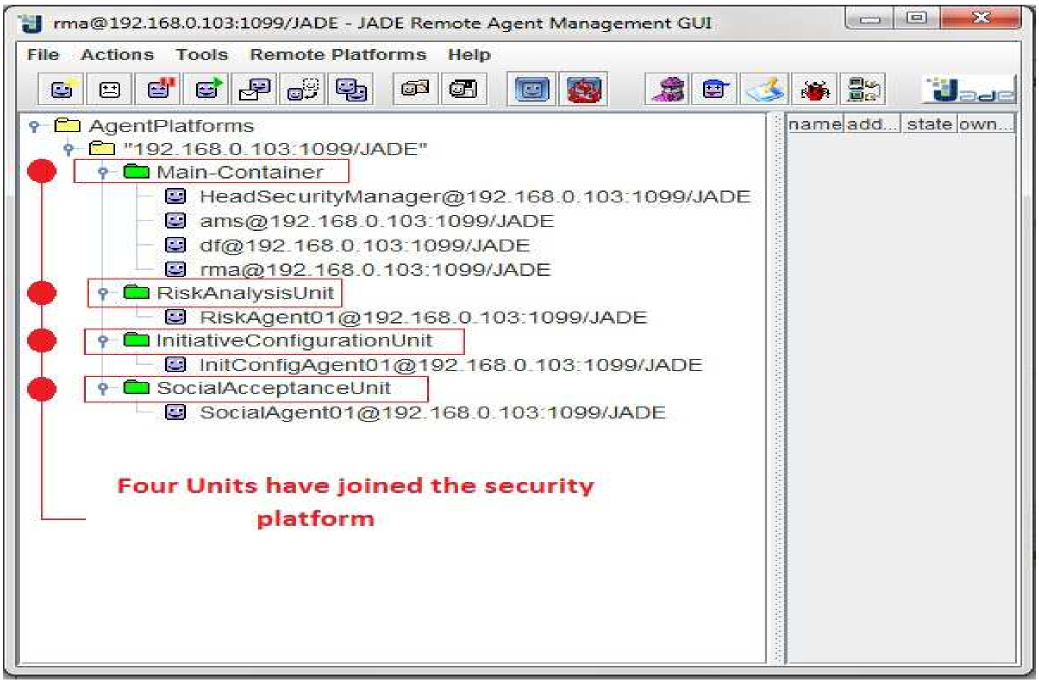
```
AgentPlatforms
  "192.168.0.103:1099/JADE"
    Main-Container
      HeadSecurityManager@192.168.0.103:
      ams@192.168.0.103:1099/JADE
      df@192.168.0.103:1099/JADE
      rma@192.168.0.103:1099/JADE
```

name	addres...	state	owner
NAME	ADDR...	STATE	OWNER

Security Manager Agent has been started

Figure 3 : JADE GUI starting Window with HeadSecurityManager Agent Started

Conceptual units represented in the conceptual view figure are implemented as Agent containers, and these containers are to have at least one Agent but it could have many of them. Figure (4) presents four containers constructed within the platform; in this demonstration all containers are constructed within the same platform and on the same machine but it could be easily developed to work in a multi-platform scheme.


rma@192.168.0.103:1099/JADE - JADE Remote Agent Management GUI
File
Actions
Tools
Remote Platforms
Help

```
AgentPlatforms
  "192.168.0.103:1099/JADE"
    Main-Container
      HeadSecurityManager@192.168.0.103:1099/JADE
      ams@192.168.0.103:1099/JADE
      df@192.168.0.103:1099/JADE
      rma@192.168.0.103:1099/JADE
    RiskAnalysisUnit
      RiskAgent01@192.168.0.103:1099/JADE
    InitiativeConfigurationUnit
      InitConfigAgent01@192.168.0.103:1099/JADE
    SocialAcceptanceUnit
      SocialAgent01@192.168.0.103:1099/JADE
```

name	add...	state	own...

Four Units have joined the security platform

Figure 4: Four Containers are constructed with the Platform

Figure (5) presents stack of technologies implemented by all Agents in the proposed scheme, where Agents need to communicate with other Agents on different Messaging protocol levels due to different network architectures available in eGovernment, for example Agents could be hosted on the same LAN segment within a ministry or on different locations in separate buildings.

In figure (5) SOAP MTP layer is added to the stack in order to grant Agents the ability to communicate Web services over the Internet due to the revolutionary development in web application methodologies and technologies.

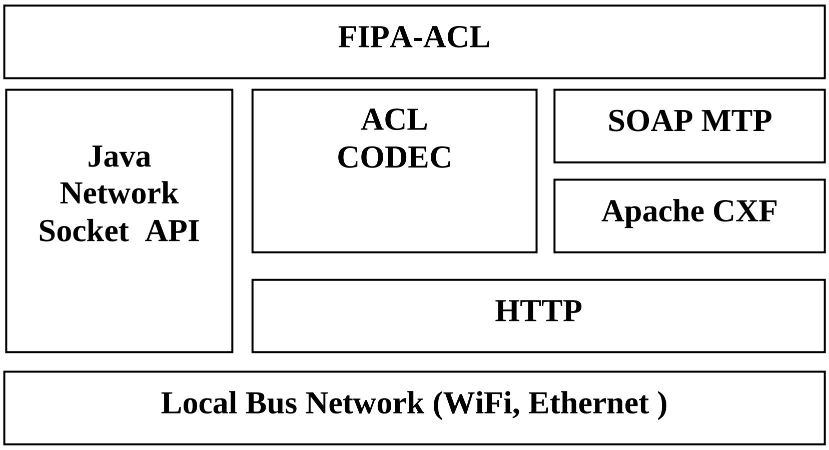
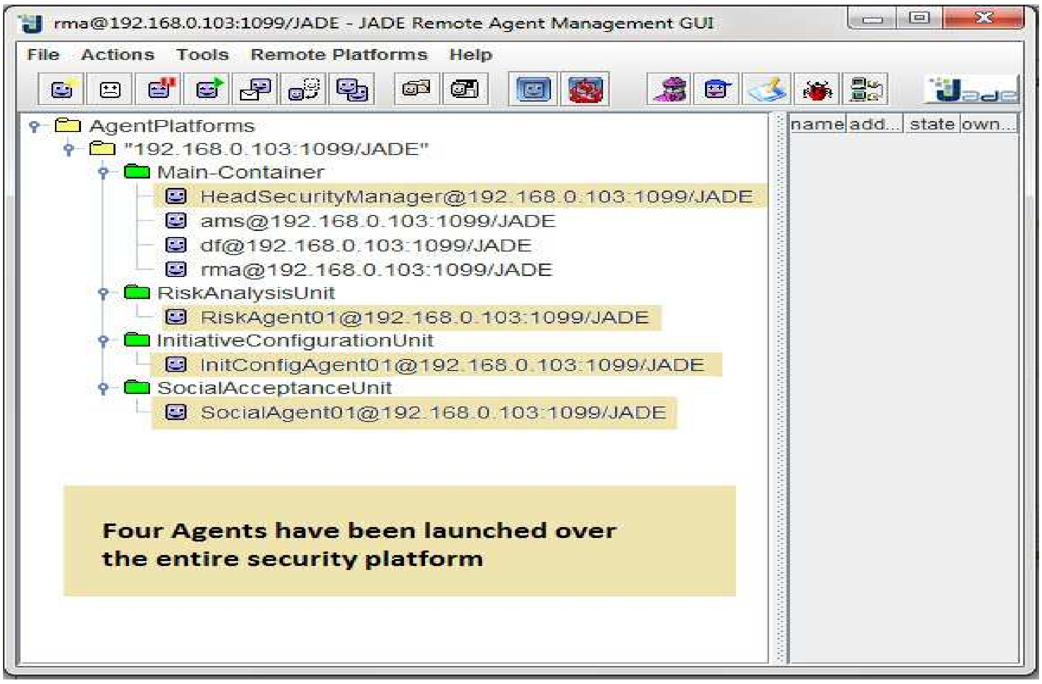


Figure 5: Message Exchange Protocols Stack In Proposed Framework

Figure (6) shows four Agents are fired up inside platform containers; this is producing Agent community that can interact with each other using message protocol stack presented in figure (7). In this paper the framework has been implemented on LAN segment with each container resides in separate computer station.


rma@192.168.0.103:1099/JADE - JADE Remote Agent Management GUI
File
Actions
Tools
Remote Platforms
Help
name
add...
state
own...

AgentPlatforms
"192.168.0.103:1099/JADE"
Main-Container
HeadSecurityManager@192.168.0.103:1099/JADE
ams@192.168.0.103:1099/JADE
df@192.168.0.103:1099/JADE
rma@192.168.0.103:1099/JADE
RiskAnalysisUnit
RiskAgent01@192.168.0.103:1099/JADE
InitiativeConfigurationUnit
InitConfigAgent01@192.168.0.103:1099/JADE
SocialAcceptanceUnit
SocialAgent01@192.168.0.103:1099/JADE

Four Agents have been launched over the entire security platform

Figure 6: Four Agents fired up in the Proposed Framework

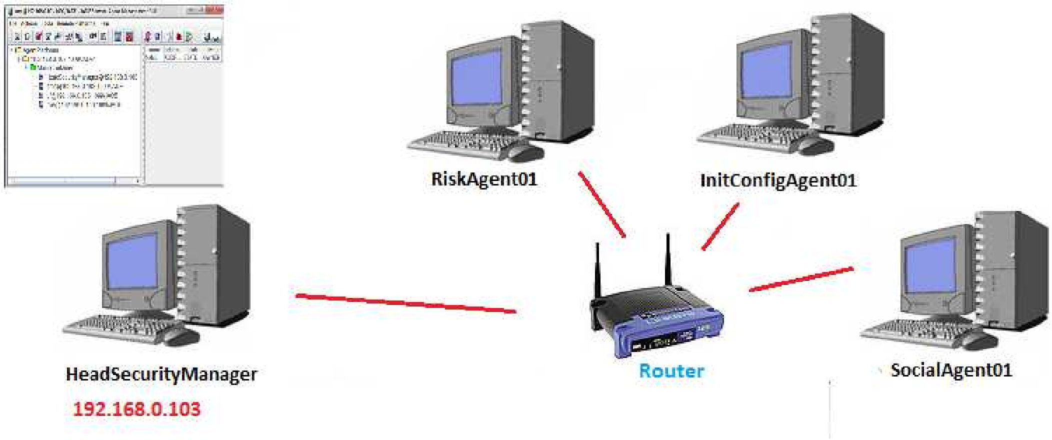


Figure 7: Network Infrastructure to test the Proposed Framework

Figure (8) presents complete interaction session among all Agents within the platform, the initiation is established from the configuration unit by sending security policy to be considered by the HeadSecurityManager, and this one in his turn will consult Risk assessment unit for rating proposed security policy.

HeadSecurityManager in requesting rating factor also from social unit through consulting SocialAgent01

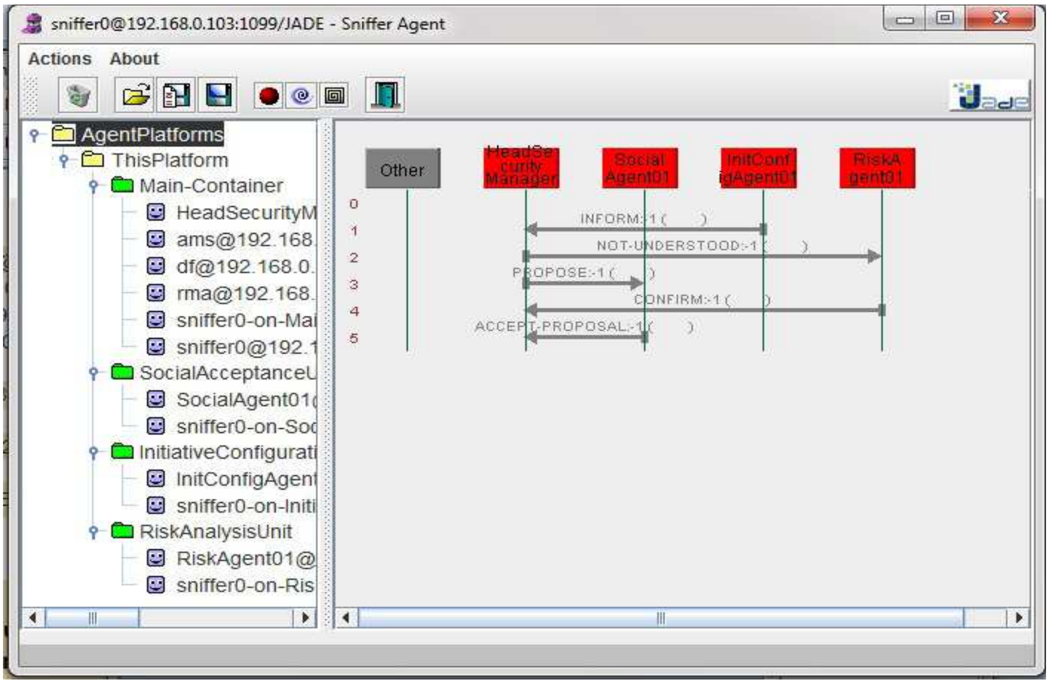


Figure 8: Complete Security Policy Assessment session

8. Conclusions

1. In recently technology developed countries there is a correlation between security policy employed by government web sites and the social acceptance to this policy. Social impact is extended over each of security factors used in eGovernment (i.e., Deploying Policy; Decision Making Scenario; Security Method; Request Mining and Authentication; Autonomous or Non Autonomous).
2. Agent social behavior can be recruited in a very effective manner in eGovernment security scheme where multiple official Agents can autonomously agreed on accurate, trusted and compatible security policy. eGovernment can broadcast to its Agencies over secure media a repository of trusted security policies.
3. Social impact measures are defined and considered along the design and implementation of official web sites (i.e., eGovernment websites) to recognize and grade different security methods ; this is done by statistically evaluate social acceptance of the deployed security policies and later on reveals new security measures. Measures are indications of accomplishing optimum management for policies, scenarios and strategies.
4. Cognitive interactions among distributed intelligent components abstracts security measures at different level of abstraction; this is due the structured knowledge that is crystallized along the interaction; this is the case when Java Agent has been recruited to accomplish the task of perceiving of the events occurred within the eGovernment infrastructure.
5. By abstracting the information flow and interpretation of these information to the conceptual level, less acceptable communities spread over new developed countries can be negotiated autonomously and their confidence to the new deployed technologies can be achieved.

9. References

http://en.wikipedia.org/wiki/E-Government

Dhillon, G. and Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, 11 (2), 127-153.

Dhillon, G. and Torkzadeh. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, 16, 293-314.

Heeks, R. (2003). Most eGovernment-for-Development Projects Fail: How Can Risks be Reduced? *iGovernemnt Working Paper Series*, Paper no. 14.

Heeks, R. (2006). *Implementing and Managing eGovernemnt.*

Siponen, M. T. and Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *SIGMIS Database*, 38 (1), 60-80.

von Solms, B. (1999). Information security management: why standards are important. *Information Management & Computer Security*, 7 (1), 50-57.

Wimmer, M. & Bredow, B. (2002), A Holistic Approach for Providing Security Solutions in e-Government, Hawaii International Conference on System Sciences, IEEE, USA.

Peter T. Knight (2007), Knowledge management and e-Government in Brazil, e-Brasil Project.

Jonathan Sofian's (2011), Socio Technology perspective for E-Government implementation in Indonesia.

Luis f, Luna-Reyes, Jing Zhang, J. Ramon Gil-Garcia and Anthony M. Cresswell, "Information systems development as emergent socio-technical change: a practice approach", USA

R. Bordini, L. Braubach, M. Dastani, , J. Sanz, J. Leite, G. O'Hare, A. Pokahr, and A. Ricci, (2006), A survey of programming languages and platforms for multiagent system, *Informatica*, vol. 30, pp. 33-44.