International Journal of Computer and Information Technology (ISSN: 2279 – 0764)
Volume 9– Issue 4, July 2020

Enhancing Mobile Agent Security Level (Proposed Model)

Mohammad Al-sharaiah A.[1]
Department of Computer Science,
Faculty of Information Technology
University of Jordan, Jordan
Amman, Jordan
Email: m.abdullah [AT] ju.edu.jo

Mutaz Khazaaleh Kh.[2]
Department of Information Technology
Al-Balqa Applied University
Amman, Jordan
Email: mutaz.khazaaleh [AT] bau.edu.jo

Feras Haziemeh A.[3]
Department of Information Technology
Al-Balqa Applied University
Amman, Jordan
Email: haziemh.feras [AT] bau.edu.jo

Abstract— **Mobile agents are application design schemes for distributed systems that consist of mobile code ideology including Mobile agent software. In the last period mobile computing process had a vision that's a set of execution code that's move from platform to another in the heterogeneous network with an ability of carrying there result and updating them self-sate.**

This paper presents several enhancements on mobile agent security and provides generalized code protection. Several novel techniques are proposed to protect mobile agents in any environments and to describe and solve practical problems in the mobile agent system.

Keywords--- computer network, security, mobile agent, mobile agent security, encryption.

I. INTRODUCTION

A. *Computer Security Attack*

Any computer systems can be attacked by exploiting through potential vulnerability [1]. The threat can be done in many form or types. Masquerading, this attack can be described as someone claims the identity of another person. Denial of service attack, when agent attacks the platform the denial of service happens by running attack script to exploit system vulnerability, this attack give the agent the opportunity to terminate the agent platform [2]. In case an agent attacks another, the denial of service attack can be explained by the example when the first agent send repeating messages to the another agent, infinite loop of conversation will not make the other agent complete its work or processes in time. In the other case when platform attack agent .the denial of service can be applied when the agent arrive to platform it expect from platform to execute it request but the platform ignore the service request which cause a delay in systems. Unauthorized Access [2], In agent gain platform, each agent must be authorized by a unique identity and each agent vis it the platform must be subject to the platform policy security, each agent that is not authorized and enter the platform can harm the data or the resources .Repudiation [2], repudiation Occurred When One Agent Makes A process Or Communication Then after that it Make a claims That it never take this action. Eavesdropping [2], when person listing to the conversation that not enrolls with it we call this by eavesdropping, any agent that is not part in communication and lessening to the secret communication is a part of eavesdropping threat. Alteration [2], when an agent arrives at an agent platform it is exposing its code, state, and data to the platform. Since an agent may vis it several platforms under various security domains throughout its lifetime, mechanisms must be in place to ensure the integrity of the agent's code, state, and data. Changes to an agent's state during its execution or the data an agent has produced while vis iting the compromised platform does not yet have a general solution. Copy and replay attack [2], in mobile agent system agent moves from one platform to another. A party that intercepts an agent, or agent message, in trans it can attempt to copy the agent, or agent message, and retransmit it. However, next sub section exposes further details in concern to mobile agent system.

B. *Mobile agents*

Mobile agents are software modules or entities that move from one host to another (machine to machine) in the network [3]. Each entity have a state ,data ,and code and can transform its self from one system to another with in distributed application that can be founded in the network .then return to home node in order to report their result to the user. This feature became the most important feature that distinguished mobile agent over traditional model[4]. The migration for agents is done under their own control from one node to another node in network to perform some task which is determined by the agent application,during the migration each agent may stop or execute or continue executing and updating its state. Some research that describe mobile agent as a software that acts like a user that exists in computer machine, and some other

research describe it as active agent have as several condition statement, exception handling method resizable prescient, but all of them agree that mobile agent is software executed in environment the communication between computer by several protocols like message passing.Mobile agent functionality for each agent depends on the agent source code Mobile agent can range from online shopping to the real-time device control to distributed scientific computing fields.

C. *Historical perspective*

In some distributed systems, the traditional structure is client server paradigm where the client and server can communicate with each other by message passing or, like RPC (Remote Procedure Call), the client sends a message then suspend itself until the reply arrives from the server (synchronous) [5].

In the clients/server model, a massive messages transfer is involved between the client and the server. But, in the mobile agent we can avoid this state because mobile agent can carry processing job from the host move to the host, then return back to original host when the process is finished.

Through time the alternative paradigm for RPC has become Remote Evaluation (REV) which has been developed by [6]. The client send to the server his procedure code with a requests to the server to execute and return the result back. In RPC the data is moved in two directions, and in REV the code is sent form client to the server, then data is sent back. In earlier system like R2D2 and chorus [7] introduced a concept that called active message that have the ability to migrate from one node to another node through network which carrying program code that by ready to be executed in that node, mobile agent system have the issue but in more generic concept,by encapsulation. In mobile agent system, the agent sent by client to a server (the agent encapsulating the code, data and execution context) not like procedure call because it does not go back to the client .and it may move to another server, transmit the information back to origin.

D. *Mobile agent features*

Every mobile agent system must have four features. Agent communication: MASs system must be able to allow that agent communicate with others by message exchange,Agent management: Each MASs system can create, execute, and terminate agents,Agent mobility: This feature is the basic feature of MAS, because agents must be able to copy and migrate the agent. Without this feature the mobile agent will lose the advantages over the traditional client/server model, Agent tracking: When agent moves or migrate from one system to another system the MAS have to locate the agent with that system. By this feature we cannot lose the contact with agent after migration.

II. BACKGROUND

Protecting the agents from attacks is still an open problem in computer science (CS), to grant protection for mobile agent system some techniques cover the parts that contains mobile agents system like Secure mobile agent contents,secure agent transfer and communication protocols , and protection the host recourses, or protection the platform [8]. To protect mobile agent, there are several approaches, these approaches are different in the cost, strength and performance. For instance designed might additional hardware that increase the security level including the cost. Other approach have low cost by using a software as security solution. The approach or proposed architecture for securing mobile agent some of them depend on using factors like time of path, or any factor that can help them in securing mobile agent.

For protecting agent the existing approach can be used or implementing method that deepened in hardware or software or by mixing than to providing a secure system. Each method have properties that make it better than other.

A. *Hardware approach*

In the hardware approaches, securing of system is done by using the specific or special equipment, the agent test this equipment's on the start or during execution agent [9] the tamper will occurred on agent code if deletion or alteration occurs when it tested by equipment.

Trust processing environment (TPE): In this approach it's execute the agent inside itself. Agent can migrate from TPE to other TPE by encrypted asymmetric form, in the TPE agent can communicate with visited site by using a secure logical interface [10].

Smart card: This approach proposed by [11]to protect agents. It depends in segmentation of agent; some segment may encrypt with public key of the card. Then the inscriptional segment will be transmitted to the card by the site during the execution, the card will be decrypted and execute the segment in identification.

B. *Software solution – approach*

In the software mechanism the security that provided have less cost and provided the ability to maintain the products Obfuscation: in this mechanism proposed by [12]which depend on software engineering rules. Like when we use go-to instead of recommendable loops, replacing procedure call by procedure body, and by stuff to much useless code to make it difficult to analysis mobile agents system. Can be used it to generate another agent where we have agent A, we can generate another agent A' that have same functionality but difficult to analysis.

Execution traces: When an agent visits a site or host to execute operation, it generates, a trace [4]. In this approach a hash function like SHA [6] to calculate a hash for the traces and sign the hash to agent including the result.

Another approach splits agent code into a white segment and black segment [13]the trace is calculated on the black segment only.

State partial: This is a complex function determined by calculation different state variable and executions it when the agent arrives to the host. This approached presented by (Farmer et al., 1996)[4] which give to the agent the ability to evaluate his privileges, the function to evaluate state and the agent when arrive to the site he can limit its action.

In the past three years, there has been a lot of scholars deal with enhancing mobile agent security. In the next few lines we will be discussing four researches deal with that. According to [14], they established an intelligent mobile agent (IMA)-based security optimization in which various agents govern the network performance such as routing, security check and transmission.

Shehada and her collages they proposed a novel Secure Mobile Agent Protocol[15]based on Broadcast for distributed service applications that would provide shared authentication, authorization, transparency, non-repudiation, honesty and confidentiality. The proposed system also provides protection from man in the middle, replay, repudiation, and modification attacks. They used scythe verification tool to prove the efficiency of the proposed protocol [16].

In another trend, an Improved Security-Aware Packet Scheduling (ISAPS) was proposed for achieving high level security and effective packet scheduling [17].

While last year (2019), Toumi and his collages they proposed a cloud computing framework to detect both insider and outsider attacks with high detection accuracy in Cloud environment. The new framework detect the attacks based on a cooperative between Hybrid intrusion detection system (Hy-IDS), mobile Agents and Firewall. The new framework has many advantages:Offering the access security, ease of resources management using mobile agents and service availability in a reliable structure with lower cost[18].

III. METHODOLOGY

Currently, there are many ways used to help researchers to explain their methods like simulation which is classified as a new technology that used and applied in any application fields. Computer assisted simulation can simulate systems and describe the behavior for any system in a simple way and describe the details of how it works.

The simulation is used to simulate and represent the behavior for network algorithms, network components and system component. In the commercial simulator the source code will not be provided to the general or public user for free. Any user who wants to use the open source code they must pay to get the license for the software package. OPNET is an example of typical commercials simulator.

The open source simulator have the advantage that everything is shared and open for public, the open source is more flexible than the commercial simulator but have a disadvantage that is the lack of complete documentation and enough systematic including the version control support, another disadvantages that the limited life time for the application of the open source network simulator. An example for typical open source simulator is NS2.

In our suggested model, the agent, as seen in Figure 1, the mobile agent system can have special security code in additional to the operation code that provide the security protection level needed and can secure the agent code, data and state.

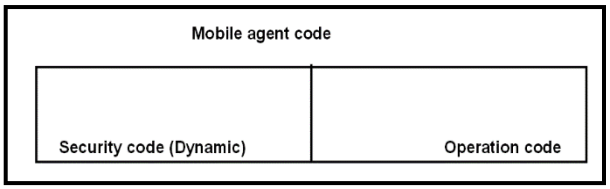

Figure-1. Mobile agent code

In our model the agent is created in the origin host that is fully trusted and will not attempt in anytime any malicious intend against any agent or host in the mobile agent system, during migration, the agent can visit the trusted node (host) and the entrusted node (malicious host).

When the agent arrives to the trusted node there is no problem for execution of the task by using resources that found in the host but when the agent arrives to the malicious host and needs to execute the wanted task and use the resources in the malicious host the attacker can start the attack against the agent to tamper with the agent code, data or state. Therefore, the agent must have a security code with operation code to provide it with the protection and security of the agent code, data, and state.

The agent may need to move to or migrate to another host that it might need to complete execution of the task, when the agent arrives to the next host it may become malicious and so on for all the host that the agent may visit them during the migration.

When the agent starts the migration it must change the security code by making update on the security code and updating certificates to forbid the hacker from monitoring its behavior or analyzing any contents. This means that the agent when dispatched from any visited host (malicious or trusted) to another host, it must update security level by changing the protection code. Figure 2 describes this process.

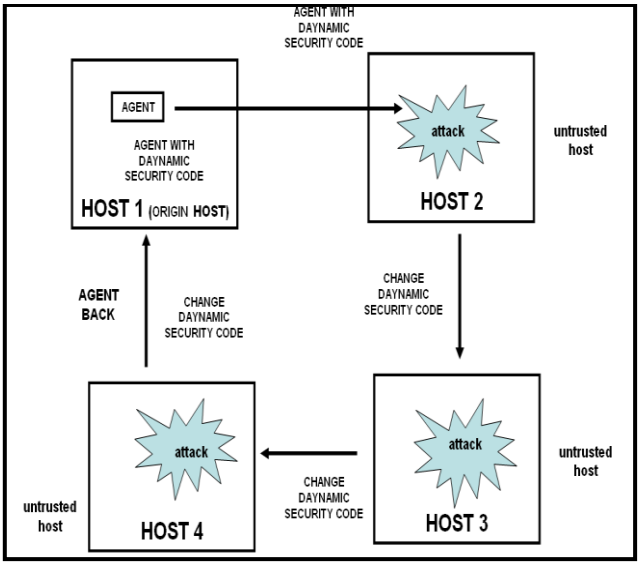

Figure-2. Agent migration with dynamic security code

Any agent, when created, must have an authentication information that could be identified by the agent properties like agent ID that must be unique, agent name, agent date of creation, agent life time and agent owner name that identified agents. Each agent must have a certificate or a set of certificates that describes the behaviors for the agents and determines all the privileges for the agent, including specifying the starting location and the address of destination host for the agents.

Aglets simulator have several built in agents which can be called aglets. Agents in open source form that give us the ability to modify the agent code by adding new lines of code that make the agent perform the wanted task.

A. Mobile agent simulation

In This part we demonstrates the simulation of two scenarios, the first scenario when the agent move to set of host with static security code, and the second scenario the agent moves to a set of hosts with dynamic security code that the agent changes and update when it departures any host In the simulation part.

B. First scenario (static scenario)

In this scenario, the agent is created in origin host (trusted host), the agent have two codes in the encapsulation (the operation code and security code), the security protection for securing the agent with a static code that's constant during all the time for agent migration, which mean the agent when migrate to host number two to host number three to host number four and return back to the origin host it has the same security code.

The agent is created by importing the package that is used in last simple mobile agent system ("Aglet") and make some changes in the agent implementation. The agent is called (XX) and the environment is set for the execution of the agent class inside Windows operating system.

The previous agent that is found in the simple mobile agent system have several built in functions that can be used in this simulated agent ,therefore, a full import of the all package contents into this work implementation has been performed .

The agent mobility can be done in the aglets system by using Aglets Transfer Protocol (ATP) that manages all agent migration between hosts.

The security code can be applied by using any algorithm that can be used for securing agent code. This scenario uses the XOR algorithm for security level in the agent because it is popular and easy to be implemented in programming language (JAVA language).

XOR Encryption is a simple symmetric cipher that's used in many applications because it has a level of trust that makes it unbreakable by brute force programs, this algorithm needs that's the encryptor and decryptor must have the same encryption key. This algorithms used because it's simple in the implementation and nearly unbreakable.

XOR is a logical operation on two operands that results in a logical value of true if and only if exactly one of the operands has a value of true. Using XOR algorithm for encryption at this stage does not mean being tied to it, any other algorithm can be used in the future to apply the security level to the agent.

The origin host that have a unique port number, we create a simple agent that have a string that's protected by using XOR algorithm for encrypting string, this encrypted string will be carried by agent from host to host ,the encryption algorithm implementation code (security code) is a static that encapsulated with agent operation code. In the aglets simulator we run the applets that have the encryption inside the origin host, and we enter the string that is encrypted into the new form. Now the agent starts its trip by moving to the next host with his encrypted data. The agent that will be used in this case have life cycle of 5 seconds, which means that the agent migration from the origins host to the destination host and retuning back to the origin in 5 seconds the time for all trip, and agent must stay inside each host around 5 seconds in maximum time for execution to complete.

C. Second scenario (dynamic scenario)

In the second scenario the security level is based on Blowfish encryption method [19]. Blowfish is a rapid and confident encryption algorithm, developed by B. Schneier in 1993. Meanwhile that time it has been hard to be cracked, in spite of various attempts. It is created for rapidity, by utilizing only simple operations such as additions and bitwise exclusive (XOR). Its speed and strength are because the fact that it utilizes an enormous key, ended 4 Kbytes of random numbers. Understandably, it is difficult to memorize such a key, however the Blowfish developer provided a sophisticated solution, a unique key

is carefully chosen once and for all, and subsequently altered by a password of your choice. The alteration is performed via repeated rounds of Blowfish encryption, this means that the key encodes itself. This self-encoding procedure is a bit extensive but only needs to be accomplished once per session.

we will use the same procedures used in the first scenario or case, but for the security protection the agent is protected by dynamic code that's altered during all the time for agent migration from host to host, which mean the agent when migrate to host number tow to host number three to host number four (cascaded migration) and return back to the origin host he must change its security code by its self for protecting the agent or at least reduce the threat or risk that can face agent during migration.

The dynamic scenario can be explained this by describing the agent migration map during four hosts machines that's different in there domain which mean each host could be malicious, because the hosts are strangest on each other, and we setup and installing a malicious software that attack the arrived agent in our architecture, to make the agent execution environment is malicious environments.

The agent must change his protection code or making alteration before he start the next jump, the Blowfish encryption method that implemented in our agent code can make an encryption with MAC address for the host that can provide for the security code a dynamic state. add to the original code an copy of code or copying another comment statement by stuff to much statements into agent body that make the agent code complexity more complicated to be analyzed, which in this way we can reduce the opportunity for the hacker to guess the agent information because the hacker need more time to analysis the agent or hacking him and the agent have a fixed period when visit the host in this way the agent can finish his visit and leave or departure the host with less opportunity to be hacked. In this level the agent have a dynamics code because he stuff to much statement in his code and make an encryption with his own MAC address.

In this simulation we use simple data that carried by mobile agent with small time intervals for agent migration and small time slots that's agent hosted in set of machines.

IV. RESULTS

In the last chapter we explain who the agent that's migrate between groups of host from the origin host to another host until he returned back to origin host after finishing the wanted task. the last simulation applied by using aglets mobile gent simulator by using one agent with four hosts the last migration have a fixed period for migration and fixed period inside each host that visited by agent with small data that carried by agent .the simulated period was around 20 second from beginning to the end which means the agent creation with agent migration and processing.

A. Security Code

When we use the static code the hacker can take number of round to analyze and discover agent less than dynamics code which applied a more complexity that's need more time for processing and analyzing agent code and information, as shown in Table-1.

Table-1. Types of code

Number of round	Node 2	Node 3	Node 4
Static code	3	3	3
Dynamic code	4	6	7

If we make a comparison between the security code that have static form and dynamics form with number of round that need to discovering and hacking agent we can see the dynamics security give the agent more complexity level and make it more secure and the hacker need more time for processing and more number of round to success to have results. Figure 3.

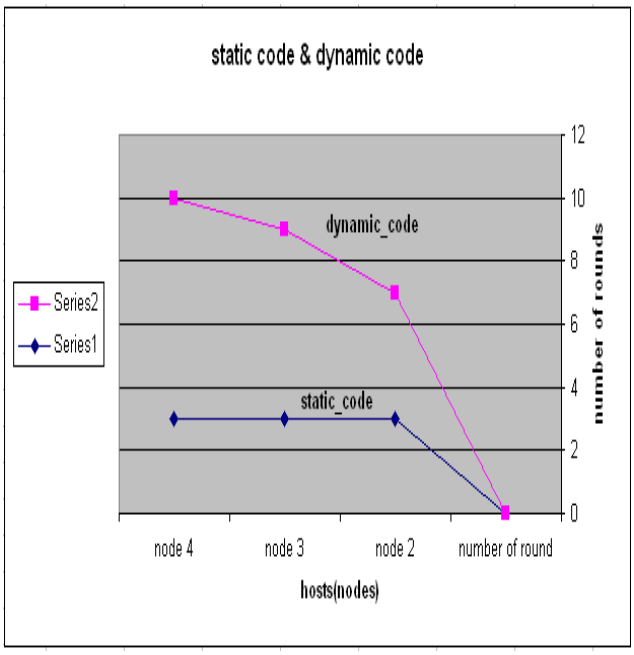

Figure-3. Comparison between the two security code scenarios

As shown in the figure above the dynamic security code provide to the agent and mobile agent system more reliability in security level during agent migration that's can protect the agent data ,states, and code from any attack from the malicious host or from any external entity that's may monitor agent behaviors during agent migration.

B. *Estimated processing time*

each agent can be classified to simple agent or complex agent, the agent can be classified as simple agent according to the data that he have or the agent contents that presented the agent, and the agent can be classified as complex agent when he have a huge amount of data or contents including the job that he must do and what the agent can do to finishing the wanted task.

The estimated processing time for the hacker to analyze the agent can be in incremental way because when the agent size become more complex he need more time for analyzing agent contents as shown in Figure 4.

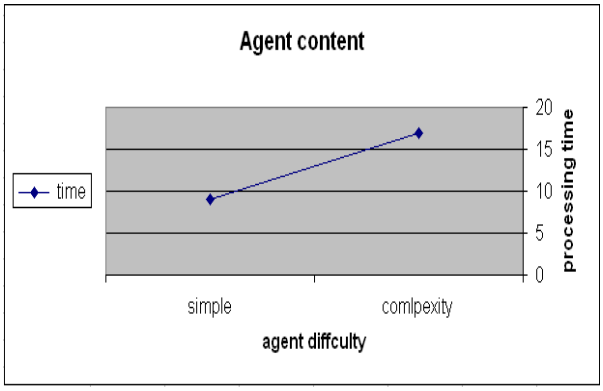

Figure-4. The estimated processing time for the hacker to analyze the agent

In this research we discover and present that the dynamics security code for the mobile agent provide more strength and confidentiality than the static security code. the dynamics code that applied on mobile code depends on using encryption algorithm such as Blowfish encryption method that have dynamics behaviors by XORing data with MAC address for hosts, including using code stuffing inside agent body to increase the complexity body.

V. CONCLUSIONS

About Our future work we will work on other scenarios in case if that the hosts are trusted and does not have any malicious intend because in our model we suppose that all the host are malicious then we check the weather for agent during the migration and testing the security level for the agent when he interact with the malicious host ,so in the future we will give more details if the agent that vis it a host that not have any malicious intent, and when the agent attacked from external entity that's outside the host which make the host malicious and change it to entrusted host.

Other issues we will expose it if the host is trusted but visited by other malicious agent that attack the host and change its the agent return back to the origin host after he visited all the host from host 1 to host 4, so next study we will make the agent that return baked to the origin for reporting its elf after each vis it to any host so the agent will not returned back after he finishing his migration the agent can back to origin after each jump to any host. We can give the each host and including the agent a list that have the MAC address for all suggested host that could be visited have set of hosts that mixed by trusted host and malicious hosts which mean agent jump from trusted to malicious then to trusted to malicious and so on. We will make agent migration in random way that's let the agent to jump from host to host in random way. In our model we supposed that about the agent migration we will check the agent performance during his migration when the migration map behaviors or by attacking the secured agent that must be protected.

REFERENCES

[1] Foreman, P. 2019. Vulnerability management. Book. CRC Press.

[2] Dittrich, D., Reiher, P. and Dietrich, S., 2004. Internet denial of service: Attack and defense mechanisms. Pearson Education.

[3] Anjum, F., &Tassiulas, L. 1999. On the behavior of different TCP algorithms over a wireless channel with correlated packet losses. In Proceedings of the 1999 ACM SIGMETRICS international conference on Measurement and modeling of computer systems (pp. 155-165).

[4] Armitage, G. 2003. An experimental estimation of latency sensitivity in multiplayer Quake 3. In The 11th IEEE International Conference on Networks, 2003. ICON2003. (pp. 137-141). IEEE.

[5] Tomas Sander and Christian F. Tschudin, 1998, Protecting Mobile Agent against Malicious Hosts, In Giovanni Vigna, Mobile Agent Security, pp. 44-60, Springer-Verlag, Herdeberg Germany.

[6] Stamos, J. W., & Gifford, D. K. 1990. Remote evaluation. ACM Transactions on Programming Languages and Systems (TOPLAS), 12(4), 537-564.

[7] Vittal, J. 1981. Active message processing: Messages as messengers. In Proc. of IFIP TC-6 International Symposium on Computer Message Systems (pp. 175-195).

[8] Harrison, C. G., Chess, D. M., &Kershenbaum, A. 1995. Mobile Agents: Are they a good idea? (pp. 25-47). Yorktown Heights, New York: IBM TJ Watson Research Center.

[9] Hohl, F. 1997. An approach to solve the problem of malicious hosts. Universitaet Stuttgart Fakultaet Informatik, Bericht, (1997/03).

[10] Farmer, W. M., Guttman, J. D., &Swarup, V. 1996. Security for mobile agents: Issues and requirements. In Proceedings of the 19th national information systems security conference (Vol. 2, pp. 591-597).

[11] Mana, A., & Pimentel, E. 2001. An efficient software protection scheme. In IFIP International Information Security Conference (pp. 385-401). Springer, Boston, MA.
[12] Loureiro, S., &Molva, R. 2000. Mobile code protection with smartcards. In 6th ECOOP Workshop on Mobile Object System. Cannes. France.
[13] Necula, G. C. 2001. A scalable architecture for proof-carrying code. In International Symposium on Functional and Logic Programming (pp. 21-39). Springer, Berlin, Heidelberg.
[14] Vijayalakshmi, A. and Palanivelu, T.G. 2017. Intelligent mobile agents collaboration for the performance enhancement in wireless sensor networks, Int. J. Signal and Imaging Systems Engineering, Vol. 10, Nos. 1/2, pp.72–83.
[15] BROSMAP: A novel broadcast based secure mobile agent protocol for distributed service applications. Security and Communication Networks, 2017.
[16] Shehada, D., Yeun, C. Y., Zemerly, M. J., Al Qutayri, M., Al Hammadi, Y., Damiani, E., & Hu, J. 2017.
[17] Nandakumar, R., & Nirmala, K. 2018. Enhancing Packet-Level Security in Mobile Ad-Hoc Networks. Indian Journal of Science and Technology, 11, 1.
[18] Toumi, H., Fagroud, F. Z., Zakouni, A., &Talea, M. 2019. Implementing Hy-IDS, Mobiles Agents and Virtual Firewall to Enhance the Security in IaaS Cloud. Procedia Computer Science, 160, 819-824.
[19] Schneier, B. 1993. Description of a new variable-length key, 64-bit block cipher (Blowfish). In International Workshop on Fast Software Encryption (pp. 191-204). Springer, Berlin, Heidelberg.