IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-1, Jan 2019 E-ISSN: 2347-2693

Mobile Agents In A Distributed Network With Trusted Node Implementation For Data Protection

L. Kathirvelkumaran[1*], R. Muralidharan[2]

[1,2]Dept. of Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, INDIA

[*]*Corresponding Author: firstauthor_kathirvelkumaran@gmail.com, Tel.: +91-9791507816*

Available online at: www.ijcseonline.org

Accepted: 26/Jan/2019, Published: 31/Jan/2019

***Abstract*—** Mobile Agents (MA) represents a comparatively new computing pattern which is used in numerous verticals as a means for anatomy disseminated applications. These Mobile Agents are programs which work in such a way that it will work independently by moving from one node to another in order to perform the assigned tasks on behalf of its owner in a distributed network. During which the mobile agents will communicate with the other agents or the hosts in the network and preserves the data when routing between one node and another. But it is difficult for the agents to transfer the preserved data to the home node due to lack of reliability. Thus in this Paper, it is discussed about how the mobile agents can preserve the collected data through a Trusted server or node by allocating a protected space in the trusted node and what are the measures are used for securing the data.

***Keywords*—** Mobile Agent, Trusted Server or Node, DSA, Public Key, Host Node

I. INTRODUCTION

Agents are colloquially called as Bots (from Robots). Bots are the predefined programs, an Artificial Intelligence that carry out the conversation via, textual methods which understands the query by matching the keywords from the Database.

TYPES OF AGENTS

Intelligent Agents: In specific, demonstrate few feature of AI, such as learning and reasoning.
Autonomous Agents: Capability to modify the way to achieve their objectives.
Distributed Agents: Being executed on physically distinct computers
Multi-Agent Systems: Distributed agents which work mutually in order to achieve the goal that cannot be accomplished by a single agent performing alone.
Mobile Agents: Capacity to relocate their execution onto different processors.
Stationary Agents: Resides on a specific host with the inability to move about but with the ability to offer services or perform tasks on favor of its host.

Basically, Mobile Agent is a type of Software Agents refers to a computer program which performs tasks on behalf of the host. These software agents have the right to decide the action which is appropriate to perform the assigned task. MA is defined as an independent program that moves between networks to get improvement of services supplied by stationary agents [1]. There are two types of MA based on Migrations: MA with Static Migration path i.e. MA will work only on the pre-defined path and MA with Dynamic Migration path i.e. depending on the present network condition, the MA choose the alternate path.

Mobile Agent has 3 major factors (C.S.A.):
Code (C.) - The agent's behavior is defined by a set of instructions called as Code
State (S.) - It can be defined as an Agent's internal variables which enables it to resume its activities after moving to another host
Attributes (A.) - These are information that describes the agent, its owner (home node), its movements, resources and key

II. SECURITY THREATS TO MOBILE AGENTS

The nature of MA directs to complex design and security threats. These threats are classified into four types as listed below based on the source of the victim and threat.

1. Agent to Platform: The set of threats in which agents exploits the security weaknesses of the agent platform launch attacks against an agent platform

2. Platform to Agent: The set of threats in which platform compromises the security of agents

3. Agent to Agent: The set of threats in which the agent exploits security weaknesses of other agents or launch

© 2019, IJCSE All Rights Reserved

attacks against other agents which may occur when there is an interaction among mobile agents

4. Platform to Platform: The set of threats in which the platform exploits security weaknesses of the other platform through external entities or its agents when there is an interaction among platforms of mobile agents
Each type of threat includes few or all of the below attacks,

Masquerading

This type of attack happens when an illegitimate user attempts to copy a legitimate user; so, the masquerade user attains the privileges from the actual user account.
This type of attack may occur in all four categories of threats. In threat categories, platform to agent and agent to platform, the identity of victim agent may be claimed by an unauthorized agent and thus the unauthorized agent achieves the permission to the services and resources to which it is not allowed. Similarly, an agent platform may pretend as another platform and therefore take in the mobile agent to its true destination, thus will permit the fake platform to extract the sensitive data from deceived agents [2],[3].
Likewise, Agents by communicating with each other, deceives another agent by extracting the required sensitive data. The same will be performed by platforms, where a remote fake platform may deceive a legitimate platform, and the later may transfer the obtained data and promote these agents to the faked platform [4],[5].

Unauthorized Access
This type of assault is relevant for agent to platform, agent to agent and platform to agent threat classes. This attack a mobile agent can have access to a meticulous platform and hence affect other legitimate agents. Moreover a mobile agent can directly interfere with another agent by invoking its public methods. It may even access and modify the agent's data or code. This alternation may affect and change the legitimate agent's behavior [6],[7].

Denial of Service

Table 1 Relates these attacks to threat classes.

Type of Threats	Type of Attack					
	Masquerading	Unauthorized	Denial of Service	Repudiation	Alteration	Eavesdropping
Agent to Platform	✓	✓	✓	✓	×	×
Platform to Agent	✓	✓	✓	✓	✓	✓
Agent to Agent	✓	✓	×	×	✓	×
Platform to Platform	✓	×	×	×	×	×

The mobile agents that requests for the services and resources to the platform will be ignored by the malicious platform. Without any prior notification, these malicious platforms will terminate the agent's execution, so that the agents will never reach its desired purpose. In the same way, the important files may get deleted, or the resources from the platform may be consumed by the malicious agent. Thus the platform and the other mobile agents are harmed due to scarcity of resources. This type of attack applies to the threat classes - agent to agent, platform to agent and agent to platform.

Repudiation
This type of attack refers to the denial of taking part in the transaction or communication. Repudiation may cause serious disputes which may not be resolved easily until and unless proper counter-measures are used. This type of attack applies to platform to agent and agent to platform threat types.

Alteration
Agent to Agent and Platform to Agent threat classes are subject to this type of attack. This attack means the malicious modification such as inserting, deleting or altering the code or data of a mobile agent without being detected. Thus, this modification will result in malfunctioning in the agents and platforms. However, detection of this malicious alteration is not simple and has no solution till now because the agent platform that visits have the right to access few code and information of the mobile agent and as a result it may modify them.

Eavesdropping
This is kind of passive attack where the malicious the malicious platform will observe state and behavior of mobile agent in order to get required data from the mobile agent, i.e. it observes and monitors the secret communications of the mobile agent. Eavesdropping is one of the possible attacks in mobile agents as the platform will monitor each and every instruction performed by the agent. This attack applies only to a threat type, Platform to Agent.

III. OBJECTIVE OF THE STUDY

Generally, Mobile Agents are subjected to any type of attacks which will be impacted due to any of the above discussed threats, because they are a lonely figure once sent to the agent space. Thus, in order to overcome these Eavesdropping and Alteration security issues on mobile agents in IP networks, Authentication is implemented when doing pre-processing with which the host machine in the network will allow the agent only when it is authorized to access it through the credentials and the same will follow the encapsulation process when it finds and reaches the host node. Also the collected data will be protected via, a

© 2019, IJCSE All Rights Reserved

Dynamic Storage Space (DSS) in a Trusted Node from where the data will be returned to the Home node.

IV. PROPOSED APPROACH

Our proposed solution is based on Trust which is a combination of blind folding and policy enforcement. Bind fold means the agent needs to trust its visiting host. Since agents trust the host, it has to provide all the required services without any malicious behavior which affects the agents. Whereas, Policy enforcement denotes the contractual agreement between the agent and the visiting hosts where both has to sign for its rights and responsibilities.

In existing system, the Mobile Agent has a public and private key at its disposal and the public key is visible to all the hosts in the network, so that the Agent could retrieve this key when it is visiting the hosts. The proposed system advances the mobile computation is being done.

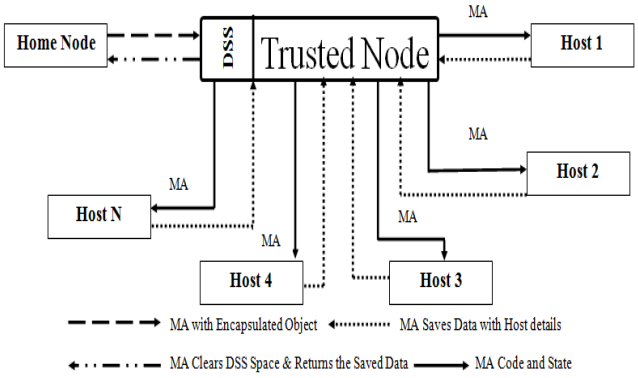

Figure 1 Proposed Approach Trusted Node

As denoted in the above figure, the Mobile Agent will be initiated from the Home node and moves to the Trusted Node where it creates a temporary storage named Dynamic Storage Space (DSS), and then the MA will move to the first host to be visited. It performs the operation of collecting the data from the visited node and sends the data to the DSS in the trusted node which will receive the data from MA and stored temporarily at DSS.

Every MA triggered from the home node will create temporary storage at its Trusted Node and each Mobile Agent which has created a space with this Trusted Node will do the same process of retrieving the data from the corresponding node and send it to the Trusted Node in the allotted DSS. Finally, after retrieving information from all the hosts, the Mobile Agents will return back to trusted node and interact with its respective DSS to provide the overall data which it has been stored until now. On getting the data, the agents will get back to its home node with the accumulated information indicating that they had completed the assigned task.

Initially, the mobile agent will get its space in trusted node by dividing into regions. And these trusted nodes offer several services to the MA when the agent is in the space created. One important service offered by trusted node is Security where the agents will be protected the happening of odd activities by unfriendly hosts. In present, many nodes are available in the network to be used as a trusted node like Mail Servers, Web Servers and DNS. As the name specifies, the trusted node have no rights in modifying the Agents' content, as the servers will not make any changes to the web page they host.

The security model advised in this paper gives more protection to the MAs' content stored at the trusted node.

Elements of the Proposed Approach

Below are the elements of the proposed approach:

- ✓ Home Node of MA
- ✓ Mobile Agent
- ✓ Trusted Node
- ✓ Dynamic Storage Space (DSS)
- ✓ Host Node

Home Node of MA

Home Node is the source of the Mobile Agent which will assign task for MA to perform on its behalf. This may also be described as the computer executing a Mobile Agent supported distributed application. Once the Mobile Agent completes its assigned task, it will return the data collected back to home node.

Mobile Agent

MA is defined as an independent program that moves between networks i.e. from one node to another to perform the assigned task [8].

Trusted Node

In a distributed network nodes, in order to facilitate the secure service and to provide a secure execution environment, a Trusted Nodes setup are handled by a third party. When assigning the task to the MA, the Home node will share the query along with the address of this Trusted Node, where the Mobile Agent can save its attributes, state and data.

Dynamic Storage Space (DSS)

DSS is the temporary storage space formed by every Mobile Agent(s) at the Trusted Node once the MAs are assigned with the task and starts from the Home Node. The storage space is dynamic because exact size and the type of storage could not be predicted by MAs once they are triggered, hence the space is dynamically expanded at the run time based on the data to be collected.

© 2019, IJCSE All Rights Reserved

Host Node

A host node can be said as Network Host, is a computer or other device which can be a client, server or both connected to a computer network. This host node is expected to be an agent-enabled one for providing the information resources, applications and services that are required by the Mobile Agents to execute its query over there.

V. SECURITY FRAMEWORK FOR PROPOSED APPROACH

The proposed model provides security at each level with the intention to secure the network created for mobile agents from any malicious attacks. This is achieved as the Home Node, Mobile Agent(s) and the Dynamic Storage Space elements are working together. Since the mobile agent saves the attributes i.e. the data in the DSS, and carries only the other two factors: code and state, there is no chance for disclosing the data collected so far to the hosts to be visited which may be hostile.

The security is also achieved by means of encapsulating the list of hosts to be visited in the network by the mobile agents in the home node. The agents will use the encapsulated object in the visiting host before utilizing the host details to run its code. Thus agents stay away from visiting any hostile host and loss it's all or any of its factors. Security at each element is discussed here.

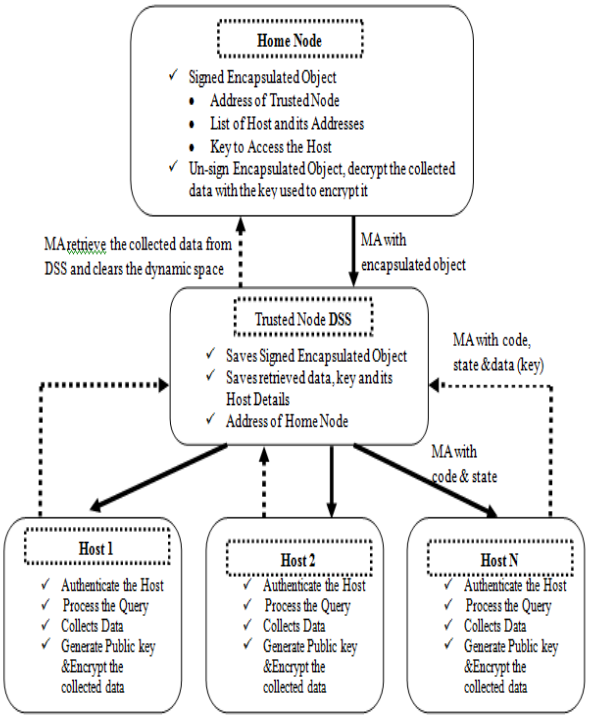

Figure 2 Security Framework for Proposed Approach Trusted Node

Process at Home Node

As discussed above, the mobile agents can execute its request only in the agent-enabled hosts. The Pre-processing technique will be processed in the home node in such a way that the list of visiting hosts (server/client) will be determined and creates an object(s). This object holds the list of visiting hosts, code (query) to be processed, address of the trusted node and the address of home node. The object is encapsulated and signed using the Public Key by the pre-processor. Then it will be handover to the Mobile agent(s), which has the privilege to un-sign the object through which it determines which node to be visited next i.e. the Trusted Node as indicated earlier.

Process at Trusted Node

The mobile agent reaches the Trusted Node and creates a temporary storage, the Dynamic Storage Space (DSS). Then the MA will transfer the encapsulated object into the dynamic storage space. After that, the mobile agent use its public key to access the encapsulated object and look for which host to be visited next to process its query. Then it takes the query and move to the host which is listed first in the object.

Process at visiting Host

The mobile agent reaches the Host in the network based on the list of hosts provided in the object. It authenticates the Host and initiates processing the query. The host in return share its resources to process the query in it. Then the mobile agent collects the data, encrypt the data using a public key generated at instant. The mobile agent moves to the trusted node, saves the encrypted data in the dynamic storage space with the details of respective Host from which the data is collected. Again saves another copy of visited host details within itself, check for the next host to be visited and traverse to it with the query to be processed and its state.

Process at Trusted Node: After Reaching the Nth Host

Once collecting the data from the last host, the mobile agent moves to the trusted node and place the data and the host details in dynamic storage space. Then the mobile request the dynamic storage space to return the saved data. DSS will return the data to mobile agent. Now mobile agent will use the public key, unlock the object and look for the next node to be visited, which is obviously the Home Node. Now the mobile agent will retrieve all the data stored in DSS, clears the temporary created DSS in the trusted node and moves to the home node.

Process at Home Node: After Completing the Search

Now the mobile agent reaches the Home node after performing the assigned task. The mobile agent hand over the information collected from the list of hosts to the home node i.e. to the Processor. Since the information collected at each host is encrypted, the pre-processor will decrypt the

© 2019, IJCSE All Rights Reserved

object using the Public key. Next it will decrypt the information using the public key which is generated at the instant in the visited node to encrypt the data collected. This process will be repeated for the data retrieved from every visited node, consolidate it and hand over to the user who requested the query.

VI. RESULTS AND DISCUSSIONS OF EXISTING AND PROPOSED APPROACH

The mechanism followed in the existing system is the mobile agent(s) will be initiated from the home node, move to the first host to be visited, process the query, retrieve the data, move to the trusted server and creates a copy of the data (attributes), the address of the home node and the traverse time of the MA as a backup, moves to the next host to be visited with the data collected, collects information in the second node, traverse to trusted server, now copies only the data collected & not the address and duration again, moves to the next node and continue the same process until it reaches the last host. Now the mobile agent will directly moves to the home node and gives the consolidated data collected from all visited hosts. Since the trusted server is stored with the traverse time and the address of MA's home node, it will verify the duration and if the time is elapsed, the trusted server will check with the home node whether the MA has returned the data. If yes, the server deletes the backup created so far and frees its space for next MA, else it transfers the data collected to the home node and then free the memory. The later part will be executed in the scenario when mobile agent may lose due to any malicious action in the network.

Thus in the existing system, all 3 factors: code, state and attributes of MAs will traversed when the agents visits different hosts in the network which may be hostile and has the high possibility of disclosing the data collected from previous hosts which may leads to data loss or data modification. The MAs will store the collected information from every host into the Trusted Server as a backup, but it carries the information to all the visiting hosts as specified above. This technique consumes huge memory space due to high volume of data carried between hosts. Thus the bandwidth and the processing speed of the MAs will be spontaneously reduced.

In the proposed system, the mobile agent is provided with the list of hosts to be visited, address of trusted node and home, and the query to be processed. These are encapsulated as an object and shared to MA(s). Also, the mobile agents will directly reaching the trusted node and creating a temporary space to save its attributes once it dispatches from the home node, carries only the code (query) and state to the visiting nodes which overcome the threat of Data manipulation/loss, and returning to the trusted node once it visits all the listed hosts, collects data and return to home node by clearing the temporary space created.

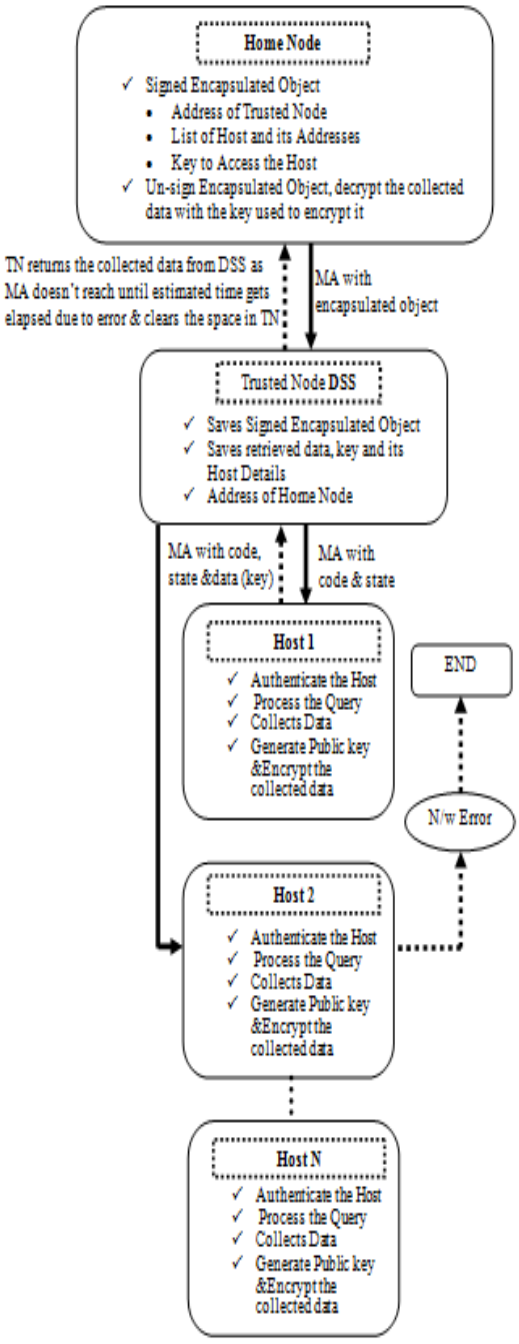

Figure 3 Proposed Approach – Sequence Diagram

Thus by traversing in the network without the accumulated data collected, the processing speed of MAs and the bandwidth will be increased. Even when the MA is lost due

© 2019, IJCSE All Rights Reserved

to any network error or if the allotted time elapses, the trusted node will return the data collected so far to the home node and clears the temporary space by itself, as referred in the above figure. Since the home node has the pre-processor which has the public key, it decrypts the object and send the data to the user by decrypting the data which is encrypted at the collected host, where the public key used for encrypting the data is stored in the object as well with the host details.

VII. ALGORITHM

Below explains the process of MA with Trusted Node,

Initialize "Query to be executed"

Pre-process the visiting Agent-enabled Hosts with Private Key

Creates Encapsulated Object (Trusted Node' address, visiting Hosts' addresses with Key, Query, Estimated Time, Home Node' address)

Pass Object to Mobile Agent with PubKey

Mobile Agent un-sign the object

Determine the Address of Trusted Node

MA create Dynamic Storage Space in TN

Saves the encapsulated Object in DSS

Mobile Agent un-sign the Object

Determines the Host to be visited

Traverse to Visiting Host with Query and State

Acknowledge Host with Private Key

Process the Query

Acquire the resources

Collects the data

Generate PubKey and Encrypt the Data

Return to Trusted Node with Encrypted Data, Code and State

Saves Encrypted Data and Host Details to TN

Un-sign the Object and Save details

Determines the next Host to be visited

Traverse to Visiting Host with Query and State

Repeat the process until reaches last Host

Return to Trusted Node

Saves Data and Host details

Determine next Node to be visited

Next Node equals Home Node

Collects all data

Clears the Dynamic Storage Space

Returns to Home Node

Un-sign the encapsulated Object

Find the Public Key to decrypt the collected Data

Decrypt the data for the Query

If Mobile Agent not returned to Trusted Node

Trusted Node waits until Estimated Time

If Time Elapsed

Returns the encapsulated Object with collected Data to Home Node

Clears the Dynamic Storage Space

Home Node finds the Public Key to decrypt the collected Data

Decrypt the data for the Query

VIII. CONCLUSION

Thus in the proposed architecture, the use of Trusted node with temporary storage DSS helps in retrieving the data even in case of any loss to the mobile agents in network. And the instant key generation in visiting hosts improves the security of data being retrieved. Bandwidth and latency time are being equally measured. The entire processing doesn't require any additional effort from the used entities .The attack type of alteration is highly focused in this paper and major attacks types are overcome as well. The improvement can made on the key size, time used for retrieving as MA itself is save returning the retrieved data to the trusted node and traverse to the next host which gradually increases the overall processing time.

REFERENCES

[1] Karnik, N. "Protection in mobile agent systems" Technical report University of Minnesota, pp.1-12, 2000

[2] PAhich P.. K. Dutta, and M.C. Govil,"Security Issues in Mobile Agents", International Journal of Computer Applications, Vol. 11, pp 1-7, December 2010.

[3] D.M. Chess, " Security issues in mobile code systems".mobile agents and security, Vol 3. LNCS1419. Springer-Verlag 1998.

© 2019, IJCSE All Rights Reserved

[4] S.M.S.I. Rizvi, Z. Sultana, B. Sun, and Md. W. Islam,"Security of Mobile Agent in Ad hoc Network using Threshold Cryptography", World Academy of Science,Engineering and Technology PP.70-75 2010.

[5] S. M.. Moussa, G.A. Agha, "Integrating Encrypted Mobile Agents with Smart Spaces in a Multi-agent Simulator for Resource Management", Journal of Software, Vol. 5, Jun 2010.

[6] Amro, Belal, Mobile Agent Systems, Recent Security Threats and Counter Measures. International Journal of Computer Science Issues (IJCSI). 11. 146-151,2014

[7] L.Kathirvelkumaran, R.Muralidharan "A Standard Framework And Migration Process of Mobile Agents Using Preprocessing Techniques", International Research Journal of Computer Science (IRJCS), Vol. 4 , Issue No 06, pp.40-43, June 2017

[8] L.Kathirvelkumaran, R.Muralidharan A Framework for Network Monitoring Performance Management of Mobile Agents Using Pre-Processing Techniques In Distributed Environment International Journal of Pure and Applied Mathematics Vol.119 No. 12, , ISSN: 1314-3395,pp. 13641-13650, 2018

[9] Rajdeep Bhanot and Rahul Hans A Secure and Fault Tolerant Platform for Mobile Agent Systems International Journal of Security and Its Applications Vol. 9, No. 5,ISSN: 1738-9984 IJSIA ,2015

[10] A.K. Sharma, Atul Mishra, Vijay Singh An Intelligent Mobile-Agent Based Scalable Network Management Architecture for Large-Scale Enterprise System International Journal of Computer Networks & Communications (IJCNC) Vol.4, No.1, January 2012

Authors Profile

Mr. L.Kathirvelkumaran pursued Bachelor of Computer Science from Bharathiar University, Tamil Nadu, India in 2008 and Master of Computer Applications from Anna University, Coimbatore, Tamil Nadu in the year 2011. He is currently pursuing Ph.D. and working as Assistant Professor in Department of Computer Sciences, Rathinam College of Arts and Science, Affiliated to Bharathiar University,Tamil Nadu, India since 2013. He has published more than 06 research papers in reputed international journals and conferences and it's also available online. His main research work focuses on Computer Networks, Network Security, Mobile Agents and its Security, IoT and Computational Intelligence based education. He has 6 years of teaching experience and 4 years of Research Experience.

R.Muralidharan is a Head, Department of Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamilnadu, India done research in the field of Object Recognition Systems. He received his PhD from Anna University, Chennai in 2013. He received M.Sc. Computer Science from Bharathidasan University in 2001 and M.Phil from Bharathiar University in 2005. He is a life member of CSI and IACSIT. His research interests are in Image Processing, Object Recognitions and Neural Networks. He has produced 6 MPhil research Scholars and guiding 7 PhD research scholars.

© 2019, IJCSE All Rights Reserved