Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.244 – 252

RESEARCH ARTICLE

Special Scheme of Hidden Data Procession for Several Applications in Wireless Sensor Networks

Janarish Saju C[1], Sharon Nisha M[2]

[1]PG Scholar, Department of CSE, Francis Xavier Engineering College, Tirunelveli, India

[2]Associate Professor, Department of CSE, Francis Xavier Engineering College, Tirunelveli, India

[1] janarishsaju@gmail.com

Abstract-- In wireless sensor networks hidden data procession is the concept of collecting, summarizing and combining sensor node's data in order to reduce the amount of data transmission in the networks. In previous studies we have found that homomorphic encryption algorithm have been applied to hide data during aggregation from sensor nodes. However the principle involved in this algorithm does not satisfy several applications in sensor environment, and second compromising in case of sensor node attack cannot be prevented and then finally the number of messages aggregated could not be detected and whether it may be a duplicate copy, therefore a special scheme "Hidden Data Procession" has been introduced which is an extended form of CRT(Chinese Redundancy Theorem) algorithm such that the security schemes are applied using "Key Distribution" technique, since it has three methodology to satisfy the above mentioned problem. Initially it was designed mainly for various application environment and second it prevents compromising node attack and finally a special method of counting capability is applied here, to prevent unauthorized data sensed, Here all the functions are implemented in the form of database as a service model and the queries are aggregated in the form of encrypted manner separately, which proves security in hidden data procession.

Keywords—Hidden data procession, Chinese Redundancy Theorem (CRT), key distribution techniques and wireless sensor networks

I. INTRODUCTION

A wireless sensor network is a network consisting of various separated devices called sensors to detect environmental conditions. A wireless sensor network system provides the way of connecting many sensor nodes. It incorporates wireless connectivity of combining sensor nodes for a separated environment as shown in Fig. 1. The wireless technology depends on your application requirements. The required applications include radio transmission, Wi-Fi connectivity, long term Bluetooth devices or satellite transmission etc. The WSN is built of "nodes" – from single to thousands of sensor nodes. Each and every sensor node has several method of construction: a radio transceiver with an internal antenna or connection to an outside antenna. Also there are many typical construction interfacing with the sensors networks. A sensor node might act like a planet

surrounding the sun, which means the sun which acts like a group head. In case of sensor environment the each and every sensor node may considered to be cluster head according to the application requirements. The costs of sensor nodes are unpredictable depending on the utilization of sensor nodes.

Fig. 1 A WSN Component, Gateway and Distributed nodes

II. RELATED WORKS

In [1] Perrig.A, et.al, (2011) proposes "SIA: Secure Information Aggregation in Sensor Networks" This is the paper which constructs framework for securing the data in sensor environment. Here the sensor nodes which act like the aggregator according to the query evaluated which strictly reduces the communication overhead, the information responded according to the query is in the form of average or median of the corresponding values. This can be achieved by constructing random sampling or interactive proofs. So even if the corresponding sensor nodes are corrupted, the sampling model of collected information provides the result to the user. And also it enables the sub linear communication between aggregators and the users, and this was the first technology evolved for secure aggregating protocol that can handle malicious attack on sensor nodes.

In [2] Stankovic, et.al, (2010) deals with "Security in Wireless Sensor Networks: Issues and Challenges" which describes a great purposes for various future applications, the inclusion of wireless communication technology in this paper includes several methods of security applications. The intent of this paper is to monitor the related security problems and occurrences in wireless sensor networks. This mechanism detects the security problems and proposes security solving applications for wireless sensor networks. This study also discusses the major view of security for implementing future, fast, and accuracy of security in wireless sensor networks. According to the use of layered codes, group heads of sensor environment does not know how the sensor data to perform data procession, which enables sensor nodes to communicate end-to-end secure communication with base station to the related sensor nodes.

In [3] David Evans,et.al,(2007) focuses on "Secure Aggregation for Wireless Networks", Here also the same criteria used as mentioned above such that the sensor nodes in proposed environment collects the data or information and distributed to the requested base station. To balance energy, intermediate sensor nodes should collects information from separate sensors nodes. However, this evaluates the risk of compromising any of the sensor nodes and provides false reading. In this paper the mechanism of new protocol was designed to avoid the compromising node attack. Here this protocol is designed with minimum energy or power, minimum cost and inexpensive sensor nodes.

In [4] HasanÇam, et.al, (2007) proposes a secure and energy considerable data aggregation protocol called ESPDA (Energy-Efficient Secure Pattern based Data Aggregation). ESPDA avoids the repeated data transmission from sensor nodes to group head called cluster head. If sensor nodes aggregate the same data repeatedly from sensor nodes, this approach gathers data and collected in the form of pattern code representation to determine the characteristics of data sensed. Cluster-heads collects the data aggregated and securely transmitting to the base station in the form of cipher texts. And this mechanism provides the way of communication by end-end process of data aggregation mechanism.

In [5] Cam.H, et.al, (2008) proposes a secure data aggregation protocol, called SRDA. SRDA requires sensor nodes to send only the difference obtained data instead of all data aggregated by the sensor nodes. Effectiveness of the SRDA is managed by the key distribution technique in case of security purposes. SRDA establishes secure connectivity among sensor nodes. The incremental security requirement for data aggregation evaluates

significant result's that show SRDA technique yields preserve data security by minimizing the energy consumption.

III. SYSTEM DESIGN

The problem of aggregating data from sensor nodes directly to the base station requires more energy consumption, which is satisfied by forming the cluster node to collect data from a group of nodes; this principle is already proposed by traditional approaches. Another need for the problem is that it haven't secured while collecting data for multi-application environment, since previous studies show that the security is made over only for single application environment. And finally third problem shows that the base station does not know how many times the sensor has been sensed, since there may be a chance for wrong update from unauthorized access. Therefore these problems need a quick remedy and solutions, which can be resolved by our "Hidden Data Procession" approach.

A. Existing System

In wireless sensor networks data procession is the scheme of collecting data from several nodes and securely passing them to base station, which reduces the large amount of transmission, here the traditional approach of "Homomorphic Encryption" algorithm have been applied, this method supports for an effective single application environment, but there is a risk for multi-application environment, since the enciphering of data for several application cannot be aggregated together, because the decrypted aggregated result will be incorrect. And the existing methodology does not counts the number of aggregated messages, which results unauthorized update or editing on the cluster head and here there is no proved security for the compromised node attack of the same. And the service is provided here in the form of connection oriented or end to end service which results high maintenance and expensive.

B. Proposed System

The proposed scheme is the "Hidden Data Procession" method, which introduces the new extended form of "Boneh et al's Homomorphic Encryption Algorithm". This is a key distribution technique and is formally related with (CRT-Chinese Reminder Theorem) algorithm, which encrypts the data from multi-application environment, such that the cipher texts from different application can be encapsulated into only one cipher texts, whereas the corresponding base station can extracts the application related plaintext via the corresponding secret keys allotted. This scheme is specially designed to prove three contributions that do not satisfy previous studies of data procession technique in which the first contribution is that it was designed especially for multi-application environment, and second it mitigates compromising attack in cluster head, and finally it degrades the damage from unauthorized updating or editing sensor readings.

IV. SYSTEM MODEL

The system model shows that the admin collects all type of sensor data, to be collected together first. Next, it will aggregate related data together. This process is done by cluster heads.

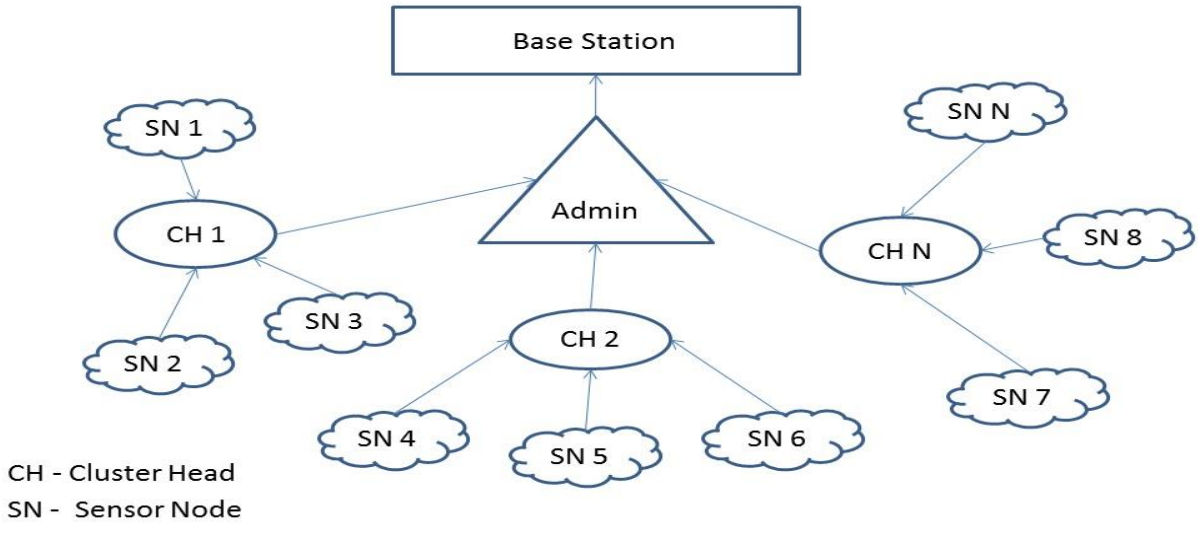

Fig. 2 System Model

Whereas the cluster head monitors each and every step, for each data's aggregated from cluster head is secured in the form of encrypted manner and also there is a special approach, counting capability of aggregated

information is applied. And finally after the clustering process have been finished. It will forward the collected data's to the base station.

V. SYSTEM OPERATION AND CONSTRUCTION

A. System Operation

The operation includes the concept of collecting data from sensor nodes in the form of aggregation which means the number of information's gathered could be reduced by means of arithmetic calculation or other operations as shown in Fig. 3

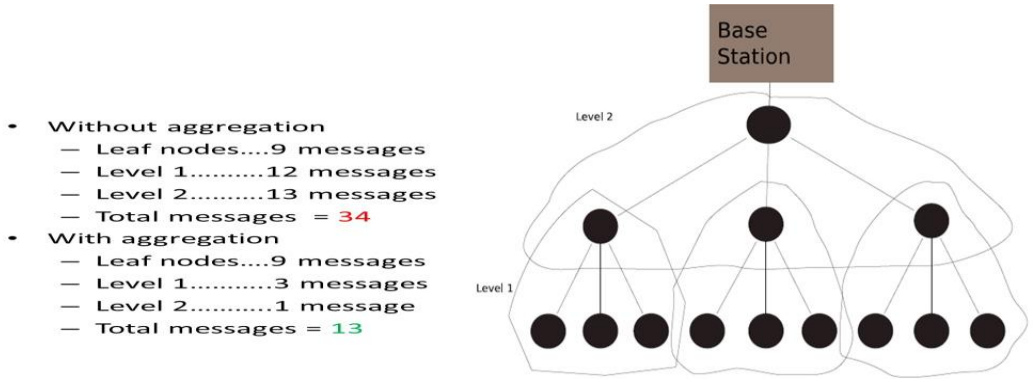

Fig. 3 System Operation

Here in this operation there are 34 messages extracted before the aggregation and showing only 13 messages after aggregation. Hence the number of messages could be reduced. And hence all the informations gathered by cluster nodes could be aggregated in the form of encrypted manner, this construction is explained in the following section algorithm specification.

B. Pre-processing

In pre-processing, sensor node (SN) gathers information from the sensor environment and securely transmits the information to the base station via hop by hop transmission technologies based on tree or cluster topology.

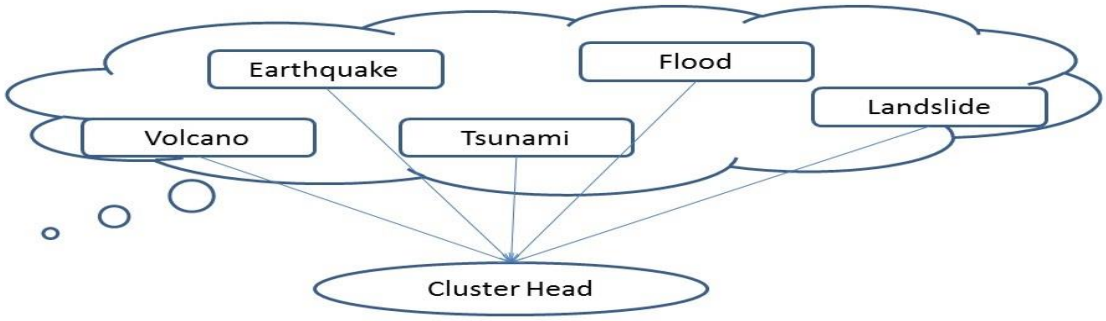

Fig. 4 Pre-processing

The existed transmission technology carries high energy cost for intermediate sensor nodes. To improve the efficiency, a cluster head is placed to manage the sub tree nodes, the cluster head which acts as the group head to collect data for allocated sensor nodes in sensor environment, thus it performs the data aggregation concept. After aggregation done, AGs would forward the results to the next hop. In general, the data can be aggregated via algebraic operations (e.g., addition or multiplication) or statistical operations (e.g., median, minimum, maximum, or mean). For example, an AG can simply forward the sum of numerical data received instead of forwarding all data to the next hop.

C. System Construction

This module is designed for multi-application WSNs. In practice, SN having different purposes, e.g., smoke alarms and thermometer sensors may be deployed in the same environment. If we apply traditional data aggregation schemes, the cipher texts of different applications cannot be aggregated together, therefore a new method of hidden data procession concept is introduced which collects encrypted data from different applications through cluster heads to the base station and formally the base station decrypts the single cipher text to evaluate multiple information's from sensor environment.

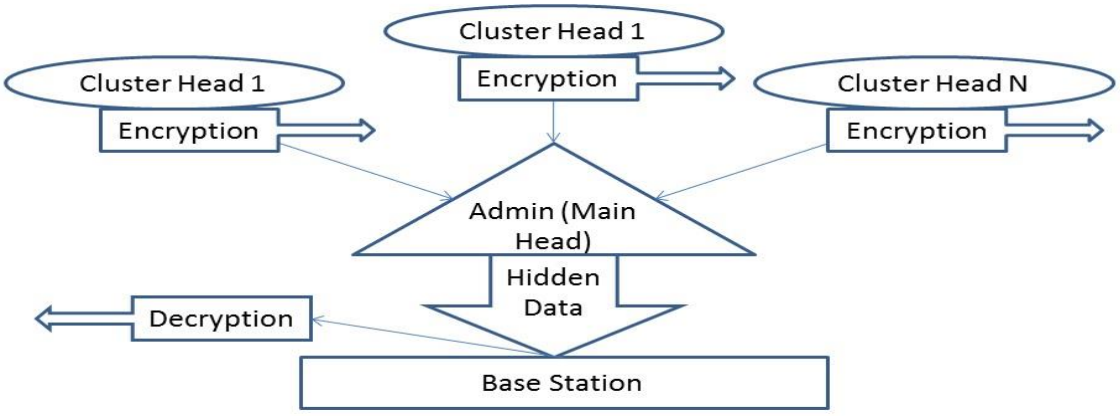

Fig. 5 System Construction

For this module a separate algorithms were prescribed, which are explained in the following section.

VI. ALGORITHM SPECIFICATION

A. Algorithm for hidden data (Single data)

1) Key Generation: (Generates private/public key pair)
   Step 1: initialize three elements (q1, q2, E), where E is elliptical curve point, q1q2 are larger primes.
   Step 2: select randomly two generators ord (H) = ord (U) = N, which are base points.
   Step 3: calculate H = q2 * U, which means ord (H) = q1
   Step 4: select parameter T, where T < q2, such that T is maximum plain text boundary.
   Step 5: generate output of public key P_K = (N, E, G, H, and T).
   Step 6: similarly generate output of private key S_K = q1.
2) Encryption [P_K (M)]: (Encrypting message M by public key P_K)
   Step 1: check for M, where M belongs to the set {0…..T}
   Step 2: randomly select R, where R belongs to the set {0….N-1}
   Step 3: generate cipher text C as C =M * G + R * H, where G, H belongs to P_K
   Step 4: generate output C
3) Data Procession (DP[C1,C2]): (Data procession for two cipher texts C1 and C2)
   Step 1: we know C1 = M1 * G + R1 * H and C2 = M2 * G + R2 * H
   Step 2: select randomly R1, where R1 belongs to {0…..N-1}
   Step 3: calculate DP of (M1 + M2), where C' as
   C' = C1 + C2 + R' * H = (M1 + M2) * G + (R1 + R2 + R') * H.
   Step 4: generate output C'.
4) Decryption [S_K(C)]: (Decrypting cipher text C by private key S_K)
   Step 1: compute $\log_G(q * C) = \log_G(q *(M * G + R * H)) = \log_G(M * q1 * G) = M$, where G=q1 * G.
   Step 2: generate output M.

B. Algorithm for group of clusters (Construction for multiple data)

1) Key Generation: (Generates private/public key pair for groups G_A and G_B)
   Step 1: initialize three elements (q1, q2, q3, E), where E is elliptical curve point also q1, q2 and q3 are larger primes.
   Step 2: randomly select three generators G1, G2 and G3, where Ord (G1) = Ord (G2) = Ord (G3) = N.
   Step 3: calculate point H = q1q2 * G3, where Ord (H) = q3.
   Step 4: select parameter T for maximum plain text boundary, and then compute $T_A = T_B$ = [T/X], where X represents sensor
   Step 5: compute P = q2q3 * G2, Ord (P) = q1, then calculate output for G_A group of public key P_{KA}, where P_{KA} = (N, E, P, H, TA)
   Step 6: compute Q = q1q2 * G2, where Ord (Q) = q2, then calculate output for G_B group of public key P_{KB}, where P_{KB} = (N, E, P, H, TB)
   Step 7: generate output for G_A for the group private key S_{KA} as (q2q3), and for G_B for the group private key S_{KB} as (q1q3).

2) Encryption [P_{KA} (M)]: (Encrypting message M by public key P_K in G_A)
   Step 1: check for M, where M belongs to the set {0…..T_A}
   Step 2: randomly select R, where R belongs to the set {0….N-1}
   Step 3: generate resulting cipher text C as C =M * P + R * H.
   Step 4: generate output C.
3) Encryption [P_{KB} (M)]: (Encrypting message M by public key P_K in G_B)
   Step 1: check for M, where M belongs to the set {0…..T_B}
   Step 2: randomly select R, where R belongs to the set {0….N-1}
   Step 3: generate resulting cipher text C as C =M * Q + R * H.
   Step 4: generate output C
4) Data Procession (DP[C1,C2]): (Data procession for two cipher texts C1 and C2)
   Step 1: compute the cipher texts C' = C1 + C2; C' = (∑Mi) * P + (∑Mj) * Q + (∑Ri) * H, where ∑Mi represents the procession result of G_A, ∑Mj represents the procession result of G_B, and ∑Ri represents randomness of both.
   Step 2: generate C' as result.
5) Decryption [S_{KA}(C)]: (Decrypting cipher text C for cluster group G_A)
   Step 1: calculate M = ∑Mi = $\log_P$ (q2q3 * C) where P = q2q3 * P
   Step 2: generate output M.
6) Decryption [S_{KB}(C)]: (Decrypting cipher text C for cluster group G_B)
   Step 1: calculate M = ∑Mj = $\log_P$ (q1q3 * C) where P = q1q3 * Q
   Step 2: generate output M.

C. Algorithm for counting the number of data's gathered for each sensor node update

1) Key Generation:
   Step 1: combine the above mentioned algorithm to generate two public key pairs.
   Step 2: place G' group of public key P_{KG} = (N, E, T1, P, Q, H).
   Step 3: place G' group of private key S_{KG} = (q2q3, q1q3).
2) Encryption [P_{KG} (M)]: (Encrypting message M in group G)
   Step 1: check for M, where M belongs to the set {0…..T_1}
   Step 2: randomly select R, where R belongs to the set {0….N-1}
   Step 3: generate resulting cipher text C as C = M * P + Q + R * H.
   Step 4: generate output C.
3) Data Procession (DP[C1,C2]): (Data procession for two cipher texts C1 and C2)
   Step 1: compute the cipher texts C' = C1 + C2 = (∑Mi) * P + C * Q + (∑Ri) * H, where ∑Mi represents the procession result of G, and ∑Ri represents randomness of both.
   Step 2: generate C' as result.
4) Decryption [S_{KG}(C)]: (Decrypting cipher text C for cluster group G)
   Step 1: calculate M = ∑Mi = $\log_P$ (q2q3 * C) where P = q2q3 * P
   Step 2: calculate c = $\log_Q$(q1q3 * C, where Q = q2q3 * P
   Step 3 : generate output M,C.

VII. PERFORMANCE ANALYSIS

Performance gain of all the techniques are compared along with the graphical representation, for which it can be compared with three representations of categories they are end to end technology, database as a service and showing cloud as a platform. For each application there could be advantages and drawbacks see Fig. 6

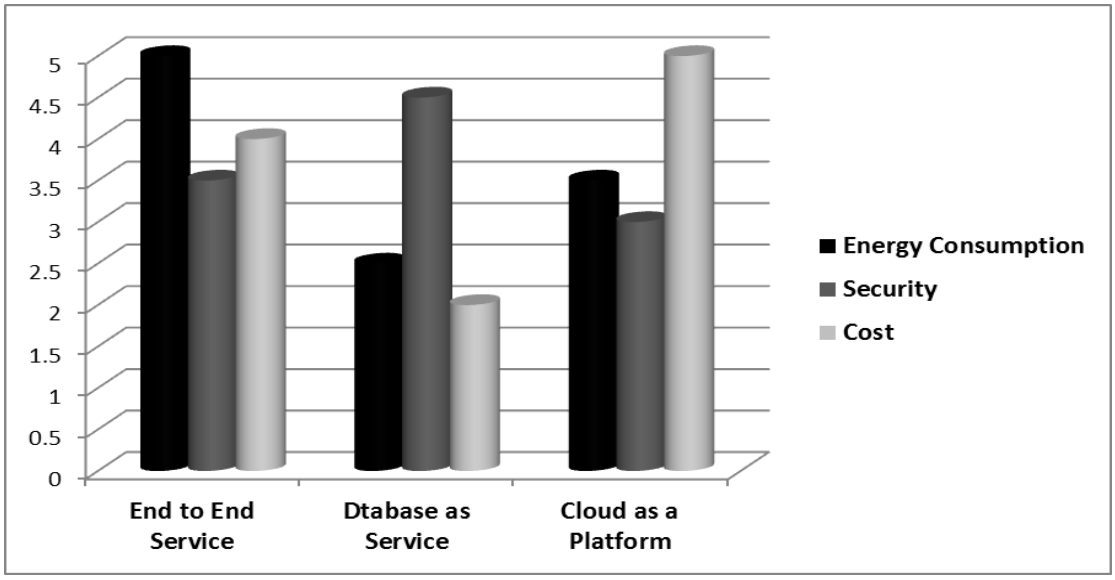

Fig. 6 Performance analysis

A. Performance Gain of Hidden Data Procession

In the above process the computation cost is considerably high. And the data procession is high. This shows that sensors nodes to perform encryption and decryption are complex. To prove the efficiency evaluates the performance gain. Initially we should classify the sensor nodes based on their tasks, and be separated to specific cluster head according to the requirements. Leaf nodes from the tree gather information from the sensor deployed and finally sends the information back to the base station. Aggregated nodes are the sensor nodes which have the collection of information these information can be forwarded to the base station. During this process the energy consumption is measured such that the aggregated results could be minimised by reducing it to single information which is already described above. The data forwarding scheme (DFS) is enhanced to every aggregated node to forward the data to the neighbourhood node. For every data transmission a hop by hop process is enhanced and is secured by applying security mechanism which may be AES and the parent node which stores the encrypted data and finally the base station collects the information in the form of single cipher text. This reduces the amount of data transmission and complexity. Thus proves effectiveness of performance measures.

VIII. RESULT ANALYSIS

The result evaluated in this paper is explained based on the construction of web documents produced as screenshots, that shows constructing web page to accepts the readings of the sensor nodes, which formally stores the collected information's as database as a service model as shown in Fig. 7

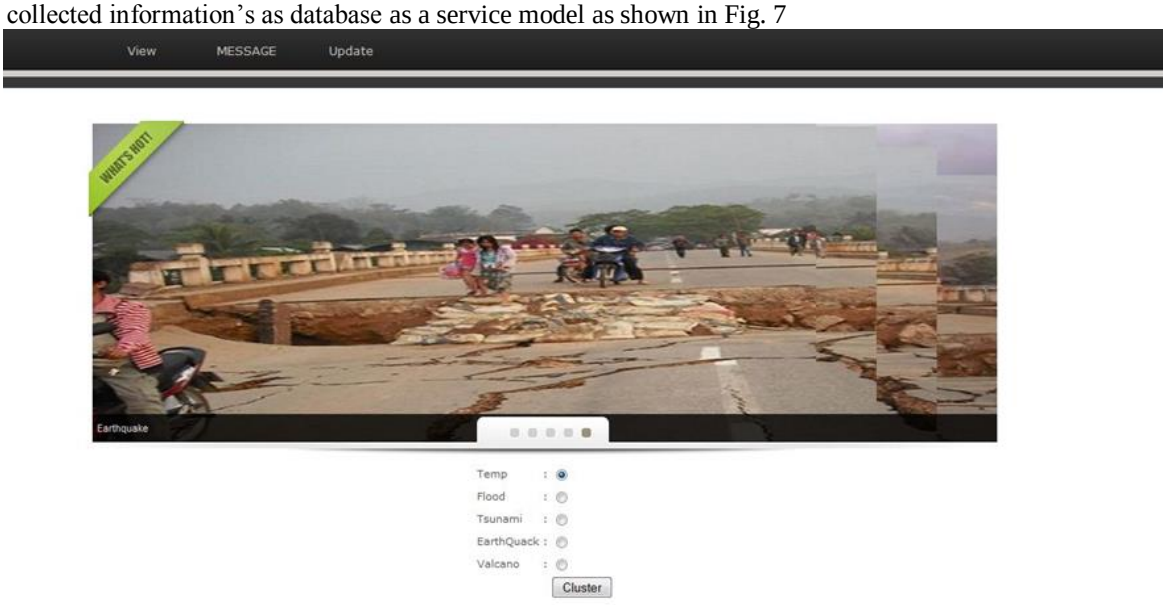

Fig. 7 Collection module for multiple data's

And formally the collected data's could be converted and encrypted by implementing the above discussed algorithm to response for the base station, such that the base station aggregates the information in the form of concealed manner, since the collected data's are already stored in cluster head in the form of encrypted manner. See Fig. 8

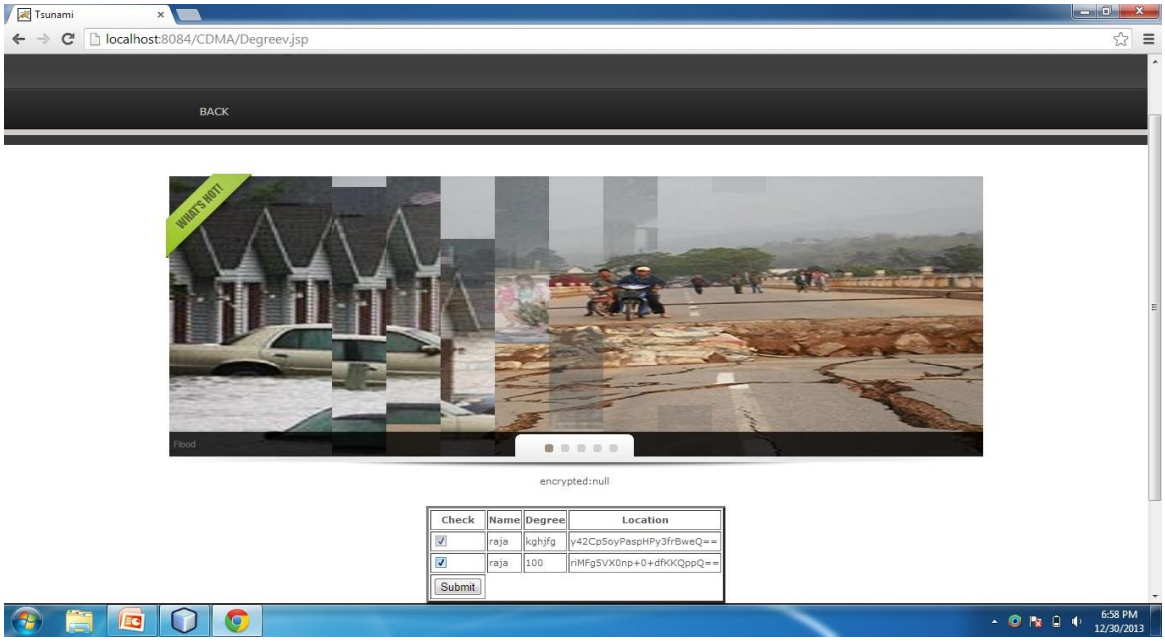

Fig. 8 Collection of data's in encrypted manner

Thus the encrypted data's are updated to the base station in the form of single cipher text and the number of data's gathered are also sensed along with each update in the sensor reading, this functions could be performed by implementing the above mentioned algorithms in the code document. And hence the base station extracts the corresponding information by decrypting the single cipher text for evaluating multiple data's collected. This shows that multiple data's are aggregated effectively to satisfy multi-application environment.

IX. CONCLUSION

Multi-application environment," Hidden Data Procession" is the first Data aggregation scheme. Through "Hidden Data Procession", the encrypted cipher texts from different applications can be collected and combined in the form of single encrypted text. For a single-application environment, it is still more secure than other data aggregation schemes. Whereas it was the first scheme proposed to satisfy several information gathered. Whenever compromising attacks occur in WSNs, it provides the way of securing by counting the expected aggregated results. All of this function satisfies through the BGN scheme proposed. Thus it provides database as service in the form of aggregating queries. In future we may propose PH scheme, which conceals the queries without decryption and may use cloud as a platform for separating queries rather than database as a service and hence it can be evaluated as much as possible for efficiency.

REFERENCES

[1] Perrig A., Przydatek B. and Song D., (2011), 'SIA: Secure Information Aggregation in Sensor Networks', Proc. First International Conference on Embedded Networked Sensor Systems, pp. 255-265.

[2] Stankovic and Wagner D., (2009), 'Security in Wireless Sensor Networks', Comm. ACM, Vol. 47, No. 6, pp. 53-57.

[3] Evans D and Hu L., (2007) 'Secure Aggregation for Wireless Networks', Proc. Symp. Applications and the Internet Workshops, pp. 384-391.

[4] Hasana Cam, Muthuavinashiappan D., and Sanli.H.O, (2007), 'Energy-Efficient Secure Pattern Based Data Aggregation for Wireless Sensor Networks', Computer Comm., Vol. 29, No. 4, pp. 446-455.

[5] Cam H., Ozdemir S. and Sanli H., (2008), 'SRDA: Secure Reference-based Data Aggregation Protocol for Wireless Sensor Networks,' Proceedings. IEEE 60th Vehicular Technology Conference (VTC '04-Fall), Vol. 7.

[6] Acharya M., Girao J. and Westhoff D., (2006), 'Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution, and Routing Adaptation', IEEE Transaction on Mobile Computing, Vol. 5, No. 10, pp. 1417-1431.

[7] Girao J., Mykletun E. and Westhoff D.,(2006), 'Public Key Based Crypto schemes for Data Concealment in Wireless Sensor Networks', Proceedings. IEEE International Conference Communication. (ICC '06), Vol. 5.
[8] Li Q. and Cao G., (2012), 'Mitigating Aggregated Data in Networks', IEEE Trans. Information Forensics and Security, Vol. 7, No. 2, pp. 45-56.
[9] Grid.S.J.T.U., Computing Center (2012), 'Shanghai Taxi Trace Data', http://wirelesslab.sjtu.edu.cn ,Vol. 19, No. 8, pp. 32-43.
[10] Chen D. and Varshney P. (2009), 'A Survey of Void Handling Techniques for Geographic Routing in Wireless Networks', IEEE Communication Surveys and Tutorials, Vol. 9, No. 1, pp. 50-67.
[11] Boneh D., Rubin.K. and Silverberg A., (2011), 'Finding Composite Order Ordinary Elliptic Curves Using the Cocks-Pinch Method', Number Theory, Vol. 131, pp. 832-841.
[12] Bhattacharyas, Luc, Roman G. and Saifullah A., (2010), 'Multi-Application Deployment in Shared Sensor Networks Based on Quality of Monitoring', Proceedings IEEE 16th Real-Time and Embedded Technology and Applications Symp, pp. 259-268.
[13] Iyer B., Li C.., and Mehrotra S., (2002), 'Executing Sql over Encrypted Data in the Database-Service-Provider Model', Proc. ACMSIGMOD International Conference Management of Data, pp. 216-227.
[14] Hacigu¨mu.H, (2004), 'Efficient Execution of Aggregation Queries over Encrypted Relational Databases,' Proceedings Ninth International Conference. Database Systems for Advanced Applications (DASFAA '04), Vol. 9, pp. 125.
[15] Liu A. and Ning P., (2008), 'TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks', Proceedings International Conference Information Processing in Sensor Networks (IPSN '08), and pp. 245-256.

