International Journal of Advance Research in Science and Engineering
Vol. No.6, Special Issue (01), September 2017, BVCNSCS 2017
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Trust Model in Sensor Grid Computing

G Mahesh Kumar[1]
Assistant Professor,
Department of Computer Science,
Bhavan's Vivekananda College,
Sainikpuri, Secunderabad, Telangana, India

Dr. S Ramachandram[2]
Professor,
Department of Computer Science Engineering,
University College of Engineering,
Osmania University,
Hyderabad, Telangana, India

Dr. Jayadev Gyani[3]
Professor,
Department of Computer Science Engineering,
Jayamukhi Institute of Technological Sciences,
Narsampet, Warangal,
Telangana, India

Abstract: Sensors are the devices which have very limited memory, computation, and power. Each sensor node is responsible to sense the environment for collecting, storing, computing and generating the huge amount of data every second. These sensor nodes are scattered at various locations randomly to sense the required data and these nodes form as a network called as Wireless Senor Network. Since the sensor nodes are having restricted resources, the processing or storing of data cannot be done accurately and timely by the sensor devices. To overcome this problem the sensor grid computing has evolved, in which all the wireless sensors networks are integrated with grid computing technology to use the resources of various heterogeneous systems from various domains for faster computation and storage. The grid computing is a technology which shares the resources among various heterogeneous systems from different domains to solve complex problems. The problem is to identify the malicious sensor nodes among numerous sensor nodes involved in communication and also the participating entities involved in grid computing technology. Each participating entity need to do a very fair transaction without any misuse of resources. Security is one of the main issues which should be considered to check that the transactions are done without any problems. The participating sensor nodes need to be monitored very closely so that no misuse of resources will be done. Even though the present sensor node is failed then the other trusted sensor node need to take care of the existing data and start processing it or it should bypass to other nearby trusted sensor node for computation, but it should not stop the processing. This paper proposes a trust model which uses a sensor grid controller component to assess the trustworthy of the participating entities in the sensor grid computing.

Keywords: Sensors, Wireless Sensor Networks, Grid Computing, Trust, Resource.

I. INTRODUCTION

Everyday a lot of data is generated from various sources throughout the environment and transferred to different locations for various purposes. The sensor nodes are playing the main role in capturing data from the environment every second and transferring to the main system for processing. Every sensor node is having limited capacity for processing, and storing. Sensor nodes lifetime is very low because it survives on battery. Sensor nodes are spread out randomly in various locations where mostly humans cannot reach. There are various sensor nodes used for monitoring and capturing data like temperature, earth quakes, floods, fire and many more. One sensor node is not enough to collect and process this information. So, collection of sensor nodes forms as a network to interact with each other in-order to complete a huge data collection and processing by sending to the base stations. This network is called as Wireless Sensor Network. Senor nodes are transferring the collected data to other nodes very frequently and the problem of network traffic is more since these nodes work on wireless communication. The radio signals are used for wireless communication and there is chance of huge data loss due to collision among the radio signals. So, the shielding of radio signals is required to avoid collision. Sensor nodes were initially used in military applications to capture the information of the terrorist attacks.

Grid Computing is a technology used for resource sharing among various heterogeneous entities involved in communication. Grid Computing pools up the resources from various idle entities throughout the world with the permission of the resource owners. Some applications like robotics, manufacturing, research and development require huge amount of resources for computation. A single node cannot do this huge computation, so the resources can be hired from the resource owners and pay only for the resources used through the Grid Computing technology.

Sensor nodes are having the limited capacity as mentioned earlier, it cannot perform huge computations. In this regard the integration of wireless sensor networks with grid computing technology is mandatory to extract very recent information through sensor nodes for processing as well as storing of data by grid computing technology which is called as Senor Grid Computing.

In Sensor Grid Computing the sensor nodes deployment should be perfect so that it can capture the appropriate

information used as alert message for the upcoming threat, so that relevant precautionary steps can be applied to overcome those threats. Every sensor node is having its own work allocated and they do communicate with other nodes for sharing of information. In wireless sensor networks there are chances where malicious nodes might exist which would have been deployed by the third party persons to extract the confidential information. Some nodes might have moved from one network to other network due to various reasons like floods, blowing wind. Every sensor node need to have a unique identifier to identify the current position and the extra nodes without unique identifier can be considered as malicious nodes and those nodes need to be destroyed immediately or make it inactive. In grid computing also there are many heterogeneous entities participating in providing and utilization of resources. Here also their might be some malicious entities which can destroy or misuse the resources. So the security is required for the sensors as well as grid entities for establishing proper trust among themselves to use the resources for capturing, computation and storing of data. The nodes can trust other nodes which are available in the same domain rather than believing the nodes from other domains. This paper proposes a trust model that uses a sensor grid controller component to make a good relationship among the sensor nodes as well as grid entities to make a reliable communication.

II. TRUST

In Sensor Grid Computing the communication is done among the sensors and also with the outside systems like huge computation servers. The participating entities in sensor grid computing are dynamic in nature where it is difficult to predict that the participating entities will be in the same location every time. The sensor nodes and the grid entities should believe each other to continue communication further. The trust establishment should be built among the communication entities to do fair transactions every time. Since the participating entities are from various domains there are many chances to misuse the resources. The grid entities and senor nodes should agree the Service Level Agreement (SLA) before start of any transaction and should follow it strictly. Any misuse of SLA will lead to huge risk imposed by other entities like penalizing them with huge amount of fine.

The trust establishment in sensor grid computing can be done either through direct trust or indirect trust. If the participating entities are well-known to each other then direct trust is established and they do further communication without involvement of third party. If the communication is established among the participating entities with reference to the third party (recommendation) then it is indirect trust. Every entity needs to maintain a good reputation, so that more number of entities will be interested to do communication with those entities only.

III. SENSOR NODE ARCHITECTURE

A sensor node collects, processes and store data which is very limited in capacity. The figure 1 as mentioned below shows various components available in sensor node architecture. The micro-controller is used to process data and controls the overall functionality of the sensor node. A micro controller is often used in embedded devices because it is ease of programming, flexible to connect to various devices; its cost is very low and also low power consumption.

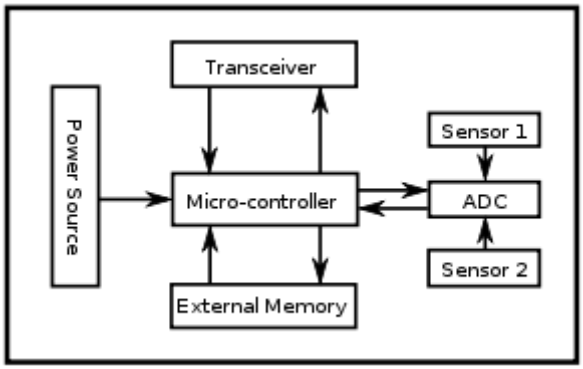


Figure 1: Sensor Node Architecture

The transceiver is a component used to transmit and receive the radio signals as part of communication. The operational states of transceiver are idle, sleep, transmit and receive. The power consumption is done when a transceiver is in idle, transmit or receive mode. It is much advisable to make the node to sleep when there is no data to transmit or receive. Every few seconds the nodes will come back to active state and sense the data to capture and transfer. The External Memory component is used to store the data. A sensor node has a Power Source component in the form of batteries to supply power. The batteries replacement is very hard since these sensor nodes are scattered in various locations which are very difficult to reach. The batteries need to be charged automatically based on the solar energy from the environment. The sensor 1 and sensor 2 are the components used to capture the data from the environment. Sensors generally collect analog signals and passes to ADC (Analog to Digital Converter) which converts the analog signals to the digital signals and transmits to the micro-controller for further processing.

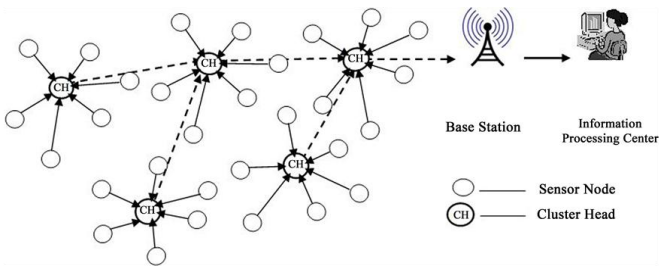


Figure 2: Wireless Sensor Network

The figure 2 represents a Wireless Sensor Network (WSN) collection of numerous sensor nodes sharing information. Each sensor node has its own limited power backup for computation, and also limited storage. In traditional method of communication in WSN all the sensor nodes used to interact with the base station directly for transmitting or receiving the data and the power consumption was more. In modern technology every WSN is having a sensor node acting as a cluster head. Every sensor in this network needs to directly interact only with the cluster head for sharing information to other WSN or to the base station to users through internet, so that the power can be saved among the sensor nodes in WSN. The Cluster Head(CH) is a node with more power and has the right to collect all the information given by all the sensor nodes in their WSN and pass it to other cluster head or directly to the base station for processing and forwarding to the users. There are more chances of node failure since they are with limited capacity and not tightly bound to one WSN since they are not fixed in one location. Once a sensor node is failed then immediately other node need to accept the task and perform it. The WSN does not have a fixed topology since the nodes can be added, removed or moved from one location to other. So, the topology is very much dynamic in nature.

IV. GRID COMPUTING

Figure 3: Grid Computing

Grid Computing is a collection of resources from various heterogeneous participating entities. Few applications which are very critical may not be able to complete the task with the available resources in the present scenario. So in-order to complete the task, extra resources is required. The grid computing enables the resources to get hired from the service providers and pay only for the used resources which will be very much cost effective. The service provider will register the resources with the grid information service entity which they want to hire for the customers when the resources are free. The grid information service is the entity which maintains the list of free resources registered by the service providers. The major problem to be solved is segregated into small jobs and distributed to few registered and accepted entities for computation. Once the job execution is done then the results will be integrated and send to the actual user. The figure 3 shows the grid computing mechanism where resources are shared among numerous devices like laptops, servers, mobile phones, printers and many more, through internet for computation.

V. RELATED WORK

Farruh Ishmanov et al. [1] proposed a secure trust establishment scheme for wireless sensor networks. In this model for estimating the trust of single node a trust estimation method considers the trust value of previous transactions, consolidated misbehaviour and current measured misbehaviour components. This model considers the previous history of the sensor nodes. If the node will perform well every time then its aggregated misbehaviour will be decreased and its trust value is increased. If the node misbehaves continuously then the aggregated misbehaviour will be increased and its trust value is decreased. To identify the current trust value the authors uses the current measured misbehaviour and its previous trust values. The authors also proposed a M-estimater scheme which is used to identify the bad-mouthing attack ie., to identify dishonest recommendations and remove them before aggregating recommendations.

Farruh Ishmanov et al. [2] proposed a robust trust establishment scheme for wireless sensor networks. This model uses a new component called misbehaviour frequency which can handle various strategies for on-off attack. It helps the network to find malicious nodes and also it can differentiate between legitimate nodes and malicious nodes. This also reduces the computational overhead in terms of number of instructions executions. Min-Cheol Shin et al. [3] proposed malicious node detection using confidence level evaluation in a grid-based wireless sensor network. This paper explains that the sensor field is framed as a grid format. Whenever the sensors are deployed randomly then each sensor will be part of the grid. Each grid is headed by the cluster head and it is dynamically elected by the members of the grid. The cluster head needs to maintain the confidence level of all the members in the grid. This paper highlights the malicious node detection mechanism in the small regions also.

Matthew J Probst et al. [4] proposed statistical trust establishment in wireless sensor network. This paper establishes reputation based trust to identify the malicious sensor nodes and also to minimize the problematic effect on its applications. This paper uses the statistical trust and also the confidence level on the trust based on the direct and indirect experiences of the sensor nodes. The nodes with high experiences which are having high rate of confidence levels are give more chances for interaction and due to the low memory and other overheads the redundancy operations are identified and removed.

Brian Tierney et al. [5] proposed a monitoring sensor management system for grid environments. In this paper, an agent-based system is used to operate the monitoring sensors remotely to collect the required data. This paper introduced

JAMM(Java Agents for Monitoring and Management) monitoring system based on java and RMI(Remote Method Invocation) used to launch various system and network management tools and also to extract , summarize and publish the results.

Chen-Khong Tham et al. [6] proposed SensorGrid: integrating sensor networks and grid computing. This paper highlights the research challenges in sensor grid computing such as scalable distributed algorithms, coordinated quality of service(QoS) mechanisms, interconnection and networking, web services and service discovery. R.A.Roseline et al. [7] proposed pollution monitoring for healthy environment using integrated wireless sensor networks and grid computing. This paper focus on how the sensors are helping in collecting the required information from the environment and how the grid computing technology is used to store the huge collected information from sensors and processing it.

VI. SENSOR GRID COMPUTING

Sensor Grid Computing is a technology in which the integration of wireless sensor networks with grid computing is achieved. Every second a huge amount of data is generated throughout the world. The data capturing from various locations is one of the most important task. There are many locations where the normal humans cannot reach, then the sensors are positioned in those unreachable locations to collect huge amount of data. Sensor nodes are having very less resources to store and process the data. Every time they need to share information from one node to another node to make the data to reach ultimately to the destination. The sensor nodes are having very less power supply because these are battery based and the lifetime of sensors are very low. The power consumption will be more to transfer the data to a destination node which is very far from source node. The sensor nodes can be formed as a cluster called as wireless sensor network. Every wireless sensor network will have a cluster head which will be elected by the members of cluster. The cluster head can be changed at any point of time due to the dynamic topology of wireless sensor network. Every sensor node in wireless sensor network needs to make communication with other nodes within the network or to the outside world only through cluster head node. The cluster head node needs to maintain the list of all sensor nodes available within the network, so that it can identify them. Every sensor node need to be given a unique identifier in the wireless sensor network. Any sensor node enters the node without the knowledge of cluster head or a new node is identified without any identifier then those nodes are considered as malicious nodes, then immediately those nodes need to be destroyed. As the sensor nodes are wireless the communication is done through radio waves where these signals can be easily attacked by malicious nodes.

Once the data is collected by the cluster head from various sensor nodes then that data needs to send for processing through the base station which connects to the systems available in the outside world. The systems are part of the grid computing technology where the accepted data from base station is stored and computed on various heterogeneous systems for faster response. The integration of wireless sensor networks with grid computing leads to the recent information capturing, processing and monitoring the environment alerts and attacks.

The problem arises here is to find the malicious nodes in sensor grid computing ie., the malicious sensor nodes as well as malicious grid entities for computation. Every node involved in sensor grid computing needs to be a trusted entity so that a reliable transaction can be done. The nodes involved within the network should be reliable and trusted by other nodes, since every node has the prior information about other nodes. The nodes from other domain cannot be believed, since they are unknown to each other. Since the nodes in sensor grid computing are dynamic in nature ie., they can join or leave the network any time and the maintenance of this information is more critical. While transferring data, there may be some attacks like hacking done by the third party nodes. Security is the key concern for every entity and these should be monitored by various authentication, authorization and cryptographic algorithms.

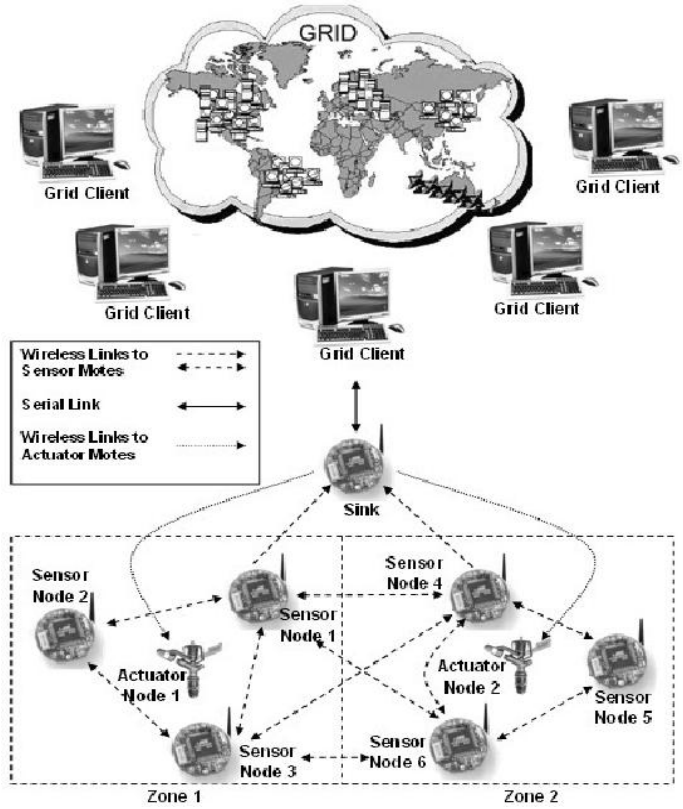


Figure 4: Sensor Grid Architecture

In figure 4 the sensor nodes 1, 2, 3 and actuator node 1 are part of zone 1 and sensor nodes 4, 5, 6 and actuator node 2 are part of zone 2. Every sensor node is capturing data and passing to the sink node which acts a gateway between a grid and sensor node. The sink node relays the request to the authenticated grid entity for computation and the results or instructions are passed to the sink node in-order to transfer to actual sensor node.

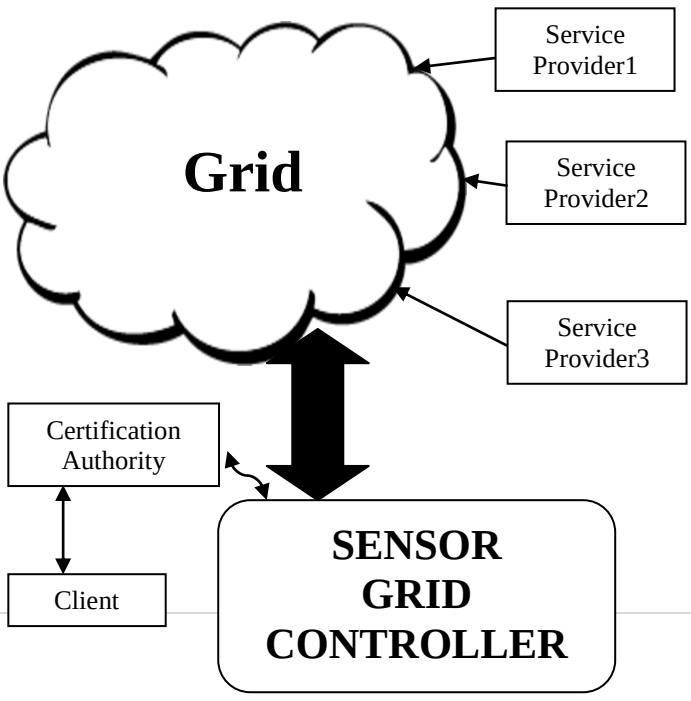
VII. SENSOR GRID COMPUTING APPLICATIONS

The following are few applications of sensor grid computing:

- Environmental Monitoring
- Healthcare Monitoring of Patients
- Smart Homes and Offices
- Safety Monitoring of Physical Structures and Construction Sites
- Tracking of Goods and Manufacturing Processes
- Weather Monitoring and Forecasting
- Military and Homeland Security Surveillance

VIII. PROPOSED TRUST MODEL

The proposed trust model explains the trusted communication between various entities like sensor nodes, cluster head nodes, base stations, clients, service providers, and sensor grid controller. In figure 5 clients interact with the sensor grid controller component for successful authentication through single sign-on procedure. Through single sign-on, a client can access the resources of other grid entities as well as resources from sensor nodes. Client can be a normal user for using the resources or might be scientific personnel for updating resources. In three scenarios the client can work with sensor grid computing. In scenario 1 the client can only request resources to the grid for processing, so the sensor grid controller diverts the communication to the Grid as mentioned in figure 5 where trusted service providers need to be identified for service. In scenario 2 the scientific personnel can instruct the sensor nodes or cluster head nodes to update, so the sensor grid controller diverts the communication towards base station to cluster head in Wireless Sensor Network(WSN) and ultimately to the trusted sensor node. In scenario 3 the client can request huge data from various sensor nodes and asks for processing, so the sensor grid controller based on the client request first makes interaction with the required sensor nodes, capture data and that data is passed to the Grid for computation.



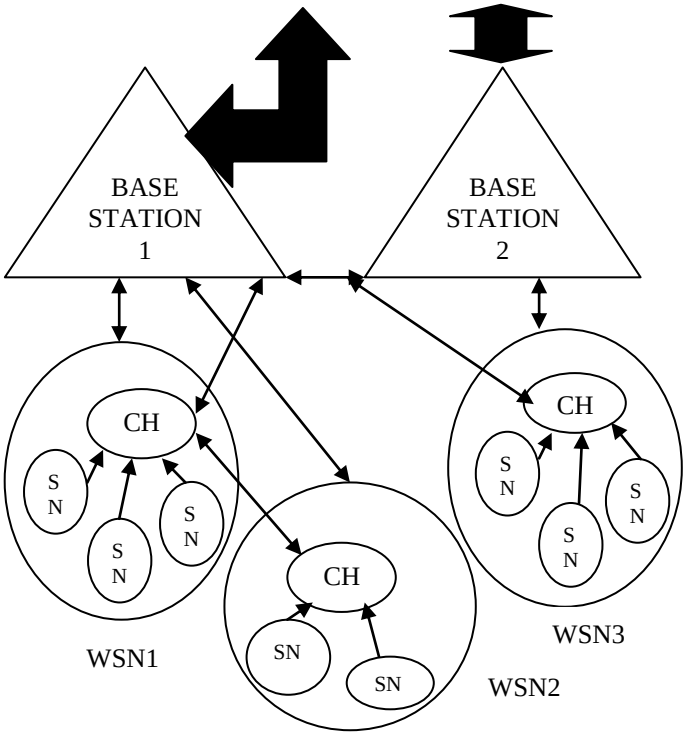
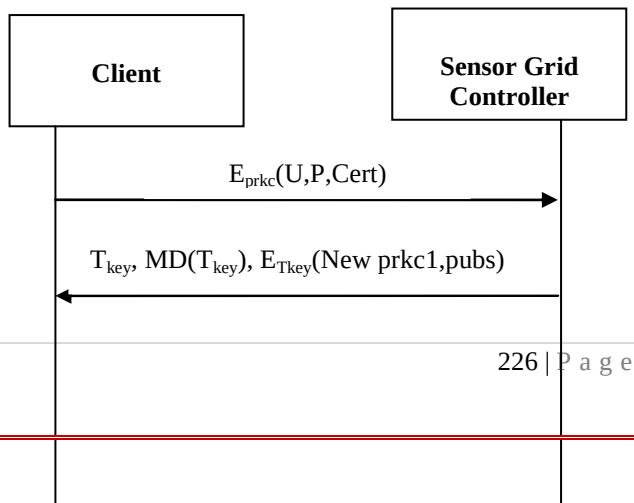


Figure 5: Proposed Sensor Grid Computing Architecture

SN – Sensor Node
CH – Cluster Head
WSN – Wireless Sensor Network

The client needs to authenticate themselves with the single sign-on credentials as well as the certificate it has got from certificate authority. The certificate authority claims that the respective entity is genuine and creates a private key and public key and a certificate for that entity. The certification authority issues a certificate and private key of the client to the client and the public key of the client will be given to the sensor grid controller. The private key of the client is used to encrypt the request and public key of the client is used to decrypt the encrypted request send by the client. The sensor grid controller also has its own private key and public key. To encrypt the response sensor grid controller's private key is used and to decrypt sensor grid contorller's public key along with transaction key is used by the client in-order to maintain confidentiality.



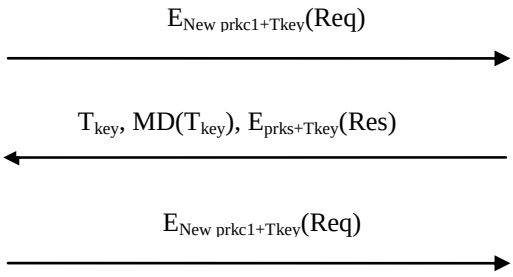


Figure 6: Client Authentication in Sensor Grid Computing

The figure 6 shows the process of authentication for client into the sensor grid computing. The steps of authentication are as follows:

1. The client sends the credentials such as userid(U), password(P) binded with the sensor grid computing and also a certificate(cert) given by Certification Authority(CA), by encrypting them with private key(prkc) of client generated by CA.

The Sensor Grid Controller uses the public key(pubc) of client given by CA to decrypt the encrypted request came from client and then authenticates the client based on the given credentials.

2. Once the client is authenticated then a new private key (New prkc1) and public key(pubc1) for client is generated by Sensor Grid Controller(SGC) and old private key and public key of client ie., private and public key of client generated by CA will be destroyed. The SGC will generate a T_{key}(Transaction Key) valid only for one transaction(ie., one request and response) used to encrypt the new private key (New prkc1) of client and public key of SGC(pubs). The SGC will send the T_{key} in plain text, MD(Message Digest) of T_{key} and also the encrypted message of New prkc1 and pubs.

The client accepts the T_{key} plain text and also MD(T_{key}). The client applies the MD on the T_{key} plain text, and if the received MD(T_{key}) is equal to generated MD(T_{key}) then the T_{key} send by SGC is correct. Then apply the same T_{key} to decrypt the New prkc1 and pubs.

3. The following request from the client will use same T_{key} along with its New prkc1 to encrypt the request.

The SGC will use the pubc1 along with same T_{key} to decrypt the encrypted request and after that the current T_{key} will be destroyed.

4. Now the new T_{key} is generated by the SGC and it uses the private key (prks) of SGC along with T_{key} to encrypt the response. The SGC sends the new T_{key} , MD(T_{key}) and the encrypted response.

The client accepts the new T_{key} plain text and also MD(T_{key}). The client applies the MD on the new T_{key} plain text, and if the received MD(T_{key}) is equal to generated MD(T_{key}) then the T_{key} send by SGC is correct. Then apply the same T_{key} along with the public key of SGC to decrypt the response.

5. The following request from the client will use same new T_{key} along with its New prkc1 to encrypt the request.

The SGC will use the pubc1 along with same T_{key} to decrypt the encrypted request and after that the current T_{key} will be destroyed.

The step 4 and 5 follows cyclic process till the complete session is over. Here the confidentiality is maintained very strictly by creating a new T_{key} for every single request and response, so that it will be very complex for the third-party persons to hack the data.

Sensor grid controller maintains the information about the clients, service providers and the base stations. Based on the type of request the sensor grid controller assigns the tasks to the respective entities. Once the transaction is completed by the client and service providers, then both of them needs to give the feedback of each other to sensor grid controller. When the same client and service provider wants to interact next time, then based on the feedback values only, the sensor grid controller decides to either allow or deny the interaction. Both client and service providers needs to have the rating above 0.5, then only they are eligible to do transaction for next time, otherwise transaction is denied by sensor grid controller.

Sensor grid controller component should also be a reliable component and it also gets the certificate of genuine certified by Certification Authority. The sensor grid controller also maintains the trusted values collected from various trusted entities involved in transaction every time for analyzing the true and fair entities. So, that next time they will get first chance to service. The base stations are working as the middleware between WSN and sensor grid controller. These base stations maintain the information of various WSN's cluster heads and its respective sensor nodes. Each base station will be maintaining and updating the information of current cluster head and sensor nodes in wireless sensor networks

Every sensor node should have a unique identifier like SNF001 for fire sensor nodes, SNE001 for earth quake sensor nodes, and also throughout all wireless sensor networks the identifiers need to be unique. Whenever the sensors nodes are failed, then that unique identifier needs to be blocked until it is active again, and that unique identifier should not be allocated to another sensor node. Every sensor node needs to have all its neighbor nodes information. As and when the information of other nodes from the same cluster is required, then the sensor node can access the information from its cluster head because the cluster head maintains its sensor nodes data. Since the cluster head maintains its sensor nodes information, suddenly if it finds a node which is not there in its list , then that extra node can be considered as malicious and that node can be destroyed. The sensor nodes are mobile in nature, so when it enters into other wireless sensor network then it needs to register its name with the concerned cluster head. Every sensor

node also needs to have a certificate for their authentication, so that at the beginning of every transaction the certificate also should be passed for verification.

Every cluster head should also have a unique identifier like WSN1CH001, WSN1CH002. The cluster head information are stored in base stations. There can be many wireless sensor networks under one base station. Whenever the transaction takes place between cluster head and sensor node then at the end of transaction the sensor node and cluster head should give rating to each other in range of 0 to 1, where 0 is poor performance and 1 is excellent performance. This information is stored in the base station. Once the rating is done , then for any transaction the ratings given by all the sensor nodes need to be aggregated and if the average rating is above 0.5 , then only the same cluster head will continue for the next cycle, otherwise the sensor nodes whose average rating is more will become the cluster head. In this regard, every sensor node and cluster head wants to do the fair transaction in-order to get very good reputation. Any work requested by the external client will be assigned to only those sensor nodes whose reputation is very good.

IX. CONCLUSION

This paper highlights the sensor nodes, its architecture and applications. This paper proposed a trust model for sensor grid computing in which the clients can interact will the sensor nodes for requesting the sensed data from the environment and due to the lack of its computing power, the grid computing has been integrated for achieving the huge processing of applications. Every entity is carefully authenticated by the component called sensor grid controller. The client needs only to authenticate themselves with single sign-on along with the certificate. The sensor node controller helps to achieve confidentiality by using private key, public key and the transaction key. The sensor nodes, cluster heads are working with the feedback mechanism and the node with high rating will get all benefits. The sensor grid controller is acting as a bridge between the grid and wireless sensor networks for reliable transactions to be done whenever required.

X. REFERENCES

[1] Farruh Ishmanov, Sung Won Kim, Seung Yeob, Nam,"A Secure Trust Establishment Scheme for Wireless Sensor Networks", www. Mpdi.com/journals/sensors, Sensors 2014, 14, Page(s):1877-1897, doi:10.3390/s140101877.

[2] Farruh Ishmanov, Sung Won Kim, Seung Yeob, Nam, "A Robust Trust Establishment Scheme for Wireless Sensor Networks", www. Mpdi.com/journals/sensors, Sensors 2015, 15, Page(s):7040-7061, doi:10.3390/s150307040.

[3] Min-Cheol Shin, Yoon-Hwa Choi, "Malicious Node Detection Using Confidence Level Evaluation in a Grid-Based Wireless Sesnor Network", Wireless Sensor Network,2013,5,Page(s):52-60, http://dx.doi.org/10.4236/wsn.2013.53007

[4] Matthew J Probst, Sneha Kumar Kasera,"Statistical Trust Establishment in Wireless Sensor Network", International Conference on Parallel and Distributed Systems, Volume 1, December 2007, Page(s): 1-8, http://dx.doi.org/10.1109/ICPADS.2007.4447736 .

[5] Brian Tierney, Brian Crowley, Dan Gunter, Mason Holding, Jason Lee, Mary Thompson, "A Monitoring Sensor Management System for Grid Environments", Cluster Computing, Volume 4, No. 1, March 2001, Page(s): 19-28.

[6] Chen-Khong Tham, Rajkumar Buyya,"SensorGrid: Integrating Sensor Networks with Grid Computing", Invited Paper in CSI Communications, Special Issue on Grid Computing, Computer Society of India, July 2005, Page(s):1-7.

[7] R.A.Roseline, Dr.P.Sumathi, "Pollution Monitoring for Healthy Envrionment using Integrated Wireless Sensor Networks and Grid Computing", Journal of Global Research in Computer Science, Volume 3, No.1, January 2012, Page(s): 21-26.