International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 5, Issue 1, January 2016 **ISSN 2319 - 4847**

Colored Petri Net (CPN) based Model for Hybrid Security Architecture based on Reputation for Secure Execution of Mobile Agents

Dr. Heman Pathak

Associate Professor, Department of Computer Science,
Kanya Gurukul campus, Dehradun

ABSTRACT

Mobile Agents (MA) are software programs that live in computer networks, performing their computations and moving from host to host as necessary to fulfil user goals. Security is an important issue for the widespread deployment of applications based on mobile agent (MA) technology. The major security threats are either threats against the hosts, or threats against the MA. This paper briefly introduces the Hybrid Security Architecture (HSA) inspired by the various existing security techniques including digital signature, encryption, intrusion detections, signed agreement, trust and others. Since all are well studied and experimented techniques, paper does not discuss all in details. This paper discusses the trust model based on reputation to provide security to both MA and executing host. In order to establish safe and secure communication between MA and hosts, each must be trusted that it would not harm other when it is given the access in a system. Paper presents a new way to compute reputation value of both host and MA based either on past experience or experiences of other trusted and known entities and third party. Reputation of host is evaluated by the previous experience of the MAs being executed on the host and also by using intrusion detection mechanisms.

Various components of the proposed architecture have been modelled by using Colored Petri Net (CPN) Tool. Once the model is constructed, various tools provided by CPN such as monitoring, state space and user controlled simulation have been used to check the correctness of the modelled system. Various data gathering and report generation tools have also been used to generate and collect the data required for analysis.

Keywords: Mobile Agent, Security, CPN

1. Introduction

Trust Management System based on reputation gained popularity in recent time for estimating the trustworthiness and predicting the future behaviour of nodes and other network entities in a large-scale distributed system where they interact with one another to share resources without prior knowledge or experience [1], [2]. Trust and reputation have gained importance in diverse fields such as economics, evolutionary biology, distributed artificial intelligence, grid computing, and agent technology, among others. Many researchers have proposed different approaches to compute Reputation Value (RV) to evaluate the trust worthiness of the entities involved. Approaches mainly differ based on the system model they have used, entity for which trust worthiness has been computed and area of application where this concept is to be used.

This paper evaluates the trust worthiness of MA and executing host based on their RV. An entity with high RV is treated as trusted while with low RV as malicious or suspicious. RV for both are evaluated and updated time to time by different components of the system interacting with these entities. Paper proposes a novel approach to compute RV for both MA and host. Hosts are protected against the attack of malicious host by only allowing the execution of trusted MA. Similarly MA is allowed only to be executed on trusted hosts.

2. Hybrid Security Architecture

HAS is the proposed model for the security of MA and the executing host. Basic model of HSA has been discussed in [8], [9]. HAS is inspired by the various existing security techniques including digital signature, encryption, intrusion detections, signed agreement, trust and others [3][4]. Since all are well studied and experimented techniques, paper does not discuss all in details. Details of reputation based trust management are discussed in [11]. This paper presents the CPN based modelling of basic model of HSA and its trust management concept based on reputation.

As discussed in [11] HSA divides the open network like internet into regions and then assigns the responsibility to one of the centralized component within the region to implement security features to protect malicious host and MA from

each other. HSA assumes that Internet is network of networks where networks are connected with each other via routers [7]. A MA wishes to visit a host within a network, first arrive at the router of the network and then passed to the designated host. Host in a network offer services and provide an executing environment to the MA. Routers are fault-free and trustworthy. Mobile Agent System is installed at each host and router to provide platform for MA. Various hardware components of the system are Router, Agent Server/Host and Local Shared Storage Space. Following section discuss the details of these components.

2.1 Router

Each MA enters in to a local network or migrates from the network via router. Fig-1 gives the details of components installed at router and their interactions with each other.

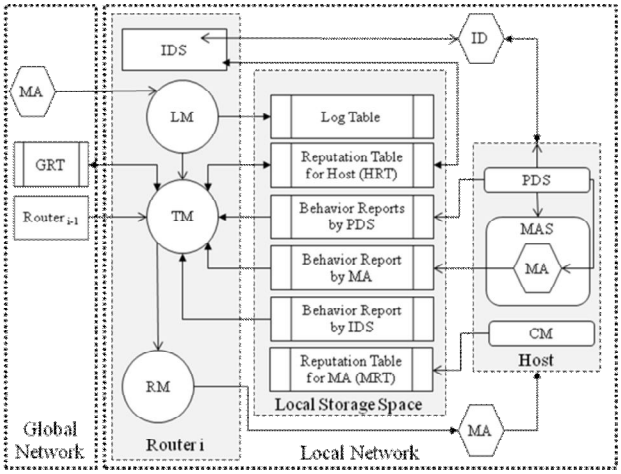

Figure 1: Different components of HSA and their Interaction with TM

Intrusion Detector System (IDS)

Each network evaluates the trust worthiness of all its hosts by the use of IDS. IDS installed at the router, randomly create intruder detectors (ID) and execute it on various hosts and record their behaviour. Behaviour reports are then analysed and RV of the host is updated.

Logging Manager (LM)

It records arrival and departure entry in log table for each MA received and migrated from the network.

Trust Manager (TM)

It is responsible for computing RV for all incoming and outgoing MA via router. It also maintains the RV of the hosts, part of the network [3].

Recovery Manager (RM)

It is responsible to initiate recovery procedure in case a MA or host is found malicious. Recovery procedure is not discussed in this paper but left for future work.

Host

Host is a computer in the network which offers services to the MA. It provides executing platform to the MA. Personal Domain Server (PDS)is a proxy server, installed at each Host. It watches the behaviour of MA and executing platform during the execution of MA and submits behaviour reports at the LSS.

Local Shared Storage Space (LSSS)

In each network there is a shared Local Storage Space (LSS), assumed to be fault free and trust worthy. This space is accessible by all hosts and components installed at router. It is used to store Log Table, behaviour reports of MA and Hosts, reputation table for MA and hosts, etc.

Global Reputation Table (GRT)

GRT is maintained by some server in the global network. It stores the list of MAs and their RVs that have been found suspicious or malicious by some watching entities. This table is concerned only when information gathered locally or from source router of MA is insufficient to make decision about the trust worthiness of MA.

Reputation Value Computation

RV for MA is collected by various components of the system and then appropriate weights are assigned to each RVs [4], [5], [6]. Mathematical computation among RVs and weights are used to compute new RV. RV is assumed to be in the range (1 to 9).

A. Reputation Value Computation for Host

Each host is initially assigned an average RV five (5). Behaviour of host is watched by its PDS and executing MA. IDS installed at router periodically launch Intruder Detectors (ID) to record the behaviour of hosts. These Behaviour

reports are used to update the RV of host. Host RV is computed locally and stored in HRT.

B. Reputation Value Computation for MA

The RV for a newly created MA is same as the RV of its base host. For an incoming MA, TM collects the RV of the MA from the last visited router. Local Reputation Table (LRT) for MA is also consulted to get the RV of incoming MA if it has previously visited the network. If these data are not sufficient then GRT is consulted to check whether MA has been tagged as suspicious or malicious by any of the entities. TM then analyse these data and compute new RV for the MA and if found trusted, passed to the target. If MA is found malicious, GRT is updated and MA is transferred to Recovery Manager. During the execution of MA its behaviour is observed by PDS. TM is responsible for analysing this report and to update the RV of the MA in the LRT.

3. COLORED PETRI NET (CPN) BASED MODEL OF HSA

CPN is a powerful tool for modelling complex systems [21], [22], [23], [24]. CPNs combine state and action into a single diagram through the use of tokens of various colors (colors can be thought of as data types) which reside in places (or states). Tokens move from one place to another through transitions. CPNs may be organized in hierarchical fashion to allow reuse and top-down or bottom-up development.

3.1 DESCRIPTION OF COMPONENTS OF HSA

In order to model the HSA, first the various components of the system are identified and then various tokens for the system are recognized. Various color-sets are used to represent various tokens and place types. This section represents the various level of model in brief. Table-1 represents the components of the system and the way they are represented in the system.

Table 1: Description of components of HSA for CPN model

Components	Description
Router	Every network has a router and it is identified by NetId
Host	A host within a network is identified by HostId
Packet	A packet consists of an Agent, sender NetId, destination NetId and type of agent.
Address	A host is identified by a two digit number. First digit for network and second digit for host.
Itinerary	It is an ordered list of addresses to be visited by MA and initialized at the time of MA is created.
Visited Itinerary	MA carries with it the ordered list of visited hosts, where MA has completed its execution.
Mobile Agent	Every MA is identified with unique AgentId. It carries its itinerary, visited itinerary and RV.
MRT	It is a Local Reputation Table of MAs visited the network.
HRT	It is a Local Reputation Table for all the hosts of network.
GRT	Global Network maintains a Global Reputation Table (GRT) for all the MA found malicious.
Log Table	It records the arrival and departure entry for all MA arriving at router.

3.2 Description of Networks

A hierarchical CPN has been used to model the HSA. The model uses some fusion places and substitution transitions as well for better representation of the components and their relations. Following section explains the design and working of each level of the hierarchy.

3.2.1 Global Network

This network page is used to model the global network through which packets are moved from one network to another.

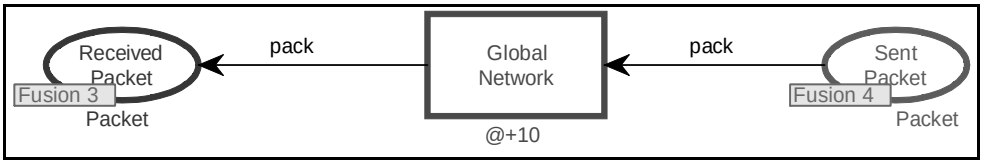

Figure 2: CPN page Global Network for HSA

At router before migration of MA, a packet is constructed and placed at place *SendPacket.* Similarly MA arrives at

place *Receivedpacket* in the packet form. Both places are fusion places so accessible to all routers. Transition *GlobalNetwork* is fired when there is a packet at source place. Transmission time of the packet may be fixed or random as per the requirement of the system.

3.2.2 *Router*

This network page models the functioning at Router. Its components are responsible for receiving and sending Agents. It contains two subpages *NewAgent* and *Host.*

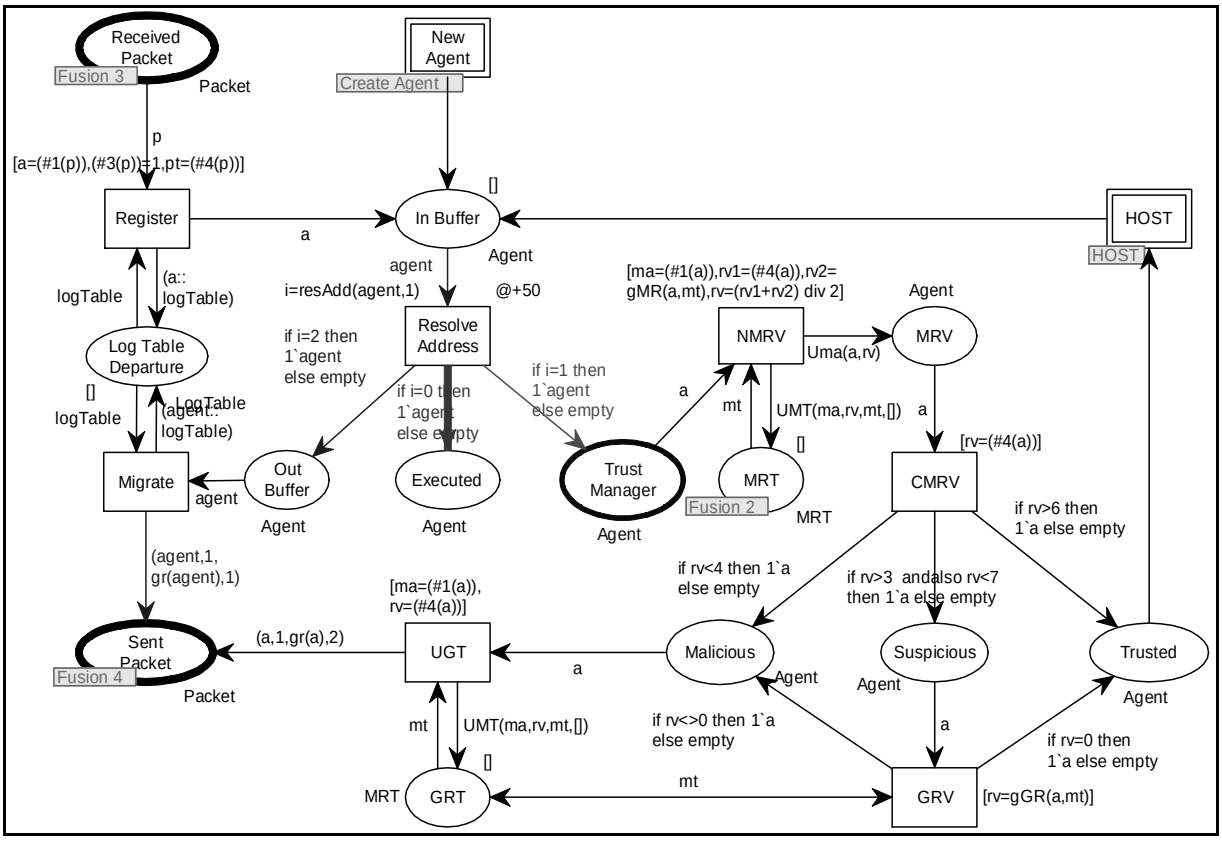

Figure 3: CPN page Router-1 of HAS which models the Local Network

- Place *ReceivedPacket* receives a packet from other part of the network.
- If target address of the packet is current network, transition *Register* is fired, which makes an entry in *LogTable*, and place the agent at place *InBuffe.*
- All MAs received, as well as created or executed by the hosts within the network are submitted at place *Inbuffer*.
- A token at place *InBuffer* fires the transition *ResolveAddress*, which perform following actions –
- If target address list is empty, MA has completed its itinerary and placed at place *Executed.*
- If next host to be visited by the MA is in the same network then agent is passed at place *TrustManager*.
    - A token at place *TrustManager* fires the transition NMRV, which collects the RV from local MRT (if any) and update RV of MA. MA with updated RV is placed at place *MRV.*
    - A token at place MRV fires the transition CMRV, which compute the trust worthiness of MA based on its RV and place it at place Trusted, Suspicious or Malicious.
    - A token at T*rusted* means MA is trusted and passed to sub-page *HOST.*
    - A token at place *malicious* fires the transition *UGT*, which updates the GRT and starts the recovery.
    - A token at place *Suspicious* fires the transition *GRV*, which concerns the GRT and update the status of malicious MA and place it at place *Malicious* or *Trusted.*
- If next host to be visited is in other network then agent is passed at place *OutBuffer*.
    - A token at *OutBuffe*r will fire the transition Migrate.
    - Before migration of MA, a departure entry is made in the *LogTable* departure. And packet is placed at place *ReceivedPacket*.

3.2.3 HOST

This network page models the execution of MA at host and Intrusion Detection System.

- A token at place *Trusted* fires transition *CheckHost*, which concerns HRT to check if the target host is trusted or not.
- If host is trusted MA is passed to place *Executing* else to the place *Waiting* where MA waits until target host becomes trusted again.

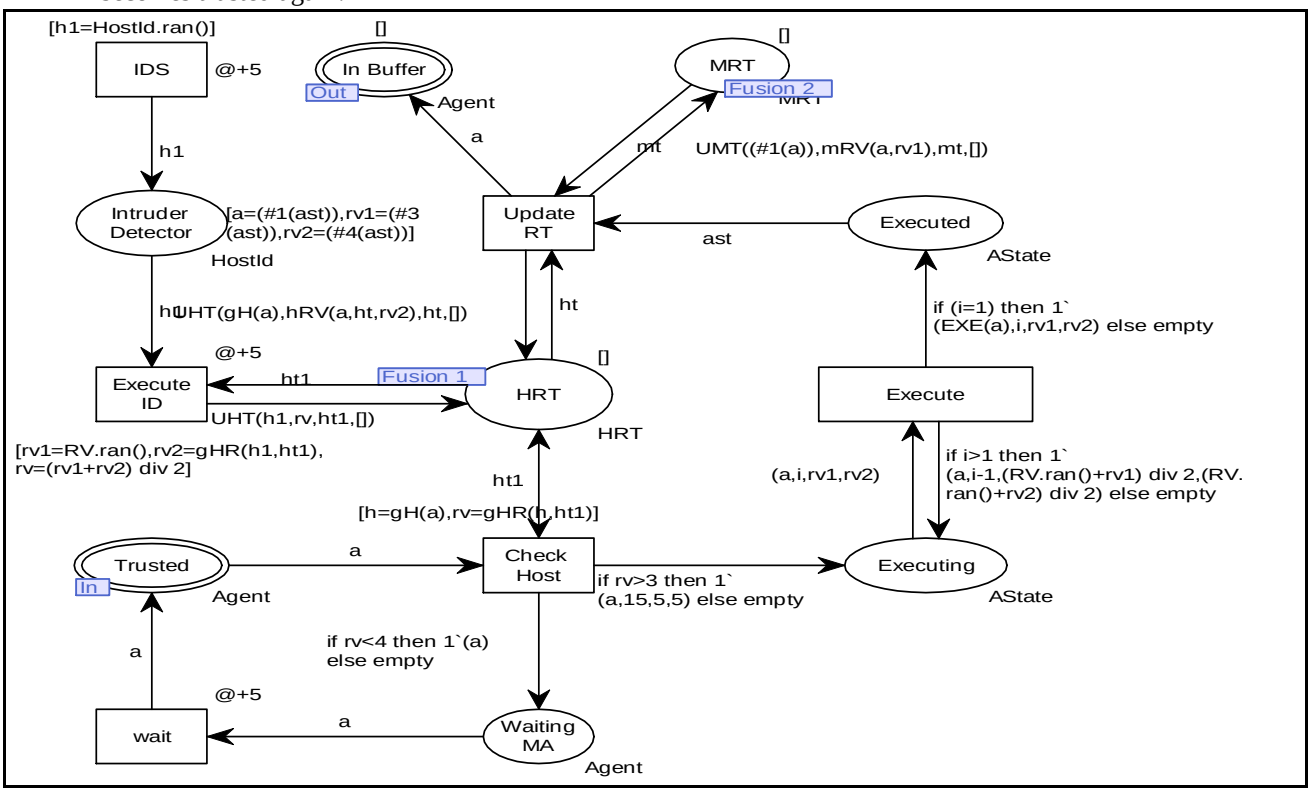

Figure 4: CPN page HOST of HAS which models the execution of MA

- Token at place *Executing*, fires the transition *Execute*, which model the execution of MA at the target host. It has been assumed that all MAs execute in fifteen steps at host.
- After execution MA arrives at place Execute and in turn fires the transition *UpdateRT*.
- In HSA behavior of host and MA are recorded during execution of MA and used to update their RV. To model this concept, random RVs are generated and modified in each steps of MA execution and used by transition *UpdateRT* to update RV of host and MA in their respective RT.
- MA is then placed at place *InBuffer* to continue its execution.

This network page also models the Intrusion Detection System of HSA installed at router.IDS has been modelled by the transition *IDS*. This transition periodically creates Intruder Detectors (ID) for randomly generated host. Again to model the behaviour report of host by ID, random RV is generated by transition *ExecuteId* and host RV is updated in HRT.

Table 2: Description of Places of CPN model for HSA

Place	Description	Type
GLOBAL NETWORK		
Sent Packet	Packets containing MA to be transmitted over Global Network.	Packet
Received Packet	Packets containing MA to be received through Global Network.	Packet
ROUTER		
LogTable	Maintains the record of all incoming and outgoing MAs at the Network.	Log Table
In Buffer	Contains all the MAs has been received, created or been successfully executed within Network.	Agent
OutBuffer	Contains all the MAs ready to migrate to other part of Network.	Agent
Trust Manager	Contains all the MAs to be executed within the Network.	Agent
Executed	Contains all the MAs has successfully completed their itinerary.	Agent
MRT	It is a fusion place to represent Local Reputation Table for MA.	MRT
GRT	It is a fusion place to represent Global Reputation Table for MA.	MRT

MRV	It contains MA with updated RV.	Agent
Malicious	It contains MA found malicious.	Agent
Suspicious	It contains MA found suspicious.	Agent
Trusted	It contains MA found trusted.	Agent
HOST		
Waiting	Contains the waiting MA whose host are not found trustworthy.	Agent
Executing	Contains executing MA together with remaining number of steps.	AState
Executed	Contains MA executed at host.	Agent
HRT	It is a fusion place for Local RT for Host.	HRT
Intruder Detector	Contains the HostId of the hosts for which ID has been created by IDS.	HostId

Table 3: Description of Transition of CPN model for HSA

Transition	Description
GLOBAL NETWORK	
Global Network	Pass a Packet from Sender to Receiver. Packet transmission time depends on type of Packet.
ROUTER	
Register	Log an arrival entry in LogTable for incoming MA. And pass the MA at InBuffer.
Resolve Address	It checks weather MA is to be executed within the network, to be migrated to other network or has completed its itinerary and being terminated.
Migrate	Send the MA to other Network but before migration launch a departure entry in log table.
NMRV	Concern MRTand update RV of MA.
CMRV	Checks the trust worthiness of MA based on RV.
GRV	Concern the GRT to update the status of suspicious MA and mark it as malicious or trusted.
UGT	Update the GRT if a MA is detected malicious.
HOST	Subpage for the execution of trusted MA.
HOST	
CheckHost	Checks the trust worthiness of the target Host.
Wait	Sends the MA in the waiting if host is not trusted.
Execute	Execute the MA until all its steps completed. And generate and modify RVs of host and MA.
URT	To update the RV of the MA and its executing Host based of their behaviour during execution.
IDS	Randomly creates ID for hosts periodically.
Execute Id	Execute the ID on the designated host and update its RV in HRT.

4. ANALYSIS AND RESULT

Once the model is constructed, several simulation runs have been used to check its correctness. Initial simulation runs used combinations of manual binding, play and fast-forward tool. Also the proper firing times of timed-transitions were noted. Once this procedure was followed for several runs, simulation using Mark-up Language code was done to generate concise simulation reports. Various data collector monitors were also used to gather statistics and to check certain properties of the CP Net. Results till this state show that most of the components of HSA are modelled correctly by CPN. Important results are still to be generated for performance analysis.

5. CONCLUSION

In the proposed architecture, only trusted MAs are transferred to the host and host gets protected from the attack of malicious MA. Also during the execution, behaviour of MA is recorded and CM saves the MA and its execution state in the LSS periodically. In case MA attacks the host during execution, this attack can be detected and RM can use the checkpoint data to bring the host in consistent state. Since MA is allowed only to be executed on trusted host, it gets protected from the attack of the malicious host. Even during the execution if it has been attacked, RM can rollback all MA execution and recover it from checkpoint data.

I have proposed an architecture which logically secure the MA and Host both from malicious attack. Various components of the system work collectively to provide solution to the said problem. Since the proposed architecture has

yet not been implemented or modelled, its practicality is still to be tested. Since most of the approaches used here are well known and has already been implemented successfully so it is quite reasonable to accept that, this architecture once implemented will solve the concern issues successfully. Its efficiency or comparative performance analysis is possible only after the implementation.

References

[1] De Capitani di Vimercati, S.Foresti, S.Jajodia et al. Integrating Trust Management and Access Control in Data Intensive Web Applications,ACM Transactions on the Web (TWEB) 6,2, 1-44 (2012).
[2] Habib S., Ries S., Muhlhauser, M., Towards a Trust Management System for Cloud Computing, In Proc. of IEEE 10th Int. Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom'11). Changsha, China (2011).
[3] K. Hoffman, D. Zage, C. Nita-Rotaru, A survey of attack and defense techniques for reputation systems, ACM Computing Surveys 42 (1)(2009) 1–31.
[4] M.T Nkosi, M.O Adigun, J.O Emuoyibofarhe, Agent-To-Agent Reputation-Based Trust Management, IADIS International Conference Applied Computing 2007.
[5] Noor T. H., Sheng Q.Z., Credibility-Based Trust Management for Services in Cloud Environments, In Proc. of the 9th Int. Conf. on Service Oriented Computing (ICSOC'11). Paphos, Cyprus (2011).
[6] O. Onolaja, G. Theodoropoulos R. Bahsoon,, A Data-Driven Framework for Dynamic Trust Management, Procedia Computer Science Procedia Computer Science 4 (2011) 1751–1760.
[7] Patel, R.B. Design and implementation of a secure mobile agent platform for distributed computing', PhD Thesis, Department of Electronics and Computer Engineering, IIT Roorkee, India, Aug 2004.
[8] Pathak H., A Novel Hybrid Security Architecture (HSA) to provide security to Mobile Agents and the Executing Host, Proceedings of the International Conference on Communication, Computing & Security Pages 499-502, Rourkela, 2011.
[9] Pathak H., A Novel Flexible and Reliable Hybrid approach to provide Security to Mobile Agents and the Executing Host, Proceedings of the International Conference on Electronics, Information and Communication Systems Engineering (ICEICE-2010), Jodhpur.
[10] Pathak H., Trust Model for Hybrid Security Architecture based on Reputation for Secure Execution of Mobile Agents in International Journal of Information and Computation Technology(IJICT), Vol.4, No.1, pp: 67-72, 2014.
[11] Pathak H., A Novel Approach to Compute Reputation Value for Trust based Hybrid Security Architecture for Mobile Agents" In the proceedings of International conference on Evolution in Science and Technology and Eyne on Educational Methodologies, Prannath Parnami Institute of Management & Technology Hisar, 8-9 March – 14.