2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI)
November 5-6, 2015
(Iran University of Science and Technology) – Tehran, Iran

Combining wireless sensor networks and cloud computing: security perspective

Zahra Shojaeerad, Saloomeh Taherifard
Sama Technical and Vocational Training College
Tehran Branch (Andisheh), Islamic Azad University,
Tehran, Iran
Zahra.shj@gmail.com, saloomeh_taherifard@yahoo.com

Seyed Mahdi Jameii
Department of Computer Engineering, Shahr- e- Qods Branch,
Islamic Azad University,
Tehran, Iran
jamei@qodsiau.ac.ir

***Abstract*— At the present study, in order to ease analysis of real time data and to ease sharing data, combination of wireless sensor network and cloud computing has been applied. In addition, in order to be able to support large amount of data and in order to meet limitations of wireless sensor networks in regard with ability to process and acceleration of communications, cloud computing would be applied. Here, functions of integration of the two technologies of wireless sensor network and cloud computing would be referred and types of clouds, functions, their properties and threats of cloud computing would be also discussed.**

Keywords*— wireless sensor network; cloud computing; security; trust evaluation model

I. INTRODUCTION

A sensor network is a computer network including a number of sensor nodes. Sensor nodes are deployed densely in the network and have the interoperability. Usually the systems are small and cheap, so that they can be different based on type of use and function. Cost of sensor nodes is also different and based on size of sensor network and required complexity, different sensor nodes would be applied [1]. The relationship between sensor nodes using internet is mostly a subject that would be challenged. This can cause sense for integration of sensor network with internet [2]. At the same time, data of sensor network should be available every time and everywhere.

In cloud computing, instead of preservation of data on personal computer, the data would be saved on a server in internet and it is possible to store data on several computers and not only on one computer. The data would remain in cloud servers and until the time that internet is available and sufficient bandwidth is also available, one can send desired data to the server. Cloud computing is emerged as the Universal Operating System, which can provide open access to storage and software services. Using cloud computing can cause rapid and effective response and fast flexibility, accessibility and time saving. Combination of wireless sensor network with cloud computing can ease sharing and analyzing real time data. In cloud computing, sever can be physical device or virtual machine. The paper is organized as follows:

II. TOTAL STRUCTURE OF CLOUD COMPUTING, WIRELESS SENSOR NETWORK AND BASIC CONCEPTS

In this system, instead of installing several software programs on several computers, only software would be implemented and loaded one time and all people would have access to it through online services. The process is named as cloud computing. Cloud computing is a model for easy access based on request of user through the network to a set of resources with lowest need for resource management and having specialized information.

Cloud computing is changing into a strong network architecture for computations in large and complicated scale. Relevant issues of security in cloud computing have important role in reducing speed of accepting it. According to type of resources, cloud computing has been formed of 3 layers. Although cloud computing has abundant advantages and applications, trust and security is one of the considerable crises. Cloud computing is depended on considering security of data; although suitable solutions are available for the current problems surely.

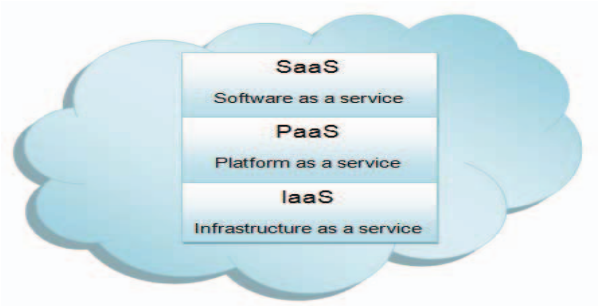


Fig. 1. Cloud computing layers deployment model

A. Cloud computing services [3]

978-1-4673-6506-2/15/$31.00©2015 IEEE

Cloud computing is formed of three layers, in which security should be considered and cloud can provide following three services:

1. Software as a service (SaaS): it is the highest layer that can place software as service on internet and as a result, need for installation of software on client computer would be met. This model provides services for clients based on their applications. No investment is required on client for the server and software permissions. Google is one of the servers of SaaS services.
2. Platform as a service (PaaS): it is the middle layer and is host of different environments for giving services. The layer feeds cloud software on implemented cloud infrastructure. PaaS can provide predefined combination of operating systems and software. Google apps motor is an example of PaaS.
3. Infrastructure as a service IaaS: it is the lowest level of infrastructure layer, in which processor, memory and hardware components would be presented by supplier of cloud service. IaaS is virtual context, which presents services. The model can provide basic storage and computing abilities as standard services on the network. Client usually deploys software on the infrastructure. Common example of IaaS is Amazon.

B. Implementation models of cloud computing

Four models have been presented based on deployment method:

1. Private cloud: the cloud infrastructures act in a unit organization and are managed by the organization or third party regardless of its location. The aim by establishment of a private cloud in an organization is maximizing and optimization of using existing resources (in home), providing security and protecting privacy to data and decrease in data transfer costs [4] from local IT infrastructures to public cloud. Private cloud can be applied for purpose of implementing cloud computing in a structure or local network and the model has no relationship with outside of the system. Private cloud provides possibility of having more control on all implementation levels and its advantage is providing more security. However, using private cloud can lead to increase in costs, since it needs hardware construction costs and employment of specialized workforce for maintenance of cloud.
2. Public cloud: in public cloud, organizations can use presented services by other organizations and can also provide their in-organization services for other organizations. This action allows companies to outsource their services and as a result, reduce service construction costs. Management and security of public cloud and is by Host Company of cloud. Cloud infrastructures are available for public and are belonged to supplier of cloud. Advantages of the model include low deployment cost, scalability and optimized use of resources. (One should just cost for the thing that is used).
3. Community cloud: several organizations that have common jobs and needs share their resources and services and create community cloud. In other words, cloud infrastructures have been created by a numbers of organizations commonly with a common policy of sharing resources.
4. Hybrid cloud: a combination of public and private cloud has been recognized as a hybrid cloud. In this model, suppliers of services can use services of suppliers of cloud completely or partially and this can cause more flexibility of using resources. Private model can be applied for sensitive models and public model can be applied for other services. Hybrid cloud can provide a combination of data and applied applications in more secure controlling and monitoring. In addition, the cloud has an open architecture, which allows being in contact with other management systems.

C. Overview of wireless sensor networks

Wireless sensor network architecture can be centralized or distributed. In centralized architecture, central node can be weak point and disadvantage of the network. If it is failed, whole network would be destroyed. Wireless sensor network distributed architecture can provide resistance against failure. Wireless sensor networks (WSN) include independent sensors of space distribution for cooperation with controlling physical or environmental conditions such as temperature, sound, vibration, pressure, movement or pollutants [1, 5]. Development of WSN has been along with military motivations using applied military programs like controlling battlefield. They are being applied currently in many industrial and non-military fields such as controlling industrial and control process, monitoring health of cars [6], environment and supervising habitat, healthcare plans and household automation and traffic monitoring [7, 1]. Sensor nodes can control conditions in different points such as temperature, humidity, movement of vehicles, Thunder and lightning conditions, pressure, soil array, noise level, presence or absence of special type of objects, mechanical stress level on connected objects and current features such as speed, direction and size of an object. Usually the sensor nodes include

components such as measurement, processing and communicating [8]. Development of sensor networks needs technology from three different scopes of research: measurement, communications and computations (such as hardware, software and algorithm). Some examples of initial sensor networks include radar networks applied in air traffic control. National Power Grid can be observed as a large sensor network with abundant sensors.

D. Applications of integration of WSN and cloud computing

Combination of WSN and cloud computing can ease sharing and analyzing data of real time sensor. Integration of the two technologies of sensor network and cloud computing is applicable for many applications. Sensor networks can be applied in many fields such as healthcare, environment and battlefield. Sensors are responsible for controlling and reporting the status. Some applications of sensor networks using cloud computing have been explained as follows:

- Supervision on Transportation control system [1]
- Military uses [9, 10]
- Ocean: in oceans, it can be applied For monitoring fishing [10]
- the weather forecast
- Healthcare [11]: there are some sensors for Circulation, respiration and ECG (Electrocardiogram) [12].

III. SECURITIES AND CHALLENGES IN CLOUD COMPUTING

Although cloud computing has abundant advantages and applications, trust and security is one of the considerable crises. Cloud computing is depended on considering security of data; although suitable solutions are available for the current problems surely. In regard with security of cloud environment, important notes are existed with different priorities (from environmental protection to protection of accessories).

A. Importance of security in cloud computing

Popularity of cloud computing is mainly because of the reality that many organizational applications and data are moving toward cloud operating system; although insecurity can be the main barrier for approval of cloud [13]. Many threats have been emerged in existing operating systems. Their security threats have been considered as high risk [14]. Figure 2 has illustrated the reality through Pyramid charts.

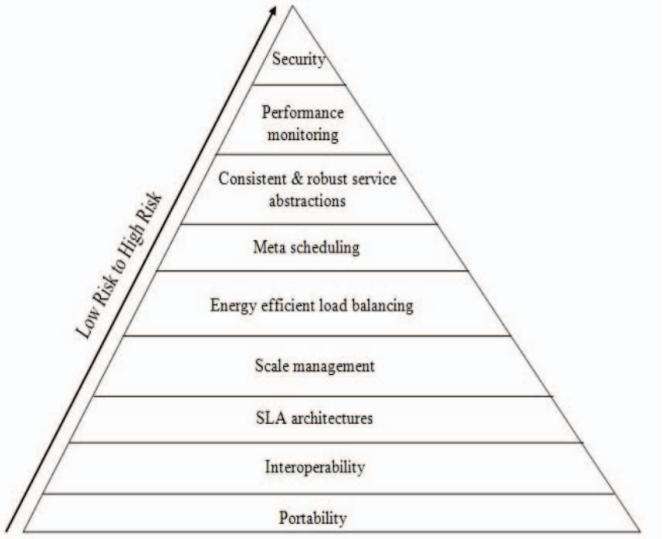


Fig. 2. Classification of threats based on risk factors [15]

A. Threats in cloud computing

Cloud computing may face many security threats existing in computing platforms, networks, intranet and internet. The threats can create vulnerability risks in several types. Searching on cloud computing threats can detect some security threats as follows [16, 17]:

- Failures in security supplier
- Attacks by other clients
- Accessibility and reliability issues
- Regulatory and legal issues
- Broken model about security
- Complete supplier of client security system
- Abuse and nefarious of cloud computing
- Insecure application program interface
- Malicious employees
- Vulnerability of shared technology
- Loss of data leakage
- Computation, service and hijacking traffic
- Unknown risk profile

B. Encryption techniques for cloud computing

Encryption of data is one of the solutions of security of cloud computing data [18]; although it can restrict efficiency of cloud computing. This is because; encrypted documents should be decrypted firstly. Previously, they could be manipulated and searched. In addition, cloud computing data should be encrypted before storage. Conducting encryption and decryption on large scale data set can be expensive and time consuming.

C. Secure protocols in wireless sensor networks

Protocols of sensor networks would be classified in two groups: 1- network structure based and 2- protocol operation based. Network structure would be also classified to three groups based on routing protocols: 1- flat based routing 2- hierarchical based routing and 3- location based routing. Protocol based operations would be also divided as follows: 1- multi-path routing based, 2- query-based, 3- Quality of service (QOS) based, 4- integration based and 5- negotiation based. In platform based routing, all nodes are in same level and have equal functions or sensor nodes have the Interoperability with each other for doing tasks. Some examples of platform protocols are GBR [19], MCFA [20], SPIN, [21, 22] Rumer Routing [23] and so on.

In hierarchical or cluster based routing, nodes have different functions in the network. In hierarchical structure, nodes with higher energy would be applied for processing and sending data; although low-energy nodes can be applied for purpose of conducting measurement and evaluation close to the target. It means that creating clusters and allocating special tasks to the Custer Head (CH) can help to wide extent to scalability of whole system, lifetime and saving energy. Some examples of hierarchical based routing protocols are SOP [24], VGA [25], and HPAR [26] and so on.

In location based routing, position of sensor nodes can be applied due to the rout of data in the network. In this kind of routing, sensor nodes would be called using their location. The distance between neighbor nodes can be estimated based on power points of input signal. Relative coordinate of neighbor nodes can be obtained with dada exchange between neighbors [27, 28, 29]. Some examples of protocols are Global position system SPAN [30], GPSR [32] and GPS [32] and so on.

D. Trust evaluation model [33]

In trust evaluation model, supplies would be divided to two provider supplies of Cloud Server User Provider (CSP) and Cloud User (CU) in cloud computing. Trust evaluation is depended on evidence of interaction between CSP and CU. Interaction and measurement between CSPs and Cus are relevant data of evidence. Evidence set (E) is as follows:

$E = \{E_1 + E_2 + \cdots E_i + \cdots E_k\}$

In the process of estimating trust, only valid evidence can affect degree of trust of supplies.

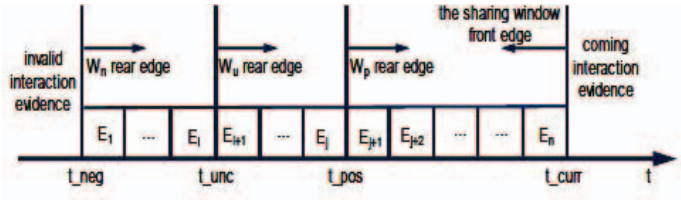


Fig. 3. Sliding window mechanism [33]

T curr refers to current time; t pos, t unc and t neg are vital times. Size of time window has been illustrated with S_n, S_p and S_u $(S_p \le S_u \le S_n)$ for W_p, W_n and W_u. The quantitative equation would be as follows:

$$\begin{cases} |t\_curr - t\_pos| = S_p \\ |t\_curr - t\_unc| = S_u \\ |t\_curr - t\_neg| = S_n \end{cases} \quad (1)$$

In the process of estimating trust, only evidence of trustable interaction can affect degree of trust of supplies. Hence, degree of trust of supplies can't be increased or decreased along certain range. In addition, negative interaction window is larger than positive interaction window. Therefore, evidence of negative interaction can affect trust of supplies for longer times.

A. Direct trust

Each of evidence can be considered as an interaction. αCode refers to evidence of positive interaction and β indicates negative interaction evidence and γ refers to uncertain interaction evidence. In t time, number of each type of direct interaction between I and j can be depicted as $\alpha_{i,j}^t$, $\beta_{i,j}^t$ and $\gamma_{i,j}^t$. In t=t0, no interaction is existed between supply f I and j; therefore, the equation is $2^{\Omega} = \{f, \{T\}, \{-T\}, \{T, -T\}\}$. Here, $\{T\}$, $\{-T\}$ and $\{T, -T\}$ refer respectively to trust, distrust and distrust-impossibility. Here, $u \in [0,1]$ is a weight factor. Interactions beyond the window size can be considered as non-reliable and wrong evidence and such evidence would not be mentioned in the estimations.

B. Trust

Existence can obtain advice data from other existences, which have so far been in contact with evaluated existence. S has direct relationship with j. j can obtain advice data about j from s based on direct trust of s to j as follows:

$$rt_{s,j}^t = \left(rm_{s,j}^t(\{T\}), rm_{s,j}^t(\{-T\}), rm_{s,j}^t(\{T,-T\})\right)$$

In trust network, more than one advice data set is existed about different existences. According to Dempster Rule, one can combine the advices. Weight of each advice has been depicted as ω_s .

$$rt_j^t(A)=rt_{1,j}^t(A)\oplus rt_{2,j}^t(A)\oplus\ldots\oplus rt_{q,j}^t(A),q=1,2,\ldots,m,A\neq f,A\in 2^{\Omega} \quad (2)$$

IV. TEST EVALUATION

A. Simulation arrangements

In simulation tests, CSPs and CUs are independent. CSPs have been classified in three categories: good CSP, bad CSP and random CSP. Their relevant ratios in all CSPs are equal to 80%, 10% and 10% and different types of services would be presented by the as follows:

1. Good CSP always presents trustful services
2. Bad CSP always presents trustless services
3. Random CSP presented trustful and trustless services randomly.

CUs have been classified in three groups: trustful CU, bad CU and random CU. Proportional distribution of each type of CU is similar to CSP.

1. Trustful CU always takes lawful measures.
2. Bad CU always takes unlawful measures
3. Random CU takes lawful and unlawful measures randomly.

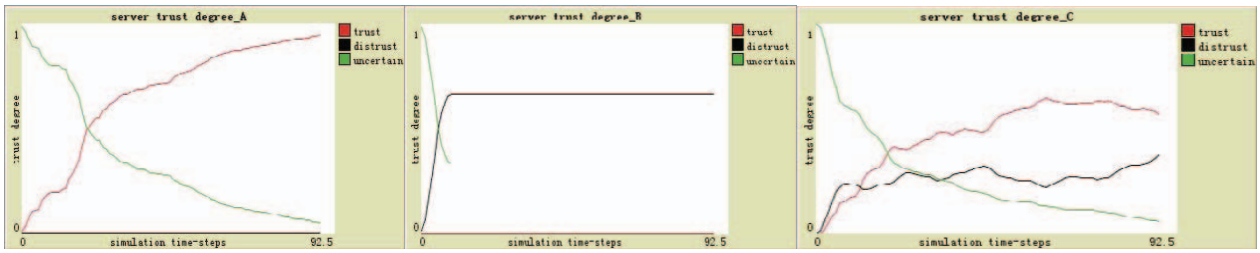
TABLE1. Summary of applied parameters in simulation test [33]

Parameter	Description	Value
n	Number of CSPs	50
m	Number of CUs	200
u	Weight factor	0.2
S_p	Size of positive interaction window	50
S_u	Size of uncertain interaction window	80
S_n	Size of negative interaction window	150

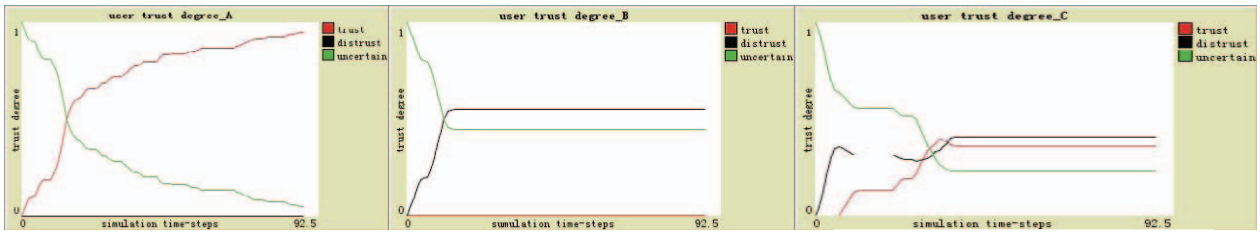
B. Effectiveness of proposed model

The results of tests are as follows. Figure 4 indicates change in degree of trust for 3 types of existence. Reliability of good or trustful existences continues its growth more and less; meaning with constant and continuous accumulation of positive interactions. On the contrary, because of negative interactions, reliability of bad existence would be decreased. When the degree of distrust achieves certain level, bad existences would have no change.

The reason is that if the degree of trust is assumed higher than threshold level, existence would be bad and they would not be allowed to have interaction with other ones. Therefore, trust degree of bad existence would be changed more than others. For random existences, change in behavior can lead to change in believability of random existences. Moreover, trust of the existences would be developed slowly and distrust would be developed fast. This helps feature of sliding window. In sliding window mechanism, positive interactions are right for a short time and negative interactions are right for long time. Therefore, trust of the existences can be increased by the recent positive interactions. However, negative initial interactions have bad effect on trust rate of the existences, so that distrust rate of them would be increased rapidly.



a. trust degree of good CSP b. trust degree of bad CSP c. trust degree of random CSP



d. trust degree of good CU e. trust degree of bad CU f. trust degree of random CU

Fig. 4. Changes in trust degree in different existences [33]

C. System counter attack

Successful interaction rate is the ratio of successful interactions to overall interactions in simulation time and can indicate system counter attack in certain environment. Therefore, due to the successful interaction, system counter attack can be measured. Using trust computing based on theory of evidence and sliding windows, bad existences can be determined effectively.

One can restrict interaction of bad existences more than before. Obtained results indicate that successful interaction rate with calculation of numbers is more than it without trust computations. According to figure 5, change in successful interaction rate can be divided to two steps including decrease and increase steps. Successful interaction rate can be decreased with the increase in bad interactions at the first.

After a while, successful interaction continues increasing regularly. This is because; the system computes trust to determine bad existences and avoids supplying services for them. Obtained results also indicate that trust computing can affect system counter attack, since it can help the system to determine bad existences properly and accurately.

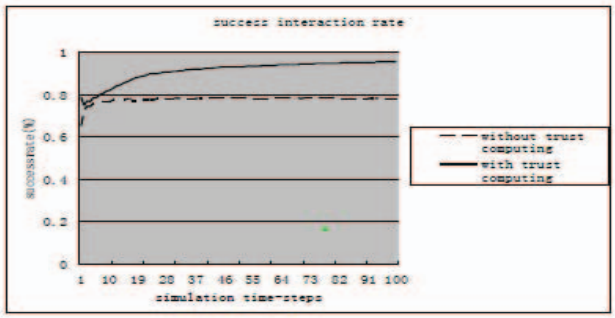


Fig. 5. Successful interaction rate [33]

V. CONCLUSION

The interaction between sensor nodes using internet is a challenging action. At the present study, wireless sensor network (WSN) has been integrated with cloud computing. In order to be able to support large volume of data, the current solution is using cloud computing. Accordingly, using cloud computing in wireless sensor network seems clear. As wireless sensor networks are restricted in regard with ability of processing, battery lifetime and communication speed, cloud computing can be applied instead of it, which can make it attractive for long-term observations, analysis and using it in different types of environments and projects. Every program should consider types of threats properly based on emerging technology. In addition, encryption system is suitable for enhancement of network security policies and also security of sent and received messages. The project can be implemented and supported in local network. Trust evaluation model has been presented based on theory of evidence and sliding

window for cloud computations. Its advantage is its simple implementation. If n is number of CSP and m is number of CU in the system, time complexity of algorithm would be O (n×m). In sliding window mechanism, interactions can be divided to right and wrong interactions. Only right interactions can affect trust degree of existences and hence, they can improve the ability to expand the system. Simulation tests indicate that trust degree of existences can be increased slowly using the proposed model and can be decreased rapidly. It can determine bad existences effectively and can also provide certain and trustable data for making security decisions for the system.

REFERENCES

[1] K. Romer, F. Mattern; "The Design Space of Wireless Sensor Networks"; IEEE Wireless Communications, pp. 54-61, December 2004.

[2] C. Ulmer, L. Alkalai and S. Yalamanchili, Wireless distributed sensor networks for in-situ exploration of mars, Work in progress for NASA Technical Report. Available in: http://users.ece.gatech.edu/

[3] F. Njeh And Dr. B. Yang "a secure cloud-enabled wireless sensor network platform", Department Of Computer Science Bowie State University, Bowie, Maryland 20715, International conference on grid computing and applications 2012.

[4] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "Above the clouds: A Berkeley view of cloud computing," *EECS* Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28, 2009.

[5] T. Haenselmann (2006-04-05). Sensor networks. GFDL Wireless Sensor Network textbook. http://pi4.informatik.uni-mannheim.de/~haensel/sn_book. Retrieved 2006-08-29.

[6] A. Tiwari, P. Ballal, F. L. Liwes, "Energy-efficient wireless sensor network design and implementation for condition-based maintenance", ACM Transactions on Sensor Networks (TOSN), http:// portal.acm.org/citation.cfm?id=1210670

[7] S. Hadim, N. Mohamed (2006), "Middleware Challenges and Approaches for Wireless Sensor Networks", IEEE Distributed Systems Online **7** (3): 1, doi:10.1109/MDSO.2006.19, http://doi.ieeecomputersociety.org/10.1109/MDSO.2006.19 art. no. 0603-o3001.

[8] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazine, August, 102 114(2002).

[9] C.Y Chong, S.P. Kumar, "Sensor networks: Evolution, opportunities, and challenges", Proc IEEE, August 2003.

[10] E. Shi, A. Perrig; "Designing Secure Sensor Networks"; IEEE Wireless Communications, pp. 38-43, December 2004.

[11] V. J. Singh, D. P. Singh, Dr. K. L. Bansal, "Proposed Architecture: Cloud Based Medical Information Retrieval Network", International Journal of Computer Science & Engineering Technology (IJCSET) Vol. 4 No. 05 May 2013.

[12] W. B. Heinzelman, A. 1. Murphy, H. S. Carvalho, M. A. Perillo; "Middleware to Support Sensor Network Applications"; IEEE Network, pp. 6-14, January/February 2004.

[13] B. Joshi, A. S. Vijayan, B. K. Joshi, "Securing Cloud computing Environment against DDoS Attacks", IEEE, pp. 1-5, 2011.

[14] A. Bakshi and B. Yogesh, "Securing cloud from DDOS Attacks using Intrusion Detection System in VM", IEEE, pp. 260-264, 2010.

[15] Dr. R. Sridaran,N. kilari, " A Survey on Security Threats for Cloud Computing", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 1 Issue 7, September 2012.

[16] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, J. Molina. Controlling Data in the Cloud Outsourcing Computation without Outsourcing Control. CCSW '09**:** Proceedings of the 2009 ACM workshop on Cloud computing security, pp. 85-90. November 2009.

[17] S. Hanna. A security analysis of Cloud Computing. Cloud Computing Journal. DOI = http://cloudcomputing.syscon.com/node/1203943

[18] M. Y. A. Raja AND S. Ahmed, "Tackling Cloud Security Issues and Forensics Model", IEEE, pp. 190-196, 2010.

[19] C. Schurgers and M.B. Srivastava, "Energy efficient routing in wireless sensor networks", in the MILCOM Proceedings on Communications for Network-Centric Operations: Creating the Information Force, McLean, VA, 2001.

[20] F. Ye, A. Chen, S. Liu, L. Zhang, "A scalable solution to minimum cost forwarding in large sensor networks", Proceedings of the tenth International Conference on Computer Communications and Networks (ICCCN), pp. 304-309, 2001.

[21] W. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks," Proc. 5th ACM/IEEE Mobicom Conference (MobiCom '99), Seattle, WA, pp. 174-85, August, 1999.

[22] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," Wireless Networks, Volume: 8, pp. 169-185, 2002.

[23] D. Braginsky and D. Estrin, "Rumor Routing Algorithm for Sensor Networks," in the Proceedings of the First Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA, October 2002.

[24] L. Subramanian and R. H. Katz, "An Architecture for Building Self Configurable Systems", in the Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing, Boston, MA, August 2000.

[25] J. N. Al-Karaki, R. Ul-Mustafa, A. E. Kamal, "Data Aggregation in Wireless Sensor Networks - Exact and Approximate Algorithms", Proceedings of IEEE Workshop on High Performance Switching and Routing (HPSR) 2004, Phoenix, Arizona, USA, April 18-21, 2004.

[26] Q. Li and J. Aslam and D. Rus,"Hierarchical Power-aware Routing in Sensor Networks", In Proceedings of the DIMACS Workshop on Pervasive Networking, May, 2001.

[27] N. Bulusu, J. Heidemann, D. Estrin,"GPS-less low cost outdoor localization for very small devices", Technical report 00-729, Computer science department, University of Southern California, Apr. 2000.

[28] A. Savvides, C-C Han, aind M. Srivastava,"Dynamic ¯ne-grained localization in Ad-Hoc networks of sensors," Proceedings of the Seventh ACM Annual International Conference on Mobile Computing and Networking (MobiCom), pp. 166-179, July 2001.

[29] S. Capkun, M. Hamdi, J. Hubaux,"GPS-free positioning in mobile ad-hoc networks", Proceedings of the 34th Annual Hawaii International Conference on System Sciences, pp. 3481-3490, 2001.

[30] B. Chen, K. Jamieson, H. Balakrishnan, R. Morris, "SPAN: an energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks", Wireless Networks, Vol. 8, No. 5, Page(s): 481-494, September 2002.

[31] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless sensor networks", in the Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '00), Boston, MA, August 2000.

[32] Y. Xu, J. Heidemann, D. Estrin,"Geography-informed Energy Conservation for Ad-hoc Routing," In Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 70-84, 2001.

[33] X. Wua, R. Zhang, B. Zeng, S. Zhou, "A trust evaluation model for cloud computing", Procedia Computer Science 17, pp. 1170 – 1177 , 2013.