International Journal of Advanced Science and Technology
Vol. 29, No. 08, (2020), pp. 2278- 2286

# Trust Based Secure Architecture for Wireless Sensor Networks

Amish Anant[1], Gouthaman.P[2], Rahul Mishra[3] and Anwar Basha.H[4]

*[1, 2, 3] SRM Institute of Science and Technology, Kattankulathur, [4]SRM Institute of Science and Technology, Vadapalani*
*[1]amishanant13@gmail.com, [2]gouthamanps@gmail.com,*
*[3]mishra.rahul959@gmail.com,[4]anwar.mtech@gmail.com*

***Abstract***

*In this digital era, Security is the utmost requirement for any person irrespective of the context in which they are dealing with. The future of technology is leading to an era of automated system with minimum human intervention. The most prominent technology that is being widely used around the world is Internet of Things (IoT). IoT can be defined as a network of embedded devices, which interact with their own to achieve desired goals. For instance, one physical device is able to interact with another physical device on its own and is able to perform particular transactions according to the situation, thereby leading to a smart place. Perhaps, there are various issues to be dealt in this domain but the imperative one is mobility. This article deals with the mobility issues in the IoT domain and the proposed solution uses Trust hierarchical management system. Moreover, this proposed structure can be suggested to various domains which comprises of IoT as a basic foundation. In our work, we have developed a framework for modeling trust within the hierarchical ad-hoc sensor networks. It promotes mobile sensor nodes to get created, preserve and exchange trust opinions under limited overseas in terms of intricate computations at sensor nodes.*

***Keywords:*** *Security, Trust value, Nodes, Cluster, Sensors, Wireless networks, Optimization*

## 1. Introduction

Internet of Things primarily comprises of plethora of wireless devices connected to each other through a network which may be secure or insecure. As said earlier, it consists of spatially distributed objects which are communicated through wireless channel, due to which there are high possibilities of security threats [1]. Being a lot in number and also smaller in size, it is one of the most challenging tasks to implement huge security principles on such diminutive devices. The demand for the security of these devices is critical and for this purpose, a novel strategy is necessary to be devised which will mend possible issues in regards to this domain. It must be designed in such a way that it binds the link between the virtual and the real world. The IoT domain has been discussed in various papers elucidating details of all components. The below section discusses that to gain additional knowledge which are necessary for the proposed methodology.

## 2. Related Works

The section begins with components of IoT and then proceeds towards applications of IoT. The most basic components of IoT are RFID, Sensors, GPS and NFC. Firstly, RFID (Radio Frequency
Identification) is a chip based technology, primarily focusing towards implementing the


ISSN: 2005-4238 IJAST

concept of wireless networking. It utilizes electromagnetic field to identify objects which are available within the domain. For instance, as soon as an object is connected with a specific RFID, it penetrates the domain then it is immediately detected by the device [2]. It is a passive device, that is, it works using the power provided by the signal received from the detecting device, and then sends this power to the chip for further functioning. Perhaps, these days there are RFIDs which are battery driven and are not passive in nature.

Secondly, Sensors, which are also known as smart devices, as they assist in providing time to time information about the changes in the environment, which is one of the most significant factor for the automation of several devices. This can be used as an input for any further process. The primary issue with these devices is that they are huge in numbers and they need to be managed in an appropriate manner. To be specific, there may be instances when majority of the whole list of devices start sending inputs simultaneously, thereby leading to lot of traffic on the main server. This could end up in confusion on which one to be selected and in order to decide upon this choice, it requires humongous background work.

Next is, Global Positioning System or GPS, which is one of the recent advancements in this domain. This assists in identifying the position of a specific entity. The entire process is carried out in a grid view with the help of a satellite that constantly supports the system and aids in tracking the precise points of the entity. Finally, Near Field Communication or NFC is the one that comes under communication domain of IoT environment. The communication domain comprises of several technologies such as, 2G, 3G and 4G. With NFC's application, the data transfer is made easier. It is a radio device which works on a frequency of 13.6 MHz and it can establish communication between any two devices when they are in the range of 20cm with maximum data transfer speed of 424kbit/s under duration of less than 1/10 of a second. This technology mainly solves the problem of slow data transfer, which could lead to more security threats, that is, greater the duration, higher are the chances of threats and phishing.

Using the above technologies, an environment is created which seems to be a lot fictional but can be made to exist in the real world. When it is implemented, the task performed by a person can be reduced to the maximum regardless of the domain. However, this remains an ideal thought due to the security issues which are encountered in this domain. For instance, RFID once implemented, there are high possibilities of duplications and may be used by any person for exploiting the data which could be private to someone [3].

The following section discusses about the various applications of Internet of Things. First, Smart Home, the automated homes unambiguously materialize, currently known as the most astonishing application of Internet of Things in every means. Currently, in a month individuals more than 50,000 searches online for Smart Homes and it is not something to be surprised of. The data from IoT analytics organization for Smart home includes nearly 256 organizations and many more novel businesses. There are many organizations which are vibrant in smart homes than any other applications in the field of IoT. Recently, the cumulative sum of expenditures done by companies for Smart homes has exceeded $2.5billion. Second, Wearables are becoming more and more popular. As customers anticipate the launch of Apple's new products, there are many other wearable deals from other major competitors. With all of the newly available IoT organizations, wearables manufacturer Jawbone has been in all means the finest financing to date. It retains in the larger section with billions of dollars! Third, Smart city exceeds a broad combination of usage situations, starting with development organization leading towards water scattering, then misuse of organization, metropolitan security and general surveillance [4]. The reputation is accumulated by means of various smart city plans assurance to alleviate genuine anguish of consumers staying in urban territories these days. IoT projects in the stream of smart city deals with action obstruct problems,


ISSN: 2005-4238 IJAST

reducing bustle and sullying thereby leading towards securing urban territories.

Next, Smart grids are an exceptional one. A futuristic network assures to utilize data with respect to the procedures of energy suppliers and consumers in an automated manner so as to improve the effectiveness, resolute quality along with financial features of energy. Then, Industrial internet which refers to contemporary web, that is one of the most outstanding IoT applications. Despite the fact of numerous market examinations, for instance, Gartner or Cisco views the contemporary web as the IoT inspiration with the well-known potential, its notoriety currently doesn't achieve the same as automated homes or wearables do. The contemporary web yet has a grand deal pulling out every delay. The automated web gets the supreme thrust of Twitter individuals (approx. 1700 tweets per month) in comparison with non-customer positioned IoT initiatives.

Subsequently, connected car which is related to automobiles has been recently thriving. Using the recent research, it is inferred that the change cycles in the automobile sector takes nearly 2 to 4 years [5]. However, there has not been such huge impact created in this industry. Despite, it appears to be announcing about its plan to venture into this domain. Furthermore, Digital health refers to associated wellbeing which remains to be the dozing goliath with respect to IoT applications. The design of connected human services structure as well as keen restorative devices stand colossal potential, this is not with the case of organizations but for the affluence of individuals when it is successfully implemented. However, digital health has not attained the maximum level. Visible applied cases and immense level startup accomplishments are yet to arrive. Smart retail is another application which is on the basis of publicizing proximity and it is in its infant stages. However, the notoriety state portrays that it is as yet an area of expertise segment. Final one is Smart farming as it has been well-known that intense agriculture is an often ignored business-case for IoT as it does not easily fit into the prominent classes, for instance, welfare, portability or automation. In any scenario, due to distant farming procedures and extensive quantity of tamed animals which could be supervised using the Internet of Things may change the way how farmers work. As of now, this notion has not yet reached towards vast level consideration.

The drawbacks in Internet of Things are firstly about having an insecure web, cloud and mobile interface. Second is insufficient authorization and unavailability of options for security configuration. Third is about network services and communication protocols which are not effective enough [6]. Final one is deficiency of transport encryption and poor physical security.

### *EXISTING SYSTEM*

Internet of Things promotes the feasibility of remotely interfacing as well as validating certifiable devices using the internet. With respect to our home, this initiative can be appropriately appended to formulate it as more intelligent, secure and automated. This newly formed IoT technique focuses towards creating a smart remote home security structure that communicates alerts to the owner by making use of the internet when there are any intrusions. In addition, similar methods can be utilized for home automation by applying sensors towards similar arrangement. The inspiration of this technique was through the post examination of currently available frameworks which alerts and sends status through the Wi-Fi associated microcontroller administered framework which can be received in the client's telephone from any division irrespective of whether the mobile phone is connected with the internet. The microcontroller implemented in this proposed model is TI-CC3200 launch pad board which comprises of a small scale controller installed along with a locally present Wi-Fi shield thereby making use of it to control and supervise the electrical machines within the house.

The following section discusses about the significance of security in sensor networks in


ISSN: 2005-4238 IJAST

which it details about where, what and how to detect for [7]. The first is about, where to detect, that is, where the data exists, such as, zero trust/software defined networks, virtualization/containerization, service orchestration/devops/elastic compute [8]. Next, what to detect, this can be achieved through non-event based raw activity wherein there is a necessity of passive feed of the activity as it happens with respect to network, system process & storage, application state and user activity.

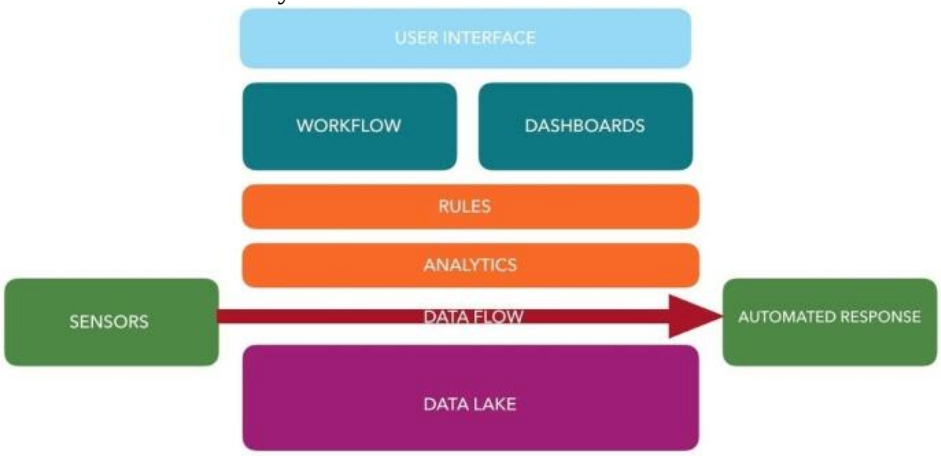


**Figure 1. Sensor Network Security Flow**

Finally with respect to the query on how to detect, this can be attained through collection of evidence. In relation to the procedure about how to forward, the process involved are Micro-batching, Priority based forwarding and secure transfer. Starting with, micro-batching is necessary since network connections are always unreliable and the ability to store versus drop data is one of the core requirements. Next is to have priority based forwarding as every activity is not significant. For instance, sending the fact that the fire alarm just went off is more critical than updating the last three hours of temperature data. Finally is to focus on secure transfer since the application may run anywhere such as cloud platforms, moving the data across secure networks is vital for maintaining confidentiality and integrity of the data [9].

The key focus or the problem definition here is to have intrusion detection in the system, maintaining the whole system throughout the working process, devising a proper cryptographic system to protect it, provisioning of proper communication protocol under several systems and maintaining records of previous intrusions and proper recognition of outliers [10].

## 3. Proposed Methodology

The current system of wireless networks in an ideal environment is running without the implementation of any security protocol. Due to which, the whole network is exposed to highly risky and dangerous security attacks which will tamper the genuineness of the data being transmitted to various systems associated with the sensors.

The proposed methodology is based on Trust Management and Hierarchical Topology for the whole system. It integrates the security in the system using the trust value, which is a variable depending upon factors like location, latency, value, etc. The hierarchical topology is implemented by master-slave architecture, where slaves are systems made via clusters and


ISSN: 2005-4238 IJAST

master is a high-power server.

All the nodes are placed in a single cluster. There is a sponsor node that acts as head of the cluster. The factors to be looked out are firewall breach, manual/physical breach, time threshold, device threshold, value threshold, check time, check value, device count threshold, trust threshold, cluster output count threshold.

The working is as follows. Each node will be transmitting its data value to the Sponsor node, which calculates the trust on the basis of value received and the following algorithm:

**STEP 1:** The value received is pushed into the table, where the previous value from the respective node is reported.

**STEP 2:** Initially, a constant Trust value is being assigned to all the nodes.

**STEP 3:** The received value is then being compared with the previous value from the same node.

**a.** Now if the value has varied in the range of value threshold for the type of device, then it will be registered successfully and a new trust value will be updated to the trust table of the Sponsor node.

**b.** But if the value has varied highly away from the value threshold of the device, then the following actions will take place:

**i.** First, a security test will be run for the perimeter of the cluster [11].

**ii.** If the security test comes clean, then the detection of manual/physical breach will be taken into consideration.

**iii.** For detecting physical/manual breach, two main factors are taken into consideration, namely Time and Distance

**iv.** If a given node reports erroneous data, then the devices in the affinity of the node will be checked for the trust.

**v.** This trust value of the mentioned devices will be recalculated immediately for Check time, as it may be a case, that these also report the same value which was being reported by a defect node, in which case, the node under scrutiny can be assumed to be safe and its trust value can be changed back to normal range.

**vi.** If the trust value of those devices is affirmative, then the node reporting erroneous value will be placed under scrutiny for Check time and even then if the value from the defective node keeps going away from the Value threshold, then it will be immediately termed under compromised status and the trust value for that node in the trust table will be termed as null and the value received from that node will be termed irrelevant.

**vii.** But if the value from the defective node comes back to normal within the check time, then its trust value will be decreased and the percentage of contribution of this node to the final dataset will also be affected.

**c.** Now the value will be stored into the table in the sponsor node from various nodes with their corresponding trust value.

**d.** To calculate the most accurate output, the best values are selected on the basis of the device count threshold, which also determines whether a cluster is good or not [12].

**e.** If the number of devices that are under a good trust threshold is greater or equal to the device count threshold, they all can be used for final output calculation.

**f.** But if the number of devices is less than the device count threshold, then the cluster is termed as bad cluster and the output from the cluster is being ignored.

**STEP 4:** Now the sponsor node will transmit the final output to Supernode, which basically stores the trust values from several other clusters and keeps comparing them to output received from the same cluster prior to this value.

**STEP 5:** If the value varies from the threshold value then the same process is repeated for the cluster which is followed for child nodes.


ISSN: 2005-4238 IJAST

**STEP 6:** The final trust value of a cluster is calculated by taking into consideration the trust values of each of the nodes, whether its good or bad.
**STEP 7:** If this final value comes under the general trust threshold for the cluster, its term good else it is termed as bad cluster.
**STEP 8:** Also, sponsor nodes talk among themselves and communicate their direct trust value which is nothing but the calculated average trust value of a given cluster.

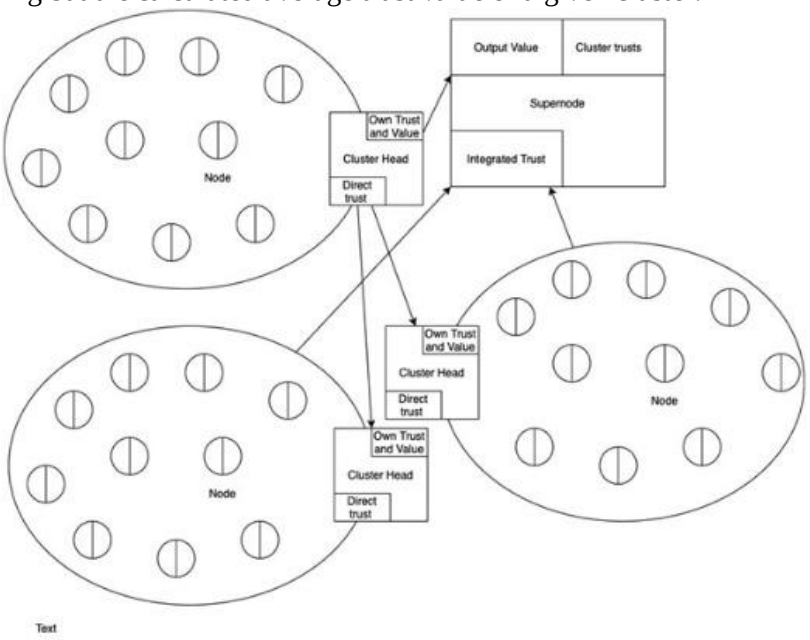


**Figure 2. Architecture of the System**

**STEP 9:** The purpose of this is that supernode doesn't need to inform the clusters about the faulty cluster as they will already know about it via their transmission. This data is also transmitted to the supernode from each cluster, which then calculates the final trust value for each cluster based on trust values received from other clusters, compares it to the value received from individual cluster under examination, and if it matches, it is termed as bad else if doesn't match then it repeats this operation within time threshold on cluster level for cluster output count threshold times and then declare its final result.
**STEP 10:** If the value turns out to be faulty then all the clusters in the network are notified about the bad cluster and security test is run for the whole network and breaches are identified.
**STEP 11:** The network goes under high vulnerability for security check duration if the above scenario occurs and trust calculation is stopped as all the values can be tainted.
**STEP 12:** The integrated trust is calculated at regular intervals by the supernode to keep in check the security of the whole network system.

## 4. Implementation

Trust Management System is one of the concepts which can help in eradication of security to a certain level [13]. It is a mathematical model, which has been taken from the modified part of the assumption taken in the latter is, let the devices be mobile & they lie inside a particular range. It deals with the problem faced in an environment consisting of a number of wireless devices.


ISSN: 2005-4238 IJAST

It is a hierarchical model consisting of several wireless sensing devices. This model consists of 3 nodes abstractly, such as command, cluster head along with abundant sensor nodes collated into a cluster. They can be formed on any grounds, namely their capabilities, their location, or their communication range etc. It is primarily super node trust based architecture. It is a node based architecture too, hence there are several nodes inside the model, in them only, one is super node, which is having high computational power, storage and power communication in comparison with other nodes.

There is also a trust calculating function, which calculates the trust for each node, and a decaying function, which gives a proper idea about which device should be called first for any operation. Basically, this model strategizes on the principle of grouping. It groups the whole lot into groups, called clusters, which consists of some particular number of sensors.

Each sensor primarily probes its surroundings, collects the data thereby finally communicate the data gathered directly to their cluster head. This can be done either in a single go, or may be by a technique called hopping. Hopping is a way of movement in which data is transferred from one point to other, by hopping from various nodes, according to the trust value they have, i.e. the node on the way which is having a higher trust value, will be considered upon the one, with lesser trust value.

Each sensor group or cluster is having a head, called the cluster head for that particular group. These cluster head have the capability to reach any of their nodes in the group & organize every sensors within the group [14]. Every cluster head receives data from various sensors, processes the data to obtain appropriate information & then forward it towards the base station, which is another station located, and may be outside the range or in the range.

Sponsor node, is the node which initiates all the operation which needs to be performed. Here, according to the application, any node could be the sponsor node. A target node refers to the node which is selected by the sponsor node, that is, it is the node to which the final information needs to be sent. It's possible that at a time we can have more than one target node.

Working of the whole system is very simple. Every node accumulates the complete direct trust values of every other nodes in the same cluster. Next, each node forwards all these direct trust values to cluster head, later which the cluster head calculates the indirect (group) trust information for every node in the cluster. In addition, it stores its own direct trust value. Therefore, the cluster head computes the integrated trust value from the obtained data.

The 2 parameters for direct trust calculation are value of successes ($S_i$) & value of cumulative cooperation ($CC_i$). Therefore, direct trust value is:

$$t_{Ai} = [100*S_i/CC_i] \quad (1)$$

For instance, if we have $CC_i=4$, then number of success, that is, $S_i$ will lie between 0 to 4, that is for each cumulative cooperation, there will be a particular associated success value, the values which we get are given in the following table. Once we have obtained our values, we use the concept of decaying function, α, so the new trust value is

$$T_A = [((100-\alpha)/100)*t_A + (\alpha/100)*t_{anew}] \quad (2)$$

where function, α, lies between certain values. If the trust value during the recent time is high, then it is understood that the overall trust value will differ by a diminutive amount and vice versa. Overall trust value:

$$T_{s,t} = \sum_{i=1}^{n} T_{Ai} / (\sum_{i=1}^{n} T_{Ai} + \sum_{i=1}^{n} (1 - T_{Ai})) \quad (3)$$


ISSN: 2005-4238 IJAST

For intra cluster trust management calculation, we make a matrix, for each node with respect to other node trust value, and store it in a cluster head main node. & finally for integrated trust computation we make a matrix again & it consists of separate trust values for group, cluster heads & base station. Gi, Group trust value,

$$G_i = \sum^{n}_{j=1} T_{Ai} / (\sum^{n}_{i=1} T_{Ai} + \sum^{n}_{i=1} (1-T_{Ai})) \quad (4)$$

Finally, the integrated trust value is:

$$I_i = G_i * W_{group} + T_{ch,i} * W_{ch} + T_{bi} * W_{base} \quad (5)$$

Where ch denotes cluster head, b denotes base, & W stands for weight.

**Table 1. Values recorded against entire duration**

| $CC_i$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| $S_i$ | 2 | 1 | 0 | 1 |
| $t_{Aik}$ | 200 | 50 | 0 | 25 |
| $t_{Ai(k+1)}$ | 220 | 10 | 30 | 52 |
| $T_{ai(k+1)}$ | 204 | 40 | 7 | 31 |

For example taking it in a real scenario, let's take an example of a room, in which we have several automated devices. It is all automated once the user enters the room. The starting mechanism works with the detection of the RFID of the user, there can be some preliminary security tests, once the user enters then all devices get activated on their own. Now let's consider the system is design is divided in time slots. If the user enters in slot A, then a particular set of actions will be performed by the server, and if in B, then another set will be performed.

Now to transfer the information, the server or base station, will send the signal, it will check the retrieval code which will contain the trust value of that node, now this node, whose trust value will be the highest among all, will search for next trustable node, like this we will reach the final node, which will be the target node.

**Table 2. Values recorded for graph plot**

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| $T_1$ | X | 4 | 5 | 9 |
| $T_2$ | 8 | X | 6 | 3 |
| $T_3$ | 21 | 1 | X | 18 |
| $T_4$ | 16 | 1 | 7 | X |
| $T_a$ | 23 | 0 | 19 | 27 |
| $T_b$ | 36 | 63 | 90 | 15 |

This can employ various shortest path techniques to get the work done as soon as possible. To check whether the user is genuine or not, further future techniques can be used such as Artificial Intelligence. In order to execute this implementation, the software utilized were NS2 simulator, Windows 7, Cygwin, Server (Xampp) and the hardware such as Raspberry Pi 3


ISSN: 2005-4238 IJAST

Model B, Arduino Uno, Jumper Wires, HC SR04 Ultrasonic Sensors, HDMI Cable.

## 5. Conclusion

According to the structure of the hardware implementation, the working ultrasonic sensors continue receiving data and transmitting it to the database. The defective sensor ,which has been altered or tampered or attacked, resets itself and keeps sending null or zero value for the entire duration of communication. Keeping in mind the signals are being received by the source which is placed within a distance of 200 meters. The model has been designed to receive signals for duration of around 10 minutes withstanding which all the signal values are reset and recorded again, storing the prior values in the database.

Now the signals from the defective sensor are studied and examined and if the values continue to be null for the entire duration of the run, then an indication is sent to the admin which in turn sends a notification to the entire system to ignore the values from the defected node, having discovered that the particular sensor has been attacked and it's trust value has been compromised. That is how the system works in a real life IOT scenario with the sensors being different appliances and the admin being the central security system.

## References

[1] M. Sharma, "Wireless Sensor Networks : Routing Protocols and Security Issues", *Fifth Int. Conf. Comput. Commun. Netw. Technol.*, pp. 1–5, 2014.
[2] O. Ozturk and M. Vajapeyam, "Performance of VoLTE and Data Traffic in LTE Heterogeneous Networks," *2013 IEEE Glob. Commun. Conf.*, no. Dl, pp. 1595–1601, 2013.
[3] Z. Ren, X. Liu, and R. Ye, "Security and Privacy on Internet of Things," 2016.
[4] K. Shafin, K. L. Kabir, N. Hasan, I. J. Mouri, and S. T. Islam, "Development of an RFID Based Access Control System in the Context of Bangladesh," *2015 Int. Conf. Innov. Information, Embed. Commun. Syst.*, pp. 1–5, 2015.
[5] X. Zhao, J. Yin, Z. Chen, and X. Lu, "Distance-Aware Virtual Cluster Performance Optimization : A Hadoop Case Study," *2013 IEEE Int. Conf. Clust. Comput.*, pp. 1–8, 2013.
[6] L. Amini, N. Jain, A. Sehgal, J. Silber, and O. Verscheure, "Adaptive Control of Extreme-scale Stream Processing Systems," pp. 1–7, 2006.
[7] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor Network Security : A Survey," vol. 11, no. 2, pp. 52–73, 2009.
[8] I. Khan *et al.*, "Wireless Sensor Network Virtualization : A Survey," vol. 18, no. 1, pp. 553–576, 2016.
[9] S. Agrawal, M. L. Das, S. Member, and J. Lopez, "Detection of Node Capture Attack in Wireless Sensor Networks," vol. 13, no. 1, pp. 238–247, 2019.
[10] F. Bao, I. Chen, M. Chang, and J. Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection," vol. 9, no. 2, pp. 169–183, 2012.
[11] D. P. Networks, L. Ramaswamy, S. Member, B. Gedik, and S. Member, "A Distributed Approach to Node Clustering in," vol. 16, no. 9, pp. 814–829, 2005.
[12] P. Sharma, B. Kumar, and P. Gupta, "An Introduction To Cluster Computing using Mobile Nodes," *2009 Second Int. Conf. Emerg. Trends Eng. Technol.*, pp. 670–673, 2009.
[13] H. Li and M. Singhal, "Trust Management in Distributed Systems," no. February, pp. 45–53, 2007.
[14] G. U. O. Jingjing, M. A. Jianfeng, and W. A. N. Tao, "A Mutual Evaluation Based Trust Management Method for Wireless Sensor Networks∗," vol. 26, no. 2, 2017.


ISSN: 2005-4238 IJAST