Acta Informatica Pragensia, 2015, 4(3): 276–287
DOI: 10.18267/j.aip.74
Peer-reviewed paper

A Fine-Grained Data Access Control System in Wireless Sensor Network

Boniface K. Alese[*], Sylvester O. Olatunji[*], Oluwatoyin C. Agbonifo[*], Aderonke F. Thompson[*]

Abstract

The evolving realities of Wireless Sensor Network (WSN) deployed to various terrain of life require serving multiple applications. As large amount of sensed data are distributed and stored in individual sensors nodes, the illegal access to these sensitive data can be devastating. Consequently, data insecurity becomes a big concern. This study, therefore, proposes a fine-grained access control system which only requires the right set of users to access a particular data, based on their access privileges in the sensor networks. It is designed using Priccess Protocol with Access policy formulation adopting the principle of Bell Lapadula model as well as Attribute-Based Encryption (ABE) to control access to sensor data. The functionality of the proposed system is simulated using Netbeans. The performance analysis of the proposed system using execution time and size of the key show that the higher the key size, the harder it becomes for the attacker to hack the system. Additionally, the time taken for the proposed work is lesser which makes the work faster than the existing work. Consequently, a well secure interactive web-based application that could facilitates the field officers access to stored data in safe and secure manner is developed.

Keywords: Attribute-Based Signature (ABE), Bell Lapadula access policy model, Wireless sensor network (WSN), Fine-grained data access control, Security.

1 Introduction

A wireless sensor network (WSN) can be generally described as a network of nodes that cooperatively sense and may control the environment enabling interaction between persons or computers and the surrounding environment. WSNs usually consist of a large number of sensor nodes that can be easily deployed to various terrains of interest to sense the environment. WSNs can be used in wide range of applications, such as military, health and weather forecast. While the main purpose of deploying wireless sensor network (WSN) is to monitor the physical world and provide observations for various applications. As WSNs are usually deployed in an environment that is vulnerable to many security attacks, it is crucial to control the access to the sensor nodes (e.g. reading the sensor data), especially when there are many users in the system. Moreover, different users may have different access privileges, in the case of WSN deployed in the battlefield, a soldier only need to access the data related to his mission, but higher rank officer often requires information gathering for overall monitoring and therefore should have more information access privilege than a soldier, (Buratti *et al*, 2009; Tubaishat, Madria, 2003, Hac, 2003).

[*] Computer Science Department, Federal University of Technology Akure, P.M.B. 704, Akure, Ondo State, Nigeria,
✉ bkalese@futa.edu.ng, solatunji@futa.edu.ng, ocagbonifo@futa.edu.ng, afthompson@futa.edu.ng

The emerging reality of WSNs developed as long-lived infrastructure required to serve multiple applications necessitates the development of fine-grained security support. Sensor nodes participation in multiple concurrent applications requires access control per-application basis (Matthys *et al*, 2010). According to Lou et al, (2006), data security naturally becomes a big concern due to very large amount of sensed data distributed and stored in the individual sensor nodes. Moreover, in mission-critical application scenarios various types of data generated by all kind of sensors may belong to different security levels, and thus are meant to be accessed only by selected users. The application is compromised if the access control is not properly enforced. Varieties of security solutions of deployed WSNs have been proposed in literatures, these provide some levels of access control by using different types of authentication schemes comprising digital signatures, hash functions and symmetric keying. However, each of these approaches operates at a coarse-grained level, as they provide a level of entity authentication which considers complete nodes as endpoint, meaning that it consist of fewer, larger components than fine-grained system. (Matthys et al, 2010). Object composition based on Object references is coarse grained while object composition is based on attributes is fine-grained (Yu et al, 2010, Lou *et al*, 2006).

Some common security aspects such as confidentiality and integrity are also desired in any other WSNs security scheme. With respect to data access control in WSNs to provide fine-grained data access control, the system provides a strategy that is able to precisely specify the capability of different kind of users to access sensor data of different types of security level, collision resistance, sensor compromised resistance and backward secrecy.

In a very large scale WSN, transmitted data in sensors is via wireless communication, mechanisms to prevent unauthorized users from interfering on the transmitted information or introducing data into the network have to put in place since the main aim is only to protect the sensitive nodes data been hack by the hackers.

Sushmita *et al*, (2011) identify most popular threat which includes: insider and outsider threat, passive and active threat, and user might collude and try to gain access to unauthorized data. In view of these, access control is put in place to curb the unauthorized users and which must satisfied these requirements: user authentication, node compromised tolerance, limit access privileges, efficiency, and integrity.

2 Literature review

In WSN, nodes monitored given field (an area or a volume) are through wireless links. The data is forwarded, possibly via multiple hops, to a sink (controller or monitor) that can use it locally or is connected to other networks (the Internet) through a gateway. The nodes can be stationary or moving; and can be aware of their locations or not. They can also be homogenous or not, (Buratti et al, 2009). Each individual nodes must be designed to provide the set of primitives necessary to synthesize the interconnected web that emerges as they are deployed, while meeting strict requirements of sizes, cost and power consumption, (Jason, 1998; Lewis, 2004; Cook and Das, 2004). Fig. 1 shows a typical WSN scenario.

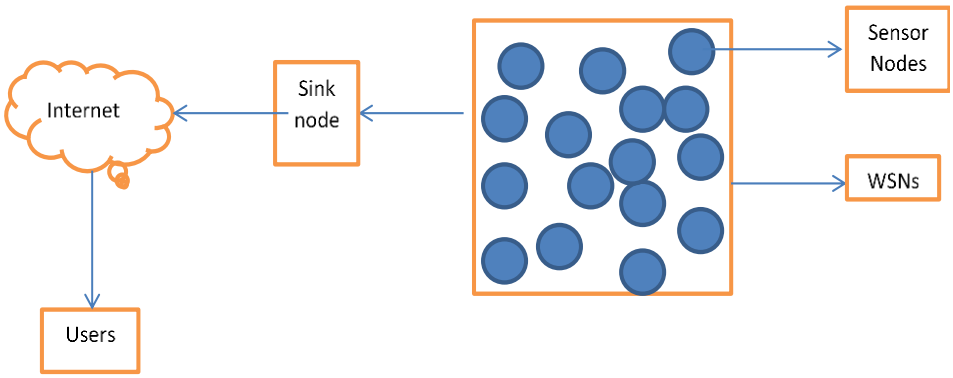

Fig. 1. *Wireless Sensor Network scenario. Source: (Lewis, 2004)*

The three categories of sensor nodes are: (i) Passive, Omni Directional Sensors (ii) Passive, narrow-beam sensors; and (iii) Active Sensors. WSNs are vary depending on the environment, such types can be the following: Terrestrial, Underground, Underwater, Multimedia and Mobile. The applications of WSNs are innumerable (Sohraby et al, 2007). The expansion and arrangement of WSN have taken traditional network topologies in new directions. Thus, many of today's sensor applications require networking alternatives that reduce the cost and complexity while improving the overall reliability. Early sensor networks used simple twisted shielded–pair (TSP) implementations for each sensor. Recently, the industry adopted multidrop buses (an example is Ethernet). Now there is true web-based networks (e.g., the World Wide Web) implemented on the factory floor (Wayne, 2000). Some topology existing in WSN are: Point-to-Point Networks, Multidrop Networks and Web Network.

2.1 Wireless Sensor Network Protocols

Data are routed from one node to other using different routing protocols (Bhattacharyya, Kim, Pal, 2010). Research and industry trends revealed that routing protocols are majorly classified into three categories, namely, Data-centric protocols: are query based and use concept of naming of desired data to eliminate many redundancy transmission within the network. Hierarchical protocols: it clusters the nodes so that cluster heads can be aggregate and reduce the data to save energy. Location based protocols: use position information to send the data to only desired regions rather than to the whole network. Low Energy Adaptive Clustering Hierarchy (LEACH), Threshold Sensitive Energy Efficient Sensor Network (TEEN), Adaptive Threshold Teen (APTEEN), Power Efficient Gathering Sensor Information System (PEGASIS), Sensor Protocol for Information Via Negotiation (SPIN), Diffusion Direct (DD), Rumors Routing (RR), Geography and Energy-Aware Routing (GEAR) and Geographic Adaptive Fidelity (GAF) are all other WSNs protocol.

2.2 Related Works

Nanda (2003) discussed some features in detail. The author described building a secure application authentication system using contexts and Fine-Grained access control (FGAC) system. The research is solely based on database applications.

Lou et al (2006) proposed a fine-grained distributed data access control in wireless sensor network. Their scheme is solely based on FGAC in which each sensor node is assigned a set of attributes, and each user is assigned an access structure which designates the access capability of the user. Thus, overload in FGAC is reasonable in practical scenarios but the efficient update of data encryption keys for sensor nodes as well as distribution of keys to the

legitimate users as well as fine-grained data access control is hard to realize due to the complexity introduced by its management technique. However, strong attacks on WSN are still possible, this is a major limitation of their work.

Buratti et al (2009), discussed the relevant issues of WSNs from the application to design and technology viewpoints. They also stressed further that, there is need to use the communication protocols such as topology and signal processing strategies. Matthys et al (2010) proposed a Fine-Grained and application centric access control for WSNs. The approach is to realize fine-grained access control in WSNs based on three elements, a loosely-coupled WSN component model named LooCI which allows easy inspection of data flows between the components that compose application, second, a flexible and extensible policy engine which also allows fine-grained control of data flows and ensures that these policies cannot be avoided and thirdly, a secure policy distribution channel ensures that only authorized actors, may deploy security policies. Since it is run-time application, it reconfigures itself after the main work has been done on each node. That is, it follows single event condition action.

Jin et al (2010) proposed an efficient attribute-based access control system in cloud computing. In their system, two CSPs namely KG-CSP and D-CSP are introduced as employees to finish outsource the heavy tasks for users' management and file access respectively. A challenging issue in the proposed system is how outsources computational task to CSPs without any private information leakage would be achieved.

Sushmita et al (2011), discussed a fully distributed fine grained access control schemes for distributed networks. The scheme is well secured against collusion of users and supports user join, revocation and access structure modifications. The communication costs are the same as that of Yu et al (2006) scheme which contained only one Trust Authority (TA); hence, it is prone to breaking down on the event that the TA is compromised. The computation costs incurred by the sensors are also the same making the schemes highly practical for distributed sensor networks.

2.2.1 Attribute Policy: Subjects and Objects

Pirretti et al (2006) defined an attribute policy (same as policy) as a specification of cryptographic operations carried out on a plaintext in the attribute-based system. Hence, through encryption, a party is able to insert expressive policies into objects, allowing the decentralized enforcement of such policies. There are two components central to policies characterization: the attributes and the objects. An attributes consists of a uniquely identifying string and names. Objects refer to all encrypted or discovered data. For example, objects in a distributed file system would be the file that it stores. The attribute policy is a specification of the attribute and threshold used to encrypt an object. For example, consider a policy *p* that mandate encryption using a single attribute *a* under a threshold of *1*. $P = t_1(a)$ while the application of attribute place of objects *(Obj)* is denoted by *E(Obj, p)* equivalent to *E(Obj,* $t_1(a)$*)* meaning that *Obj* has been encrypted under attribute *a* using *1*-out-of-*1* threshold encryption function. This object can only be encrypted by a user with right attribute.

3 System Design

Bilinear map, pairing-base is employed in the design. Consider two cyclic groups $\boldsymbol{G_1}$ and $\boldsymbol{G_2}$ of prime order q generated by $\boldsymbol{g_1}$ and $\boldsymbol{g_2}$ respectively. Let $\boldsymbol{G_T}$ be a group of order q, we consider mapping *e* as follows: e: $\boldsymbol{G_1} \times \boldsymbol{G_2} \rightarrow \boldsymbol{G_T}$.

KP-ABE is used for achieving fine-grained data access control. KP-ABE is a type of attribute Based encryption in which each ciphertext is associated with a set of descriptive attributes. Each private key is associated with an access structure or policy that specifies which type of cyphertext the key can decrypt. Thus, a user is able to decrypt a cyphertext if and only if the attributes associated with a cyphertext satisfy the key's access structure or policy. The KP-Attribute Based Encryption scheme consists SETUP, KEY GENERATION, ENCRYPTION and DECRYPTION algorithms.

a. **SETUP**: In the setup phase, the system parameters are chosen by the key attribute authority. The threshold parameter d is decided, such that if a user U_j has at least d attributes in common with the sender T, it can decrypt the message.
Let q be a prime power. $\boldsymbol{G_1}$ and $\boldsymbol{G_T}$ are two groups of order q and
Let g be the generator of the group $\boldsymbol{G_1}$.
e: $\boldsymbol{G_1} \times \boldsymbol{G_1} \rightarrow \boldsymbol{G_T}$ (3.1)
Let W be the total number of attributes.
$t_1, t_2, \cdots, \boldsymbol{t_w}$ and y are chosen at random from $\boldsymbol{Z_q}$.
$\boldsymbol{Z_q}$Set of integers {0,1, ⋯, q − 1}

The following public parameter are published

$$[\boldsymbol{T_1} = \boldsymbol{g^{t1}}, \boldsymbol{T_2} = \boldsymbol{g^{t2}}, \ldots, \boldsymbol{T_w}, \boldsymbol{Y} = \boldsymbol{e}(\boldsymbol{g}, \boldsymbol{g})^{\boldsymbol{y}}] \quad (3.2)$$

Where $(t_1, t_2, \cdots, t_w, y)$ is a master secret key, $\boldsymbol{T_i} \in \boldsymbol{G_1}$.

b. **KEY GENERATION**: The server generates secret keys for the users, depending on the set of attributes it has and its group. It takes groups $\boldsymbol{G_1}$ and $\boldsymbol{G_T}$, the threshold parameter d, set of attributes that a user has as input and outputs the secret keys. The algorithm chooses a d – 1 degree polynomial $p(x)$ at random, such that $p(0) = y$. For i-th attribute,

$$SK_i = \boldsymbol{g^{p(i)/ti}}, \quad (3.3)$$

then the secret key is output as

$$SK = (\boldsymbol{SK_1}, \boldsymbol{SK_2}, \cdots, SK_{n-1}) \quad (3.4)$$

c. **ENCRYPTION**: The server generates public keys and encrypts the message using its public keys. The sender T runs the encryption algorithm, the inputs of which are the message M, the set of attribute U_j it has, and the public parameters. It outputs a ciphertext $\boldsymbol{C'}$ for the message M. The algorithm randomly chooses a value $\rho \in Z_q$. The ciphertext is calculated as

$$\boldsymbol{C'} = (\boldsymbol{u_j}, C = \boldsymbol{MY^{\rho}}, \{\boldsymbol{E_i} = \boldsymbol{T_i^{\rho}}\}\ i \in \boldsymbol{u_j}) \quad (3.5)$$

d. **DECRYPTION**: This algorithm enables a user with valid set of attributes to decrypt the message. The decryption process is performed at each node. It takes as input the ciphertext C, the group $\boldsymbol{G_1}$ and the parameters that a receiving user has and outputs the message M.
Then,

$$e(\boldsymbol{g}, \boldsymbol{g^{\rho p(0)}}) = e(\boldsymbol{g}, \boldsymbol{g^{y\rho}}) \quad (3.6)$$

3.1 Network Architecture and Assumptions

In this work, we consider military WSN to be the network consisting network server or trusted Authority, several sensor nodes and many users. We denote the network server as T, user or subjects as U_j and node or objects as N_i respectively. Both users and nodes have their

unique IDs. The *T* can always be online for easy detection of intruders or threat. It is in charge of issuing, revoking and updating attribute keys for users. The proposed architecture is divided into six phases which are: system initialization phase, user query generation phase, sensor node verification, establishing secure channel between the network users and the sensor nodes, new user and the user revocation. Conventionally, we assume that Subject (Subj) have sufficient computational resources to execute some expensive cryptography operations and also assume that there is loose time synchronization among the sensor nodes. In this scheme, each sensor node is preloaded with a set of attributes- the detected military operations which has been classified as security levels, (TOP SECRET , SECRET, CONFIDENTIAL AND UNCLASSIFIED) as well as public key (PK) depending on a set of attributes that a sensor possess. Each user (Subj) is assigned an access policy with the corresponding secret key (SK). A user (Subj) is able to decrypt the information from the sensor node (Obj), provided it has the matching set of attribute and access policy. Some of the architecture algorithms are:

USER QUERY GENERATION: After the system initialization, subjects can enter the network to access the nodes base on their access privilege. Let assume that group member's Public keys consists of $\boldsymbol{Y_1}, \boldsymbol{Y_2} \cdots, \boldsymbol{Y_N}$ With Que, subjects compute $\boldsymbol{H_1}$(Que) p. To sign $\boldsymbol{H_1}$(Que) p will takes the following step

i. For all i∈ $\{\boldsymbol{1} \cdots, \boldsymbol{m}\}$ and $\boldsymbol{U_i} \neq \boldsymbol{U_j}$, $\boldsymbol{U_J}$ randomly choose $\boldsymbol{a_i} \in \boldsymbol{Z_q}$ and for which the $\boldsymbol{a_i}$ are pairwise different. Compute $\boldsymbol{R_i} = \boldsymbol{a_i}$ p (i≠ j)
ii. Choose a random number $\boldsymbol{a} \in \boldsymbol{Z_q}$
iii. Compute R_j where
$$\boldsymbol{R_j} = \boldsymbol{aP} - \sum_{\boldsymbol{i=1, i\neq j}}^{\boldsymbol{m}} \boldsymbol{H_2}\ (\boldsymbol{Que})\boldsymbol{P}, \boldsymbol{R_i})\ \boldsymbol{Y_i} \quad (3.7)$$
If $R_j = \boldsymbol{\partial}$ or $R_j = R_i$ for some i≠ $\boldsymbol{j}$, then go to (ii).
iv. Compute ∝ where
$$\propto = \boldsymbol{a} + \sum_{\boldsymbol{i=1, i\neq j}}^{\boldsymbol{m}} \boldsymbol{a_i} + \boldsymbol{x_j}\ \boldsymbol{H_2}\ (\boldsymbol{H_1(Que)p},\ \boldsymbol{R_i})\boldsymbol{Mod\ p} \quad (3.8)$$
v. The signature of Que made by the subgroup s from the group $\{\boldsymbol{U_1}, \boldsymbol{U_2} \ldots \ldots \boldsymbol{U_n}\}$ is given by $\boldsymbol{\sigma} = \{\boldsymbol{R_1}, \ldots, \boldsymbol{R_m}, \boldsymbol{Y_1}, \ldots\ \boldsymbol{Y_m},\ \boldsymbol{\sigma}\}$. After that, U_j sends the message {Que, $\boldsymbol{\sigma}$} to the sensor nodes.

SENSOR NODE VERIFICATION: Upon receiving the message {Que, $\boldsymbol{\sigma}$}, each node firstly checks whether the time stamp T_j included in Que is within a given period of time. Then verification of signature $\boldsymbol{\sigma}$ on the query Que is:

i. Compute h_1, where $h_i = H_2\ (H_1(Que)P, R_i) \forall \boldsymbol{1} \leq \boldsymbol{i} \leq \boldsymbol{m}$
ii. Check the equation
$$\boldsymbol{\sigma P} = \sum_{\boldsymbol{i=1}}^{\boldsymbol{m}} (\boldsymbol{R_i} + \boldsymbol{h_i}\ \boldsymbol{Y_i}) \quad (3.9)$$

Signature validity is checked. Then response is sent to the user U_j; otherwise, the message {Que, $\boldsymbol{\sigma}$} is rejected.

SECURE CHANNELS ESTABLISHMENT BETWEEN NETWORK USER AND SENSOR NODES: During the user query generation phase, user U_j randomly chooses c ∈ $\boldsymbol{Z_q}$ and compute cP. cP is added to the query command Que for sensor node to confirm the validity of the query command. It takes the following steps to achieve it

i. The node randomly choose d∈ $\boldsymbol{Z_q}$ and generate dP
ii. Compute sk = d(cP) as the session key between itself and the user U_j. Thus the node can uses the key sk to encrypt require sensor data of U_j.

Subsequently, it uses SK to encrypt sensor data with symmetry encryption. At the same time, it encrypts SK using public key encryption with U_j's public key cP. Then, the node send the

encrypted sensor data to U_j with the private key c, only user is capable of decrypting the session key SK and therefore recovering the original sensor data.

USER REVOCATION: The revocation takes the following steps. Let the value of Y be $(Y)_{old}$

1. TA broadcast $Y^1 = e(g_1, g_2)^{\Delta a}$
2. Each TA can calculate new value of Y as $(Y)_{new} = (Y)_{old}\ Y^1 = e\ (g_1, g_2)^{\Sigma^a \Sigma \boldsymbol{Z_q}\ p^1 \boldsymbol{a}}$. The public parameter $(Y)_{old}$ is change to new $(Y)_{new}$.
3. A new polynomial $p[j]_a(x)_{new}$ is calculated for user U_j TA

$$P[j]_a\ (x)_{old} - p_a + p^1 a$$
$$= p[j]_a\ (x)_{old} + \Delta a$$

Therefore, $p[j]_a\ (0)_{new} = p^1 a - \sum R \sum_{\boldsymbol{m} \in \boldsymbol{Z_q}\{\boldsymbol{a}\}} \boldsymbol{R}\ [\boldsymbol{j}]_{\boldsymbol{am}}$ (3.10)

4. Each TA $a\sum \boldsymbol{Z_q}$ IS selectively broadcast the value of $\boldsymbol{g_1}^{\Delta_a}/\boldsymbol{t_{a,i}} = g_1^{p[j]_a}(i) + \Delta a$, while $i \in B[a]\ j$, to each non revoke authorized users U_j.

The secret key is $(SK_{a,i})_{new} = (SK_{a,i})_{old}\boldsymbol{g_1}^{\Delta_a}/\boldsymbol{t_{a,i}}$ for each attribute $i \in B[a]\ j$, and given to users.

3.2 Classification or Users' Grouping

The principle of Bell Lapudala model (Ogundele, 2011) which requires subject be given access to the objects (an entity that contained information that is protected.) is adopted. The groups are classified into two distinct classes: the subjects and the object.

Subjects Class: The ranking start from OF – 10 (top most rank) and goes towards OF – 1 which is the least. The category notations are:

$\boldsymbol{S_1}$= { $\boldsymbol{S_G}$, $\boldsymbol{S_{LG}}$, $\boldsymbol{S_{Mjg}}$, $\boldsymbol{S_{Brg}}$}, $\boldsymbol{S_2}$ ={$\boldsymbol{S_{col}}$, $\boldsymbol{S_{Lcol}}$, $\boldsymbol{S_{Lmaj}}$, $\boldsymbol{S_{cpt}}$, $\boldsymbol{S_{Liut}}$,}, $\boldsymbol{S_3}$ = { $\boldsymbol{S_{2nd\ lieut}}$, $\boldsymbol{S_{mwo}}$, $\boldsymbol{S_{wof}}$, $\boldsymbol{S_{ssgt}}$, $\boldsymbol{S_{sgt}}$,}, $\boldsymbol{S_4}$ = {$\boldsymbol{S_{rof}}$, $\boldsymbol{S_{lcorp}}$, $\boldsymbol{S_{corp}}$}.

The subjects categories can be grouped together to form a general class given as: S= {$\boldsymbol{S_1}$, $\boldsymbol{S_2}$, $\boldsymbol{S_3}$, $\boldsymbol{S_4}$, } in which $\boldsymbol{S_1}$,> $\boldsymbol{S_2}$, > $\boldsymbol{S_3}$, > $\boldsymbol{S_4}$. This shows that group S_1 is the highest ranking in the classes of subjects, follow by the $\boldsymbol{S_2}$ down to the least.

Object Class: They are encrypted information or data pre-deployed to all the nodes which can be categories as follow O= {$\boldsymbol{O_{ts}}$, $\boldsymbol{O_s}$, $\boldsymbol{O_c}$, $\boldsymbol{O_{uc}}$,} where O stand for the object and the subscripts are the security classification level ranging from top secret to the least i.e Top secret (ts), Secret (s), Confidential (c) and Unclassified (uc).

Access Policy: The access policies are formed from the subject and the object class. Let the O be a universal set and L_1 to L_4 be the level at which each subjects can operate in the network as represented below:

$\boldsymbol{O_{L1}}$ = {$\boldsymbol{O_{ts}}$, $\boldsymbol{O_s}$, $\boldsymbol{O_c}$, $\boldsymbol{O_{uc}}$,}, O_{L2} = {$\boldsymbol{O_s}$, $\boldsymbol{O_c}$, $\boldsymbol{O_{uc}}$,}, O_{L3} = {$\boldsymbol{O_c}$, O_{uc}}, O_{L4} = {O_{uc}}

In view of these, $S_1 \rightarrow O_{L1}, S_2 \rightarrow O_{L2}, S_3 \rightarrow O_{L3}, S_4 \rightarrow O_{L4}$, this means that for a subject to be able to encrypt an object, the subject must belong to the group list pool that had register with the network administrator based on their attribute possess.

Let S_n denotes all subjects class where $(n \in \{1, \ldots, 4\})$ and O_y denotes all the object class O_y where $(y \in \{ts, s, c, uc\})$. A direct mapping between the members of n and y, this implies that every member of n takes a corresponding value of y. Thus, S_n combined with O_y gives:

S_n: $O_y \rightarrow S_1\ O_{L1}$, S_n: $O_y \rightarrow S_2 O_{L2}$, S_n: $O_y \rightarrow S_3 O_{L3}$, S_n: $O_y \rightarrow S_4 O_{L4}$

Therefore,

$$A = \begin{cases} 1 \text{ iff } S \subset S_n O_y \in \{1ts, 2s, 3c, 4uc\} \\ 0 \text{ Iff } S \not\subset S_n\ O_y \end{cases}$$

Where A is an access, S =subject, S_n = subject Class, O_y = Objects class

4 Results and discussion

User Authentication

The system was able to authenticate both the administration and the users using the back end (Database) user authentication system. The authentication is done by comparing the user input in the front end, process it at the middle layer, and then authenticate it in the database. If the matching is correct by entering the right username and password, the system grants access. Else access is denied.

Creating Account

Users enter their Username, e-mail, phone number, Password, Re-enter password, Full name and Rank which generates access level automatically. In most cases the username might be part of the user's full name and in some cases it might be different from the user's full name. The essence of re-entering password is to ascertain the correctness of the password given. In most cases the full name might be more than two names depending on the choice of the user. Also, the ranking order assigned to users is different from one another depending on the cadre of the personnel. These rank orders ranges from highest to the lowest in the military. Each user is expected to have an accessible e-mail address that could be used to contact personnel in case of any information that needs prompt action. An access level of each user differs from one another as this could be used to differentiate a user that is assigned access level from those that do not have. Another security measure is the user's phone number which is a unique identifier; these can as well be used to distinguish a user from others.

Uploading a File

On this part, Admin specifies or gives a description or the name of the locality where the data is generated and also the type of officer or personnel that can view it. Access level is selected which generates or assigns secret key to the file. The essence of these is to secure the uploaded file from unauthorized user such that without the rightful secret key coupled with an assigned access level, such user will not be able to deploy a file (confidentiality).

Accessing an Uploaded Files

Accessing an already uploaded file, a user needs to enter assigned secret key before download of any files. Once the secret key is entered correctly, it compared with the stored secret keys in the database, which will determine maybe access will be granted or not in order to download any file. This security measure; secret key prevents unauthorized users from accessing files in the database.

Performance Analysis

The performance analysis is evaluated using the following standard metrics namely: execution time, energy consumption, and size of the key.

The execution time measures the duration of the operations performed by users during the decryption and while querying a sensor data. The energy consumption estimates the energy consume during the process and also considers eave-dropping because the propose system work on a wireless network environment and it is necessary to consider intruders who may want to hijack information transmitted on the wireless network and compromise its privacy. The energy consumption is different from conventional wired and wireless networks, wireless sensor networks have a major energy issue because most wireless sensors cannot be charged after being deployed, and energy loss causes node failure and finally leads to entire network failure. The energy problem is very complex. Many researchers proposed different ways to

reduce energy consumption as much as possible. However, an accurate measurement of energy consumption remains a challenge to the work.

Users	Response time (sec)	Size of the data (KB)
User 1	5	10
User 2	10	20
User 3	12	30
User 4	15	40
User 5	20	50
User 6	25	60
User 7	30	70
User 8	35	80

Tab. 1. *Response time for decryption. Source Authors.*

Tab. 1, shows the chosen users from a group of sensor network during decryption period and their response time being recorded. The size of a given key (ABE) is set to be 260 and 292 which is considered enough to secure the sensor data. The response time and the size of the key (ABE) vary in length during decryption process.

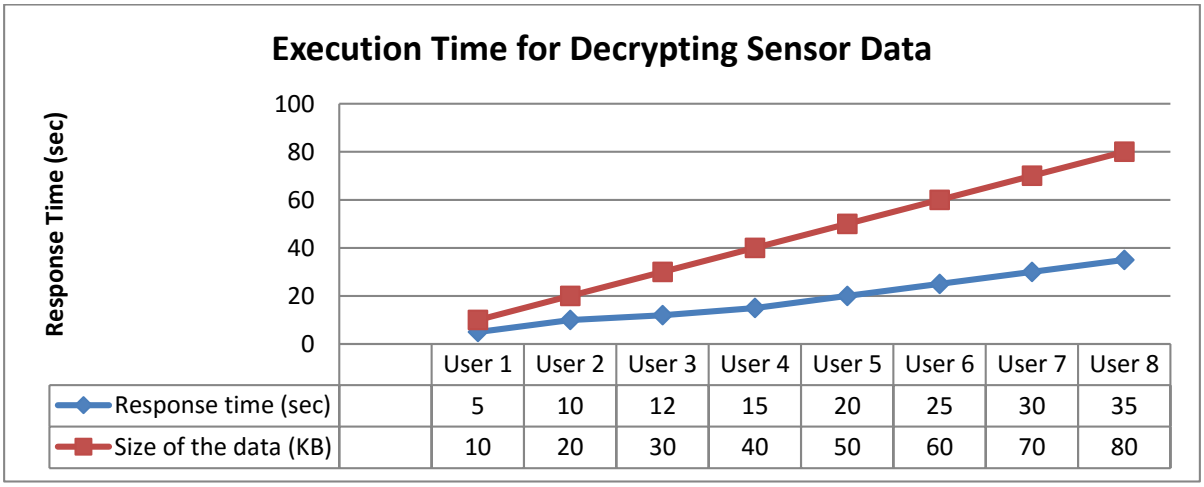

Fig 2. *Execution time for Decryption in a Sensor Node. Source Authors.*

Metrics	Proposed system	He et al (2011)
Execution time	Take a very short time to execute a given data	Takes a longer time
Energy consumption	Unable to actualized the real total energy consumption due to lack stable electricity	It actualize to an extent
Size of the key	260-bit and 292-bit (ABE)	160-bit and 192-bit (ECC)

Tab. 2. *Summary of comparative analysis. Source Authors.*

5 Conclusion

In this work, a fine grained data access control that enforces security controls and ensures data accessibility only to authorized entity has been developed. The architecture address the security challenges often encounters in a WSN especially in a mission-critical application. Technology is a dynamic concept which is constantly changing and as it is changing, the security measures should also change to keep up the standard. This system is easy to use, secure and has an interactive user interface and can also be used for purpose of authentication, limit of access privilege and user revocation for secure access into the system. It is therefore; recommended that this research work should be adapted to different terrain of life such as health institutions and government. The main challenge is the power consumption for effective data delivery and also improve the bandwidth of WSN.

References

Alese B. K. (2000). *Vulnerability Analysis of Encryption / Decryption Techniques of computer network security*. Master Thesis. Akure: Federal university of technology Akure.

Bhattacharyya, D., Kim T-h, & Pal, S. (2010). A Comparative Study of Wireless Sensor Networks and Their Routing Protocols. *Sensors*, 10, 10506-10523. doi: 10.3390/s101210506

Buratti, C., Conti, A., Dardari, D., & Verdone, R. (2009). An overview on wireless sensor networks technology and evolution. *Sensors*, 9(9), 6869-6896. doi: 10.3390/s90906869

Cook D. J. & Das S. (2004). *Smart Environments: Technology, Protocols and Applications*. New York: John Wiley & Sons.

He, D., Bu, J., Zhu, S., Chan, S., & Chen, C. (2011). Distributed Access Control with privacy support in wireless sensor networks. *IEEE Transactions on Wireless Communications*, 10(10), 3472-3481. doi: 10.1109/TWC.2011.072511.102283

Ferraiolo, D., Cugini, J., & Kuhn, R. (1995). Role Based Access Control: Features and Motivations. In *Proceedings of the Annual Computer Security Applications Conference*, pp. 241-248, New Orleans: IEEE Computer Society Press.

Hac, A. (2003). *Wireless sensor network designs*. Etobicoke: John Wiley & Sons.

Han, K. Kim, K. & Shon, T. (2010). Untraceable Mobile Node Authentication in WSN. *Sensors*, 10, 4410-4429. doi: 10.3390/s100504410

Shon, H. (2012), *All-in-one CISSP Exam Guide*. Emeryville: McGraw Hill Osborne.

Hill, J. L. (1998). *System Architecture for Wireless Sensor Networks*. Doctoral Dissertation. Berkeley: University of California.

Lewis F. L. (2004). Wireless Sensor Networks. In D.J. Cook, S.K. Das (eds.), *Smart Environments: Technology, Protocols, and Applications*. New York: John Wiley.

Li, M., Lou, W., & Ren, K. (2010). Data security and privacy in Wireless body area networks. *IEEE Wireless communications*, 17(1), 51-58. doi: 10.1109/MWC.2010.5416350

Matthys, N., Afzal, R., Huygen, C., Michiels, S., Joosen, W., & Hughes, D. (2010). Toward Fine-grained and application-centric Access control for wireless sensor networks. In *Proceedings of the 2010 ACM Symposium on Applied Computing* (pp. 793-794). New York: ACM. doi: 10.1145/1774088.1774252

Nanda, A. (2003). Fine grained access control. International Oracle users group publication. Retrieved from http://www.proligence.com/nyoug_fgac.pdf

Ogundele, O. S. (2011). *Design of multilevel access control model for delegation based on attributes separation of duty and trust*. Master thesis. Akure: Federal University of Technology Akure.

Pirretti, M., Traynor, P., McDaniel, P., & Waters, B. (2006). Secure Attribute-Based Systems. In *Proceedings of the 13th ACM conference on Computer and communications security* (pp. 99-112). doi: 10.1145/1180405.1180419

Shon, H. (2012). Cryptography. In *CISSP All-in-One Exam Guide*. New York: McGraw-Hill Education.

Sohraby, K., Minoli, D., & Znati, T. (2007). *Wireless sensor networks: technology, protocols, and applications*. New York: Wiley.

Ruj, S., Nayak, & A. Stojmenovic, I. (2011). Distributed fine-grained Access control in Wireless Sensor Networks. In *IEEE International Parallel & Distributed Processing Symposium* (pp. 352 - 362). New York: IEEE. doi: 10.1109/IPDPS.2011.42

Tubaishat, M., & Madria, S. (2003). Sensor networks: an overview. *IEEE Potentials*, 22, 20-30.

Wayne, W. M. (2000). *Wireless Sensor Network Topologies*. Retrieved from http://archives.sensorsmag.com/articles/0500/72/

Campete, S. A., & Yener, B. (2005). Key distribution mechanisms for wiles sensor networks: a survey. Retrieved from https://www.cs.rpi.edu/research/pdf/05-07.pdf

Yu, S., Wenjing, L., Kui, R. (2006). FDAC: Toward fine-grained distributed data access control in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 22(4), 673-686. doi: 10.1109/TPDS.2010.130