International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 2– No.3, May 2012 – www.ijais.org

Formal Modeling for Multi-Level Authentication in Sensor-Cloud Integration System

Dinesha H A
Crucible of Research and Innovation
PES Institute of Technology
BSK 3rd Stage Bangalore-85

R Monica
M.Tech in Software Engg..
PES Institute of Technology
BSK 3rd Stage, Bangalore-85

V.K Agrawal
Director, CORI
PES Institute of Technology
BSK 3rd Stage, Bangalore-85

ABSTRACT

Recent developments in sensor networking emphasized the need for integration of sensor networks with the cloud. This improves the processing power and battery life of the sensor nodes. Once the sensor data is routed to the cloud, possible measures need to be adopted to secure the sensor data. Thus, strict authentication checks have to be provided to facilitate authorized customers to utilize the services provided by the cloud in the form of sensor data. In this paper, we present an authentication system by employing the multi-level authentication technique in securing the sensor data in cloud. This technique generates/authenticates the password in multiple levels to access cloud services. Thus, the proposed scheme helps in improving the authentication level by order of magnitude as compared to the existing technique. We modeled the proposed system using Petri nets.

General Terms

Cloud Computing, Sensor Network, Security

Keywords

Ant colony routing algorithm, multi-level authentication technique, sensor cloud integration.

1. INTRODUCTION

Recent advances in electronic and computer technologies have paved the way for the proliferation of wireless sensor networks (WSN) [1]. WSNs are autonomous systems consisting of tiny sensors. These are associated with integrated sensing, limited battery lifetime, resource constraints and limited range. The limited battery lifetime limitation can be overcome by integrating the WSNs and cloud computing technology. The cloud technology is an internet-based model which enables convenient and on-demand network access to a shared pool of configurable computing resources [2]. Various services such as, software, hardware, data storage and infrastructure are provided over internet. These are accessed from web browsers, desktop and mobile applications. Cloud Computing Technologies which are grouped into 4 different services that are depicted in figure 1 as SaaS, DSaaS, IaaS and PaaS [3]. Cloud Computing DsaaS Technology [3] provides scalable resources to store the sensor data and make that data available on demand. Since wireless sensor networks are limited in their processing power, battery life and communication speed, cloud computing offers the DsaaS service. This makes sensor data available for long term observations and for shared use of data and services in different kind of projects or analysis.

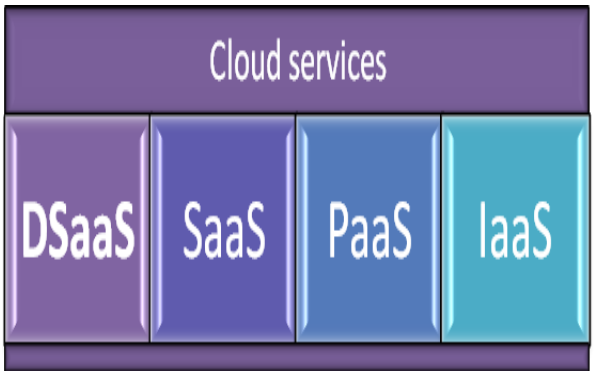

Figure 1: Services provided by cloud computing

In order to allow the flow of sensor data to cloud server [4], we propose to use ant colony routing algorithm [5] [6] [7]. This helps in establishing the shortest path between the sensor network and cloud server through an appropriate gateway [8]. Once the sensor data is uploaded to the cloud, it requires appropriate mechanisms for delivering the data only to the authorized users [4]. In this paper, we propose to use an authentication technique, called as "multi-level authentication technique". This technique authenticates the cloud access in multiple levels. To break the authentication, one has to know the login details of all the levels. Here, in this paper, we use formal modeling for our system to precisely discuss the availability of the cloud services for the intended users, along with the provision of appropriate modeling [10], algorithm and formulations. Thus, we expect, with this proposed technique the probability unauthorized accesses can be greatly reduced.

This paper is organized as follows: Section 2 discusses the multi-level authentication technique for securing sensor data. Section 3 provides the system architecture and an algorithm along a probability theory for the proposed multi-level password authentication in sensor-cloud integration system. Section 4 deals with the system modeling. This has various sub sections which involves activity diagram and Petri nets based model for the complete multi-level password generation technique for sensor-cloud integration application. Finally, the paper is concluded in section 5.

2. MULTILEVEL AUTHENTICATION TECHNIQUE FOR SECURING SENSOR DATA

To access the sensor data from cloud, we are using multi-level authentication technique. This technique authenticates the cloud access in multiple levels. It generates the password and concatenates the generated- password at multiple levels. Based on the leaf level- concatenated -password, one can access the cloud services provided that the password authentication is successful in all the previous levels [11]. Fig. 2 shows the architecture of multi-level password generation technique. This architecture helps in checking the authentication against the services and privileges. It also helps to ensure which customer has what kind of privileges to use the sensor data in the cloud. This is evaluated by multiple levels authentications, where authentication activities take place in organization, team and user levels. First level of authentication is organization level password authentication/generation. It is for ensuring the cloud access authentication from cloud vendor. If unauthenticated organization or hackers tries to access the data in the cloud, they would be terminated in this level itself. The second level of authentication is a team level password authentication/ generation. It is to authenticate the team for particular cloud service. Likewise, based on the system requirements, authentication system can have even further n levels. Finally, the last level will be the user level password authentication/generation, which ensures that customer/end user has particular privileges and permission to access the data [11].

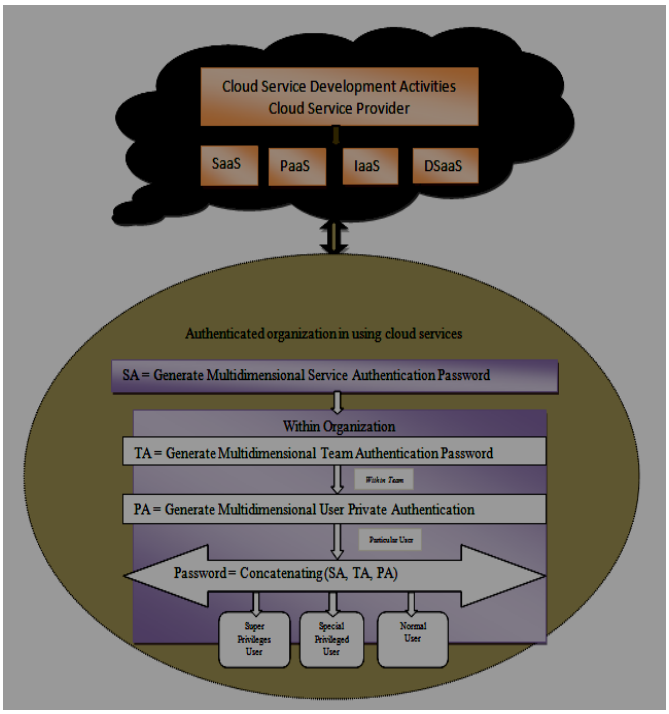

Figure 2: Proposed multi-level authentication technique for securing sensor data

3. SYSTEM ARCHITECTURE

Proposed system architecture shown in Figure 3, where the provision security of multi-level authentication to the sensor data is clearly depicted. As seen in the above figure 3, the sensor network has the ability to sense the environment, process the captured data and deliver it to the destination- which is nothing but the base station, for which we using zone based ant colony optimization technique [9]. Through an appropriate gateway the sensor node can be integrated with the cloud. The data packets from the sensor network can be routed efficiently to the cloud server using ant colony routing technique [12]. This finally relieves the burden of the sensor nodes to some extent and improves the processing power and battery life. Along with the provision of storage service offered to the sensor data, security services are also provided by the cloud servers. The security mechanisms are provided with the help of multi-level authentication technique which authenticates the cloud access in multiple levels. This technique provides authentication activities at organization, team and user levels. One can deploy applications more rapidly across shared server and storage resource pools than is possible with conventional enterprise solutions.

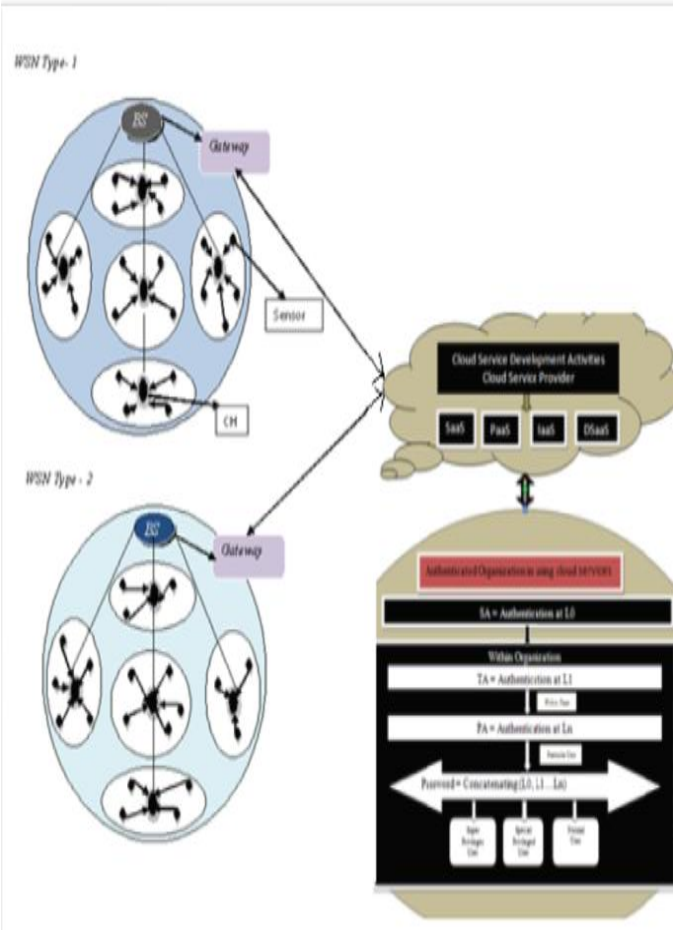

Figure 3: System Architecture of the Proposed Cloud computing based sensor data analysis environment

Algorithm: Multilevel authenticated cloud sensor integration

3.1 Proposed Algorithm

The algorithm for the complete multi-level password authentication/generation technique for securing sensor data is discussed in this section. Important notations being used in the algorithms are: CH- Cluster head, BS - Base station, CS - Cloud server, SA-service authentication, TA- team authentication and PA- privilege authentication. Initially, the sensor data is processed, routed and uploaded to the servers of the cloud which provide access only to authenticated users. For this purpose, we have proposed Multi-level authentication technique. Multi-level authentication system reads the details given by organization, team and user and produces the password output at different levels. These are discussed as follows:

Step 1: Sensors would process & route the data packets to CH

Step 2: CH collects data packets and route it to the BS

Step 3: The routed data would be collected by the BS and upload the information to the CS

Step 4: CS acts as a repository to store the info & provides access only to authenticated users.

Step 5: Authentication check: Multi-level authentication checks

SA - Organization level password generation—Authentication at level 0.
If SA is authenticated organization then
TA - Team level password generation—Authentication at level 1.
If TA is authenticated then
……
…….
……

PA – User level password generation—Authentication at level n.
If PA is authenticated user then
Password = Concatenate L0, L1….Ln
If password privileged authenticated then
Then
Provide access to the sensor data in the cloud
Else
Go to step 6
End

Step 6: Exit

3.2 Probability of Breaking Multi-Level Authentication

Probability of breaking multi-level authentication to access sensor data from cloud can be formulated by using the probability theory. According to this technique, one has to know the password of all the levels in order to access the required sensor data. According to this scheme, the authentication is provided at n levels for which we have N1*N2…*Nn possible options. Therefore, the probability of hacking correct password is 1/N1*N2*N3…*Nn =>1/Nn as given in [11].

4. SYSTEM MODELING

This section presents an activity diagram for multi-level authentication technique for securing sensor data in the cloud. We also provide a Petri net model for the proposed algorithm in the preceding section. The model helps in understanding and analyzing the proposed authentication system.

4.1 Activity Diagram of Multi-level Authentication Process

The proposed system activity diagram provides the clear picture of the activities of rendering security to the sensor data uploaded to the cloud servers. The security is provided using multi-level authentication system. At the first phase of this process the sensors would process the data and route it to the cluster head. This in turn would collect the data and route it to the base station which would upload the huge amount of the integrated data to the cloud. The servers of the cloud provide secure access to the information only to the authenticated users. The authentication activities provided by the cloud take place in organization, team and user levels. First, activity happens at organization level. It reads the authentication password and checks to authenticate the organization for cloud access and then it enters into a second level authentication. The second activity happens at team level. It reads the team login details and checks for authentication. Once it is done; it then enters into a user level authentication. User level activity reads the authentication information to check for the user permission and privileges.

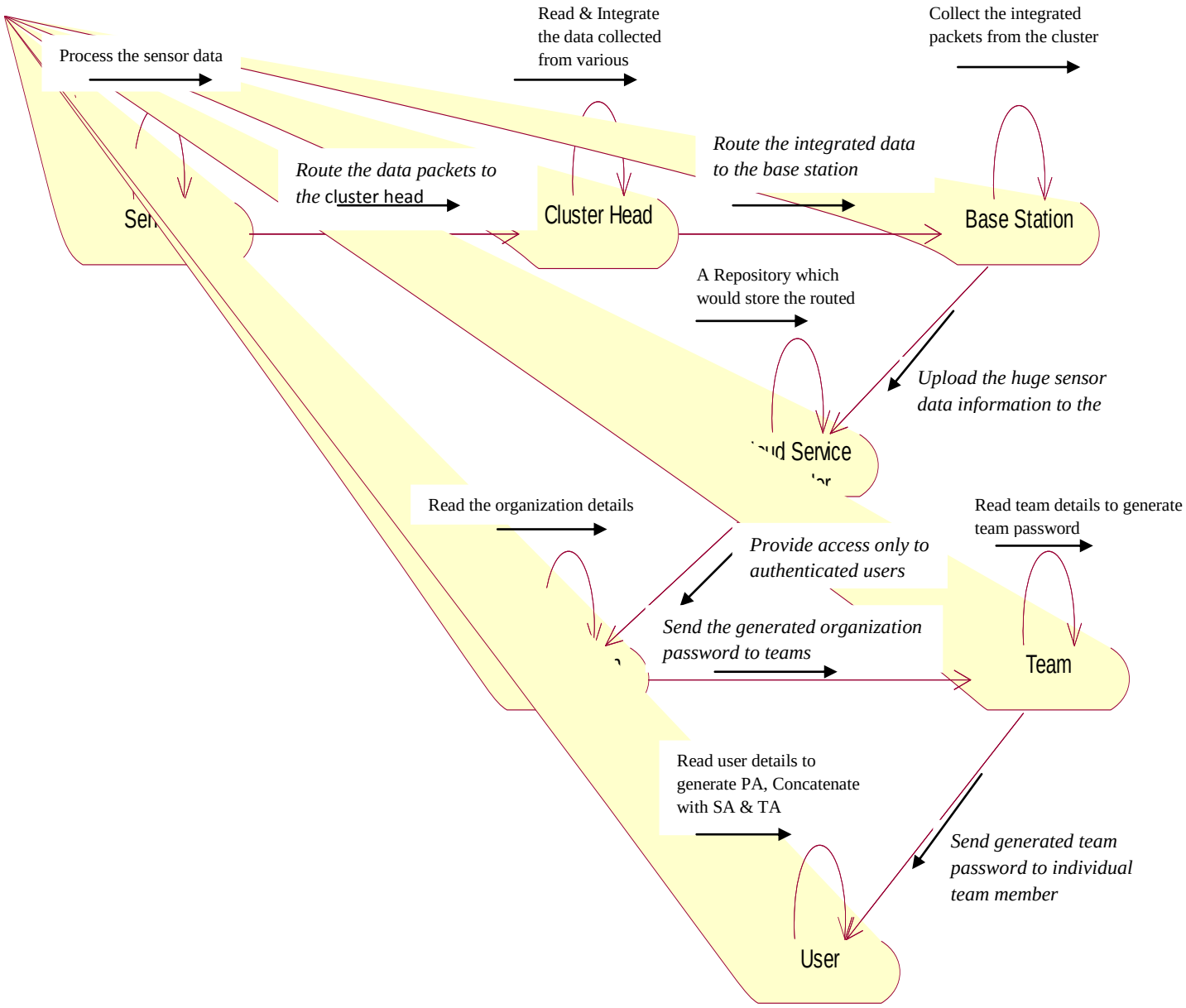

Figure 4: Activity diagram for secured sensor cloud integration using multilevel authentication technique

4.2 System Modeling Using Petri Nets

The system modeling is done using Petri nets, which are vividly portrayed in figure 5. Petri nets are a special form of bipartite directed graph represented by < P, T, In, Out> [10], in which Place (denoted as p) and Transitions (denoted as t) are disjoint sets of nodes, and In and Out are sets of edges. We carry out formal modeling for our system to precisely discover when the user can and cannot access the services of the cloud. The model is explained as follows. As shown in figure 5, the sensor data are accessed in round robin fashion represented by places p1, p2, p3 and p4 and transitions t1, t2, t3 and t4. The sensor data are represented by places p5, p6, p7 and p8. The availability of data is indicated by the presence of tokens in these places. When the cluster head is ready, it puts a token at cluster ready place p9. This enables the required sensor data to be passed on to the sensor data queue. Similarly, when base station is ready to receive the data, it provides a token at ready place p15. The base station data are further passed on to cloud server for data storage. When a client request arrives for the token at place at p16, the system starts validating the authentication word at p19, p20 and p22 levels.

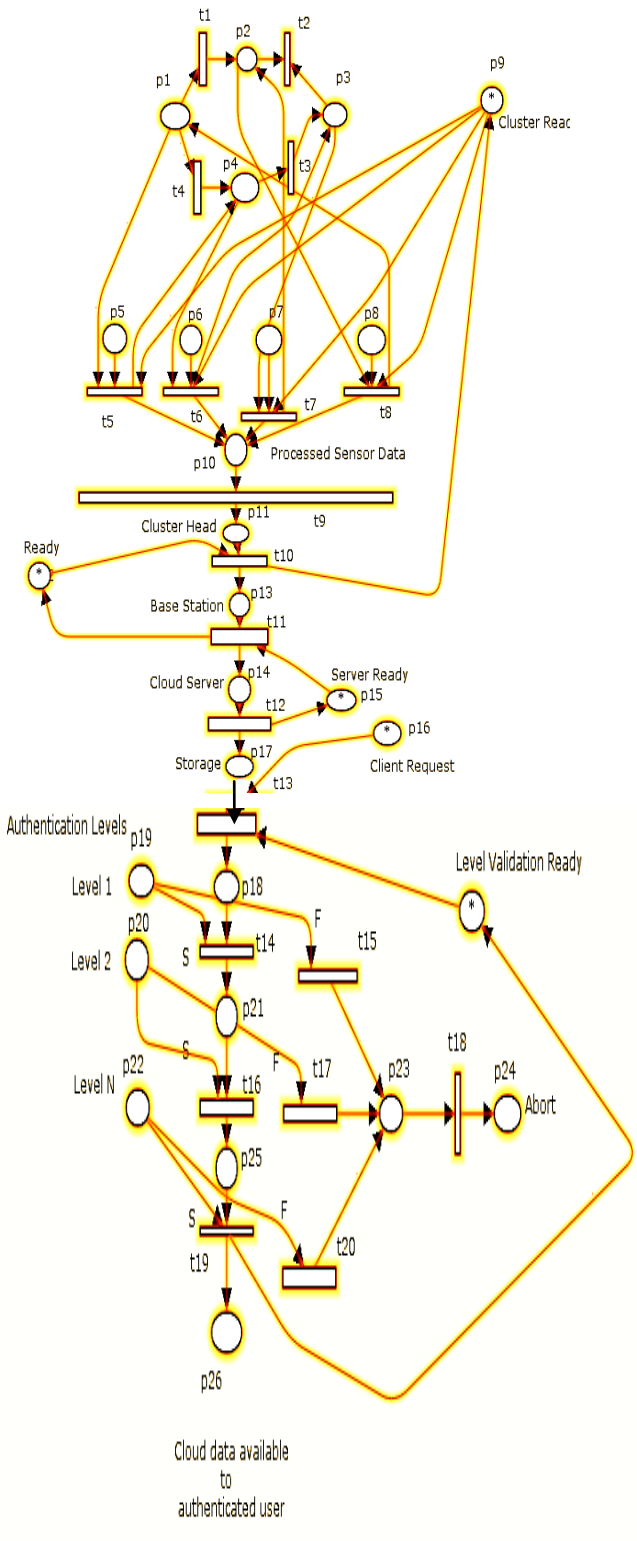

Figure 5: System modeling using Petri nets

The client is authorized only when all the levels are successfully validated. Otherwise, the request is aborted. Using this model, detailed analysis with respect to authentication scheme may be carried out which is a topic of our future research.

5. CONCLUSION AND FUTURE ENHANCEMENT

In this paper, "Formal Modeling for Multi-Level Authentication in Sensor-Cloud Integration System" is done. It is expected to help in the analysis and provision of authenticated access to the data in the sensor-cloud integration system. We have described this authentication system by employing the multi- level authentication technique to secure the sensor data in cloud. This technique generates/authenticates the password at multiple levels to access cloud services. A strict authentication and authorization can be achieved through this technique. The proposed System is modeled using Petri net. Detailed analysis with respect to authentication scheme may be carried out. Our future work will be carried out in adding multi-dimensional password generation method to this system.

6. ACKNOWLEDGMENTS

Our sincere thanks to Prof. K N B Murthy, Principal and Prof. Shylaja S S, HOD, Department of Information Science and Engineering, PESIT, Bangalore, for their constant encouragement

7. REFERENCES

[1]. Center Bo Wang, HongYu Xing "The Application of Cloud Computing in Education Informatization, Modern Educational Tech..." Computer Science and Service System (CSSS), 2011 International Conference on IEEE, 27-29 June 2011, 978-1-4244-9762-1, pp 2673 – 2676.

[2]. NIST Definition http://www.au.af.mil/au/awc/awcgate/nist/cloud-def-v15.doc

[3] Cloud Computing services & comparisons http://www.thbs.com/pdfs/Comparison%20of%20Cloud%20computing%20services.pdf

[4] A Framework of Sensor - Cloud Integration Opportunities and Challenges, Mohammad Mehedi Hassan, Biao Song, Eui-Nam Huh, Published in: · Proceeding ICUIMC '09 Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication ACM New York, NY, USA ©2009, ISBN: 978-1-60558-405-8.

[5] Maumita Bandyopadhyay, Parama Bhaumik, "Zone Based Ant Colony Routing in Mobile Ad-hoc Network", IEEE conference, 2010

[6] Zone based ant colony routing for MANET to improve the performance By Dr.H Sarojadevi, Bhuvaneshwari Patil.

[7] Mesut G¨unes¸, Udo Sorges, Imed Bouazizi, " ARA – The Ant-Colony Based Routing Algorithm for MANETs ", International Workshop on Ad Hoc Networking, Vancouver, British Columbia, Canada, August 18-21, 2002.

[8] Rinku Sen., "Exchanging of Information between Cloud Computing Server and Sensor Node for Effective Application Development", ISDMISC 2011

[9] Selcuk Okdem and Dervis Karaboga; "Routing in Wireless Sensor Network using Ant Colony Optimisation using Routing Chip"; Sensors, vol. 9, pp. 909-921, 2009

[10] Petri Net Theory and the Modeling of Systems, James Lyle Peterson, publisher: prentice-hall

[11] *Multi-level Authentication Technique for Accessing Cloud Services*, Dinesha H A and Dr.V.K. Agrawal, IEEE, International Conference of Computing, Communications and Applications, PSNA College of engineering and technology, Dindigul, Tamilnadu.

[12] "Wireless Sensor-Cloud Integration Using Ant Colony Routing Algorithm", *R Monica* , Dinesha H A and Dr.V.K. Agrawal, International conference on Cloud Computing and Service Engineering CLUSE 2012, R.R College of Engineering, Bangalore.