A Novel Node Integrity Based Authentication Model For Dynamic Wireless Communication Networks

Madhuravani Bandanatham
MLR Institute of Technology
India
madhuravani.peddi@gmail.com

Murthy DSR
Geethanjali College of Engineering & Technology
India
dsrmurthy.1406@gmail.com

ABSTRACT: *Communication in wireless networks has significantly increased over the past few years due to its complex topological structure and malicious attacks. Secure wireless networks must address several issues: data security, node security, key distribution, malicious attacks, node compromise attack, replay attack, etc. Further, many traditional security and authentication models have been implemented on limited wireless nodes with predefined node configuration. Detection and prevention of the security issues in wireless networks with low computational cost has become a major problem in traditional authentication protocols. Therefore, a novel secure authentication mechanism is essential for ensuring the message integrity, security and against attacks. In this paper, a novel message integrity based secured authentication model was implemented on the wireless network topology for secure node communication. The entire model is presented in two phases – sender side data encryption with integrity embedding phase and receiver side data decryption with integrity verification phase. Experimental results proved that the proposed authentication model has low communication cost and low storage overhead compared to traditional authentication models.*

Keywords: Wireless Sensor Networks, Authentication, Integrity Verification, Chaotic, ABE

Received: 15 September 2017, Revised 19 October 2017, Accepted 4 November 2017

1. Introduction

In recent years, wireless networks have received a huge attention due to their applications in various domain areas such as wildlife monitoring, traffic monitoring, military environments, data communications, etc. In wireless networks, security and authentication are the major issues for efficient and reliable communication. Based on the type of the communication protocol various communication problems and attacks are addressed. Although wireless networks are economically feasible, their computational requirements and constraints prevent the direct communication in the existing authentication protocols.

Authentication in each node will authenticate with the other node in the wireless network through security codes or schemes. Also, it is hard to authenticate every node in the network during communication. Each sensor node has the capability to process, sense and communicates with each other, so it is data centric network. The data transmitted between the wireless nodes may be sensitive, and the whole network will be threatened if any malicious node enters into the network.

Wireless sensor networks need to guarantee the node security, data security including authentication, confidentiality, integrity and attack monitoring. Cryptography and integrity models are the major security technologies used to secure wireless networks during the node communication and data transfer. At present, the models to secure the wireless network are node encryption, integrity ensuring, message authentication, broadcast verification, and node validation. Most of the traditional security models focus on key exchange, key distribution and data management mostly. The key management and authentication models in wireless networks become a major issue due to its network size and static node configurations.

Data hiding is an essential technique used for the purpose of annotation, identification and integrity checking. Wireless sensor networks have two types: hierarchical and distributed. In distributed wireless network, each node communicates with each other node in multi-hop wireless communication and data are sent to the base station directly. In hierarchical wireless sensor networks, the network consists of the cluster heads and base station for data communication. Each sensor node communicates with the other nodes in a cluster and then sent data to the cluster head for data integrity verification and storage.

Sensor nodes in the wireless environment are resource scarce and are deployed in a static environment to report about the region of interest. To increase the flexibility and capability of sensor nodes, dynamic mobility in sensor nodes was implemented. The mobile wireless sensor network consists of sensor nodes that are movable in a network. Mobility is achieved in sensor node by equipping it with mobility for changing their location. Recent researchers prove that mobile wireless sensor network outperforms than the stationary sensor networks but lacking security and data storage. Some of the advantages are

1. The lifetime of sensor nodes increases using mobile sensor networks.
2. Reduces energy consumption during communication.
3. MWSN has better channel capacity compared to the stationary sensor networks.

Even though there are several advantages, sensors are kept unattended for long time and they are not equipped with tamper resistant hardware. This arises many types of attacks in MWSN.

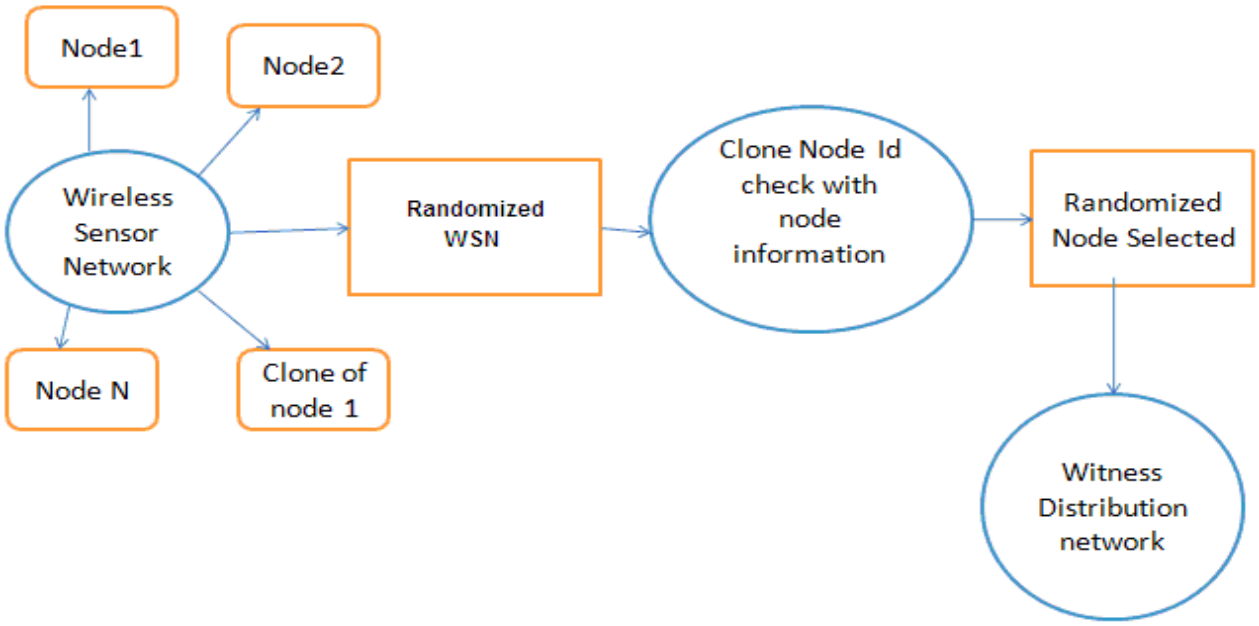

Figure 1. Clone node creation and detection

Create a group of sensor nodes. The randomized network gives the different unique ID to each node and makes that node as original node. Here, WSN is partitioned into randomized node cluster with the arbitrary shape as shown in figure 1.

Randomized Node Clone Creation:

• Randomly Select Clone Node in the arbitrary network as cn.

• Attacked node= nodes.elementAt(cn);

• Add node in the network.

• clonedNodeID = attacked.nid;

• encode clone signature and message.

• Hashing the position of the nodes in the network.

Detection Approach:

• Each node board cast its ID and location to its claim.

• Neighbors receive the broadcast and each neighbor sends the claim.

• The claim is sent to any of the location. This is selected using the pseudo-random function.

• Before broadcasting, every node signs its message.

• Signature is verified at the destination end.

• At the Client WSN:

1. The signature check is carried out by verifying the received signature.

2. Message freshness: The ID and location information is extracted from received message. At the destination end, it simply stores the ID and location if the claimed node is first carrying that ID and location.

3. If it receives the same ID and location for the second time, it checks for the coherence for ID and location. This is the proof of detection of a clone with two in-coherent claims. Coherent values are identified by using signature and hash values of the positions. It detects the cloned node.

4. **C**lone node information is broadcasted to all other nodes. By this, we can avoid the claim of the cloned node with other nodes in the network.

Traditional data encryption models ensure secure transmission with high computational resources, which could significantly decrease the communication performance. Mobile sensors have a large collection of sensor data such as the accelerometer, clock, microphone, light sensor, thermometer, and compass. Virtually every sensor data are time-stamped and enabling it to be paired with data values of other sensor devices. Mobile applications use this sensor information by operating user requested queries. Computations on the sensor data could be complex to process user queries on the mobile devices. So, different offloading or energy efficient methods are used to handle large sets of sensor data.

Wireless network selection has been studied a lot in recent few years, but there are still many problems that have not been solved. Thus much effort has been necessary for developing wireless selection algorithms using multi-criteria radio access technology. Some problems result in sub- optimal network selection results; while some problems are serious enough to make a network selection scheme unable to work. These problems are described as follows:

• A wireless network selection scheme usually considers multiple groups of factors simultaneously, including operator policies, network attributes, node preferences, terminal properties, application QoS levels.

• Besides attributes, another important part nof a network selection scheme is the weights of these attributes. Weights decide the relative importance of different attributes, while this relative importance usually decides the best network. Therefore, correct

weights are necessary, while wrong weights usually lead to wrong decisions.

• Another problem is the consideration of traffic load during network selection because a network with the limited resource should not be selected.

Nowadays, multiple wireless networks are being developed simultaneously, and these networks have different characteristics and could complement each other. In our study, a large number of characteristics of these networks should be considered, including monetary cost, power consumption, mobility support capability, bandwidth, bit error rate, and so on.

To ensure data security, many encryption models have been implemented to encrypt data in wireless networks. Some of the traditional data security schemes in wireless networks are described below.

Data Security Schemes In Wireless Networks

Attribute-based encryption and decryption scheme was firstly suggested by *Sahai* and *Waters* in the year 2005. In order to gain more security and access control, the above scheme was proposed. This is considered as an important objective for this algorithm. Users' attributes act as a basic component for the generation of secret key and cipher text. Decryption is effective and possible if and only if, secret key, as well as cipher text, are equivalent to threshold *d.* This algorithm is collision resistant. The major flaw of this approach is that users' public keys are essential for the process of encryption through data owner. As monotonic attributes are included here, the approach restricts the application of the model in real world scenarios.

The conventional ABE scheme is extended to give rise Key policy attribute-based encryption scheme. Access tree structures are used for the representation of this model. Each user is associated with an access tree. Threshold gates are used to denote the nodes of these access trees whereas, leaf nodes are represented by attributes respectively. In the case of KPABE, both ciphertext and secret key are merged with attributes. Here while cipher text is merged with attributes, the secret key is integrated with monotonic access trees. The combined components are responsible for management and control of cipher text in decryption. It can be successfully applied in one-to-many communications channels. The only lacuna of this approach is that it has no control on who has decryption rights.

CPABE scheme was introduced by *Sahai.* This scheme follows the basic concept of the merger of the cipher text with access policy as well as the combination of secret keys with attributes. Users are able to decrypt ciphertext if and only if the respective attributes satisfy the access policy. The idea of CP-ABE is just the reverse mechanism of KP-ABE. CP-ABE acts as the basic unit for many other schemes because of its flexible nature. KP-ABE has the disadvantage of no control on decryption rights. This issue of the previous approach is resolved here. It has also implementation in real world scenario. This proposed scheme faces also a severe problem, that is: - It cannot be implemented in an enterprise scenario. This flaw occurs because of low flexibility and inefficiency/ poor efficiency. The whole process of decryption requires attributes of a single set. Thus, users are eligible to select single attribute or combination of attributes from that specified set. Later this disadvantage of CP-ABE scheme was encountered and overcome by another newly developed approach, i.e., CP-ASBE (Ciphertext Policy Attribute Set Based Encryption).In this approach, key attributes can be selected from various different sets of attribute sets. This problem of the prior model was resolved here. This scheme is not effective for merging attributes in case of multiple keys.

Hierarchical attribute-based encryption model was developed by *Wang*. The whole model was represented by the hierarchical structure. The key generation process is carried out by a root master, which interacts with several different domain masters. Every domain master again interacts with numbers of enterprise users. The said model has its applications in cloud enterprise domain and in proxy re-encryption. This scheme is theoretical one and it's impossible and too expensive to implement practically. Conjunctive clause attributes are managed by same domain authority, whereas similar attributes are managed by multiple domain authorities.

All the previously described schemes are categorized under monotonic access structures. Monotonic access structures do not contain any negative constraints. A novel modified version of attribute-based encryption along with non-monotonic access structure was implemented on WSN. The negative constraints are generated only in case of non-monotonic access structures and these constraints are absent in the case of monotonic access structure. The only drawback of this method is that the data overhead is increased exponentially because of these above said negative constraints. The negative constraints increase the data overload but do not relate to data.

Wireless Sensor Network (WSN) can be defined as collection of small computing devices connected through a network. In WSN, the small computing devices are called as sensor nodes and these have very restricted amount of resources. Here, the sensors gather all required information from its surrounding range and transfer these information to another sensor node, known as Gate Way Node (GWN). GWN is also known as Base Station that is very efficient in terms of computation. If required, only authenticated wireless nodes are allowed to request and access the gathered data.

There exist two types of node authentication process in Wireless Sensor Networks, those are mentioned below [1]:-

1. It is mandatory to authenticate each node themselves at GWN, before accessing the gathered data from sensor nodes.

2. All nodes can directly request sensor node in order to authenticate themselves with it.

As the sensor networks contain huge amount of sensitive data, many attackers try to get access to these sensitive information in an unauthorized way. Some common attacks of WSN are:- node capture, physical tampering and denial-of-service. Therefore, varieties of security measure have been taken in order to make WSN more secure and reliable.

As Wireless Sensor Networks are very much different than that of traditional Wired Networks, previously developed security algorithms can't be implemented here. There exist some challenges in the application areas of WSN, those are stated below:-

1. Wireless Sensors have limited energy, computation speed along with poor communication.

2. These are mostly implemented in accessible locations. Thus, the chances of physical tamper also increases.

3. These types of networks generally interact more with its surrounding nodes. Therefore, the security risk also increases.

Elliptic Curve Cryptography (ECC) is a most accepted approach in multi-factor authentication. It decreases the computational cost to a great extent while providing extended security than that of conventional authentication schemes. ECC is applicable in different areas like smart cards, RFIDs, WSNs, digital signatures, and so on [1-6]. Bilinear pairing is an important function of ECC. According to [7], the overall cost of a single bilinear pairing is twice greater than a single modular exponentiation. Hence, this rises as a major security issue in ECC approach. An attacker may compel the server or users to invoke ECC repeatedly.

Generally, the authenticated wireless nodes store their sensitive credentials at the cluster head. By means of some mathematical operations, the wireless nodes need to verify their identity in order to get access. In [10], an interception attack takes place that blocks the message travelling from wireless source node to its nearest target node containing authentication details. In some protocols these authentication details are encrypted but, there also exist some protocols where these remain unencrypted. In some cases the message contain a time stamp, after exceeding that time stamp the message expires automatically. Security is a major concern in case of WSN due to an unauthorized deployment of sensors in their environment. In these scenarios, high risk of eavesdropping and network tampering exist. Wireless sensors are basically dynamic in nature, due to frequent rearrangement of communication channels. Most of the previously developed encryption and decryption algorithms require very high computational resources. This results in decreasing the sensor life span. Besides these due to the drawback of limited memory space and processing power, traditional cryptographic algorithms are of no use**.**

Attacks On Wsn Routing Protocols

Most of the sensor networks have simple network routing protocols [9]. This makes the network more vulnerable to different types of attacks. Some types of network layer attacks are mentioned below:-

• Spoofed, Altered, or Replayed Routing Information
In this type of attacks, the routing details which are interchanged in between different nodes are targeted. This can occur either by spoofing, altering or replaying the routing details. The attackers apply many techniques to utilize the valuable network resources unnecessarily. Creation of routing loops, random expansion or compression of routes, false error detection alarm etc. are categorized under this category.

• Selective Forwarding
Generally, multi-hop network transmits messages throughout the network by forwarding it from node-to-node. In case of a

selective forwarding attack, the malicious nodes do not forward that packet as it is. It may delete packets in order to hamper the network transmission process. There are also chances of partial or total network failure.

• Sinkhole Attacks
In this type of attacks, the aim of the attacker is to divert all the network traffic towards the compromised nodes. It acts like a sinkhole and the attacker is placed at the center. In case of sinkhole attack, the compromised node seems more attractive to all other nodes in the network.

• The Sybil Attack
In this attack, every node is represented by multiple identities. Most of the geographic routing protocols suffer from this Sybil attack. All location-based routing techniques interchange their coordinate details with the surrounding nodes to result an efficient routing scheme.

• HELLO Flood Attack
In most of the routing protocols, a HELLO packet is sent by a specific node to its neighbours. All nodes receiving the packet are considered to be in the radio range of the sender node. An attacker having high transmission capability can broadcast to all nodes in a network with a HELLO packet. This unnecessary wastage of network resources will create network congestion.

• Acknowledgement Spoofing
Most of the network routing protocols depends on implicit or explicit link layer acknowledgements. An attacker is capable to spoof link layer acknowledgements for overheard packets of their neighbours.

In a specific region, stationary, movable and powerful base stations may exist. Let us consider, all the nodes are aware of their destination ID. At the time of need, each node is capable to transmit data to the respective base station. The whole network topology changes time to time because of mobility. It is not possible to transmit data directly to its base station. Therefore, a hop is detected in the direction of its destination. The process continues until the data reached to its required destination. These hops are needed to be authenticated in order to provide secure transmission of data. Thus, we have added a new field (i.e., secret field) in the previous format of request packet [5].

2. Related Works

[1] Addresses security issues in cluster-based wireless sensor network, where nodes are mobile and dynamic in nature. In the first step, whenever a node enters in a new cluster, it should be authorized by the cluster head using mutual communication. In the second phase, the old and newly formed clusters are communicated to each other for security analysis or data exchange. This newly formed cluster re-authenticates the newly admitted node through the authentication process. The authentication process is done with the help of pair-key and the hash value of the wireless node and the cluster head. Most of the traditional models failed to minimize the response time, load balancing and conserve energy. If the energy increases, then response time also increase, so energy (E) is directly propositional to response time (R). The model proposed in [2] has three phases of virtual wireless instance i.e., idle, sleep and busy. Busy state signifies virtual wireless instance is operating at high speed, but incomplete workload whereas idle state signifies virtual instance is operating at high speed but no workload immediately. Sleep state virtual demands more time to alert as differentiate to the busy state. The algorithm analyzes least load LL, left capacity, LC, and unbalanced load UL. If LC specifies left capacity operating at a low level, then this state launches a large number of wireless instances.

[3] designed and implemented a novel authentication protocol with integrity verification process in secured WSNs. In this model, shared key-pair is used for ensuring authentication. Here, node authentication technique exchanges a common key matrix between the sender and receiver as an authentication key. As the number of nodes increases, it becomes difficult to manage and provide security to each node in the network. [4] Implemented an energy minimized and delay resistant centralized MAC protocol for wireless networks and contemporary encryption techniques. This model mainly focuses on using the SEA together with the EDCMAC not only to provide a cost-effective solution but also to allow highly secure and energy-aware/ delay-sensitive data transfers in WSNs remaining functional much more long time. The work is to be furthered to realize the integration of the SEA and other common WSN MACs.

Further, an extended amount of researches carried out to propose efficient cryptographic schemes for WSN. They developed a

new cryptographic approach and named it as Elliptic Curve Okamoto-Uchiyama (EC-OU). They considered a public key encryption technique in their proposed scheme for WSN [5]. However, it requires large memory space in order to store this generated cipher text. Thus, the issue of limited memory space can't be resolved in this technique.

[6] presented a special type of block cipher cryptographic technique. It basically uses two separate techniques, those are:- chaotic S-box algorithm and Substitution-permutation (SP) networks. The proposed approach supports variable-sized encryptions, whereas discards floating-point operations. In [7], Light Encryption Devices are developed which uses the concept of light weight block cipher. In the interval of four rounds, the algorithm produces a new key by using the old key and X-OR operation. Thus, the presented approach needs more numbers of CPU cycles than that of traditional algorithms. [7] implemented an improved block cipher technique and termed it as TWINE . It requires a key of 80-bit or 128-bit. In order to provide more security, the length of keys is increased. This will result in high consumption of energy.

In order to resolve the issue of high computation overhead of asymmetric cryptography, [8] proposed a new algorithm. It depends on a cyclic group having elliptic curve points. They presented an improved approach of encryption by merging ECC and Chaotic map. Here, these curve points are responsible for verification of sensor nodes.

Later, [9] modified the previous technique and presented an updated version of SecLEACH algorithm for secure cluster-based WSNs . This proposed approach combines random key pre-distribution with authenticated broadcast mechanisms in order to provide security in WSNs. It results hierarchical WSNs along with its cluster details.

The main objective of any wireless network scheduling problem with data nodes, cluster head and base station is defined as minimizing the total cost in the secured data transmission caused by downtime t_d, the cost of migration t_m, the cost of execution. t_e, operational cost t_o, and cost of communication t_c.

$$Total\ Cost: = Min\ \{t_m + t_o + t_e + t_c + t_d\}$$

Subject to Constraints:

• At any time t, a task takes only single resource from the wireless node.

The sum of all requested resources against the available tasks=1;

$$\sum_{i \in R} r_i = 1$$

• Each task should handle one resource per cluster head.

$$r_{ij} \le R_i, \forall r_{ij} \in Clusternode_j$$

R_i; Set of all i^{th} cluster resources.

• Total resource utilization of all tasks should not exceed the total execution time of the resources.

$$\sum_{j \in Tsks} r_{ij} e_i \le E_i$$

Where e_i denotes execution time of the server task on resources.
E_i denotes total execution of the resources.

• Total memory usage of all tasks per resource should not exceed the total available resource storage.

$$\sum_{j \in Tsks} r_{ij} m_i \le M_i$$

Memory Constraints:

$1 \le i \le R$; Total resources.

$1 \le j \le T$; Total Processing Time

$r_{ij} \in \{0,1\}$

Let $E = \{ (i, j) : i, j \in V_m, i \neq j \}$ is a set of nodes joining the virtual wireless instances, with ant travel distance or cost.

Let $C_{vm} = \{ c_{ij} : i, j \in V_m, i \neq j \}$ is the cost of traversing between the virtual wireless instances (nodes).

Let ψ be the total number of ants each with capacity ψ_c and task assignment to wireless instances based on the stochastic demands and variables. Here wireless node instance, demands are stochastic variables ρ_i, where $i = \{ 0,1,, \ldots n\}$, which are independently distributed variables with known data distributions. Here the total demand of each Wireless instance is not known until the ant is not arriving at the wireless instance. Here they consider the demand ρ_i does not exceed and ψ_c follows a normal distribution with probability mass function(pmf).

$$pmf = Probabililty(\rho_i = d),$$

Where d is total demand of Wireless instance $d \in w$: whole number.

$$\text{Pmf} = \sum_{i=1} P(d_i), \text{ In case of discrete model}$$

$$\text{Pmf} = \int f(d_i)dx, \text{ In case of continuous model}$$

These stochastic capabilities may incur unpredictable usage in communications within mobiles and the cloud. In particular, recent studies, illustrate that the power usage for transmitting a fixed amount of data is inversely proportional to the accessible bandwidth.

According to the Wireless instances, node demand of the ant resolves whether to continue to the next Wireless instance or to go back to the user task execution for re-stocking of new task.

$B_{i,j,k}$ = *Binary flow variable*

$B_{i,j,k}$ = 1, if the path between (i, j) is traveled by k^{th} agent.

$B_{i,j,k}$ = 0, otherwise

$J_{i,k}$, Task components uploaded at i^{th} wireless instance by k^{th}.

ψ : Total number of ants initiated by the task controller.

η : Remaining unallocated tasks of the ants.

C_j: Capacity of tasks carried by the ants.

$\alpha^p_{j,k}(\eta)$: Predicted cost of forward task actions.

$\alpha^r_{j,k}(\eta)$: Predicted cost of restocking tasks.

If $\alpha_{j,k}(\eta)$ is the task allocated to the j^{th} Wireless instance by the k^{th} agent, then the objective function can be formulated as:

$$\alpha_{j,k}(\eta) = \min(\alpha^p_{j,k}(\eta), \alpha^r_{j,k}(\eta))$$

where

$$\alpha^{p}_{j,k}(\eta) = c_{j,j+1} + \sum \alpha_{j+1,k}(\eta - d)\,\mathrm{p}_{i+1}, if\ \mathrm{d} \le \eta \text{ and}$$

$$\alpha^{p}_{j,k}(\eta) = \sum 2c_{\hat{\partial}j+1,0} + (\eta + c_j - d)\alpha_{j+1,k}\,\mathrm{p}_{i+1,d}, if\ \mathrm{d} > \eta$$

$$\alpha^{r}_{j,k}(\eta) = C_{0,\mathrm{j}+1} + \sum \alpha_{j+1,K}(C_j - d)p_{j+1,d} + C_{j,0}$$

Integrating eq(1) we get

$$\int_{C} \alpha^{r}_{j,k}(\eta) = C^{2}{}_{j,0} + C^{2}_{0,j+1\cdot} + C_{j,0}\sum \alpha_{j+1,K}(C_j - d)p_{j+1,d}$$

Let $Q_i(t)$ be the number of unfinished components request at the beginning of the t-th execution.

$$Q_i(t) = \max[\alpha^{r}_{j,k}(\eta) - 1, 0] + \sigma(\alpha^{r}_{j,k}(\eta))$$

The one-opt component search algorithm works as follows.

• Initializing the feasible solution with all the available components.

• After that a neighborhood search based unitary Hamming distance (data that differ in only one bit to the original data) is used to find the best solution.

[10] analyzed that, many research efforts have been carried in this domain concentrating on computing utility and new applications. They analyzed various pre-existing techniques calculating storage patterns on cloud, which led to some storage and sharing problems. These above mentioned issues are needed to be resolved, which encourages the authors to present a modified tree-based approach. It also resolves some other problems such as data encryption, boundary maintenance and data proof. All these operations are controlled and managed by view management scheme. Some of other advantages of this technique are:- entity privacy, data availability and safe data sharing etc. Each and every user has its own view and also has a secure boundary.

[11] proposed a attribute-based encryption scheme along with fine-grained access provision. They identified the sole demerit of CP-ABE model, that is:- the data owner has no idea about the original data users. Thus, level of fine-grained access reduces. Before the data owner starts interchanging information, it searches all relations between data access policies and users and, its attributes. Through this method, original data users' information are obtained. User access is obtained only where attribute access is same as user access. The researchers performed validation on their theory and evaluated the proposed work. They found that, the issue of fine-grained access is resolved by the said technique. The resulted outcome outperforms other existing traditional approaches. Further future work can be carried out to implement this suggested method in multi-privileged one-to-many communications.

[12] developed a new approach for ABE using quadratic residue technique based on big data . The proposed technique is based upon three basic concepts of bilinear pairing, quadratic residue and lattices. Attribute-Based Encryption is a modified version of Identity-Based Encryption, that considers set of attributes rather than identities. The authors stated that, their scheme is an enhanced access control scheme in order to calculate cipher text for group of users. The group of users is included under one common access structure. The concept of bilinear pairing is more frequently used for ABE. The researchers' above said technique works by quadratic residue and attribute integration. The whole concept can be categorized under a common category of fundamental arithmetic theorem. The major advantage of this scheme is that, it discards unauthorized user access in case of a squared value.

[13] presented access control reinforcement for searchable encryption scheme and termed it as SE-ACAS technique. Their prime objective was to improvise the access control of data. This is a merged mechanism involving both searchable encryption along with access control techniques. This above said method achieves confidentiality both from cloud and user perspective. It also

restricts data access for unauthorized users. In terms of ACAS properties, the hybrid approach is more prone to attacks. In order to overcome this drawback, the authors added a secure filter to the client site. The researchers merged the ideas of SSE-1 and KP-ABE schemes. The method has some advantages, those are:- multi-users access control, confidentiality, preservation of ACAS properties. The researchers evaluated the performance according to search strategy and indexing strategy. They also stated that, indexation time is directly proportional to the collection size. In other words on increasing indexation time, collection size also expands. The above said search time does not depend upon the volume.

[14] developed a new modified version of CP-ABE approach based on searchable strategy . Their technique depends on partly hidden access structure along with attribute revocation. The authors considered DBDH and DL assumption for enhancing security of their method. It also supports lazy proxy re-encryption. Multi-valued attribute helps to hide users' information through the access structure. Flexibility of this technique is improved significantly and remarkably. Future research may involve including anonymous decentralized multi-authority scheme in order to add improvisation. Besides this safety, generality, efficiency and performance can be increased on providing further efforts.

3. Proposed Model

The proposed model in the present work considers large wireless sensor network architecture. The nodes are dynamic and distributed over the large area. In this model, wireless nodes communicate with each other node using unicasting mode. In our model, we assume each node in the dynamic network has a neighbor list with location, unique-id, data, credentials. The main objective of this model is to authenticate security and integrity to each node during data communication. The entire model is presented in two phases – sender side data encryption with integrity embedding phase and receiver side data decryption with integrity verification phase.

3.1 Sender Side Data Encryption With Integrity Embedding Phase

In this phase, each node in the communication network encrypts the data with integrity computation as data security and authentication process. The basic workflow of this phase is shown in figure 2.

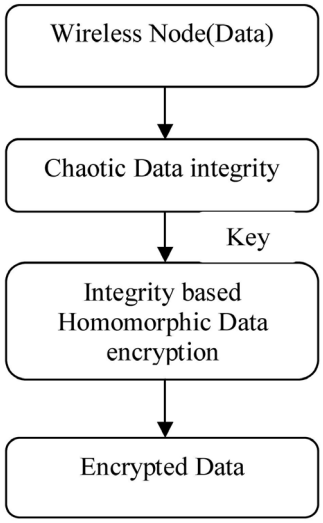

Figure 2. Proposed Integrity based Data encryption

The process of key generation increases the computation cost and it is responsible for decreased key strength and poor network dynamics. Hashing is an advanced cryptographic algorithm which is responsible for conversion of variable-length binary string to fixed-length. Therefore, hash-based encryption techniques are more efficient than that of traditional cryptographic algorithms in terms of resource usage and computational cost. In this phase, a novel chaotic hash model is used to generate a dynamic 512, 1024 bit hash code as encryption key. In the wireless communication, each node performs integrity and encryption and sends the encrypted data to the destination node. As data are encrypted in source node and decrypted in destination node, the cluster head is only allowed to pick and combine data from the member nodes without decrypting those.

Node Chaotic Integrity Algorithm:

Input: M(Node data), Secret key, initialization parameters.

Step 1: Read wireless node ID and Data D as M .

$$M = \text{Node(ID)} + \text{Data(D)}$$

If message size is not multiple of '*n*' then

Append the bit sequence 1000…000 at the end of the message.

Step 2: Divide the message into blocks of length *n* as $B_1, B_2,...B_n$.

Step 3: After padding, each block is again divided into '*m*' sub-blocks, each with 32-bit length and it is represented as $P_1, P_2,...P_m$.

Step 4: Secret key is generated using the wireless node's id and the random function as $S = Node(id) + Random()$. Generated secret key is initialized as X_0 for multi-chaotic system.

Step 5: Extended multi-chaotic system with one of the dynamic chaotic map function i.e Controlled Chebyshev Chaotic Map as:

Let *n* be a real integer *x* from the set *G* onto *G* such that,

$$T_n(x) : G -> G : [-1,1] -> [-1,1]$$

$$T_n = k\cos(n.\cos^{-1} x) \quad (1)$$

The recurrence relation to the equation (1) is given as

$$T_n(v) = (vT_{n-1}(v) - T_{n-2}(v)) / k \text{ and}$$

$$T_0(v) = k, T_1(v) = kv.$$

Step 6: In each round function, iterative multi-chaotic system generates output X_i to the transformation box as:

$$X_i = C_1 \oplus C_2 \oplus C_3$$

Step 7: In the transformation box, the following operations are performed on the Y and chaotic output.

$$Y = \lfloor 256X \rfloor$$
$$P'_i = P_i \oplus Y \oplus X_i$$
$$\text{Permute}(P'_i)$$

Step 8: Generates Hash value as

$$H_i = \text{Permute}(P'_i)$$
$$\text{Hash } H = H_1 + H_2 + H_3....H_m$$

Generated hash *H* is used as the key for the proposed homomorphic encryption model.

Integrity based Node Encryption Model

Setup: This phase setup public key parameters of the sender using the cyclic group generators, random number generator and generated hash value H.

Each node is associated with secret key and it will be generated using three pattern keys as

$$Key := \{key\ H, g, G_g, \alpha\}$$

Key recovery:= {*Nodelist, H, g,* G_g, α}; known to T.A

Node data Encryption Process:
Input: {Node key H, Neighbor list, Node data};

Encryption algorithm encrypts the node data using key and security credentials. In this encryption process, two methods are implemented for encryption and decryption i.e Additive and Multiplicative homomorphism. Additive and Multiplicative homomorphism are used to transform the input byte values into complex structure. Split node data D into two bytes as B_1, B_2 recursively for additive homomorphic encryption and multiplicative homomorphic encryption.

Additive Homomorphic Encryption is computed as

$$EncN(B_1 + B_2) = EncN(B_1) + EncN(B_2);$$

Multiplicative Homomorphic Encryption is computed as

$$EncN(B_1 . B_2) = EncN(B_1) . EncN(B_2);$$

Let $n = \alpha * \beta$; where α, β are cyclic group generators with key *H*.

$$\gamma = g^{B_1} B_2^{\,n} \bmod(n^2)$$

$EncN(B_1) := EncN(B_1) = (B_1 + \gamma * \beta)\ mod\ n$

$EncN(B_2) := EncN(B_2) = (B_2 + \gamma * \beta)\ mod\ n$

$EncN(B_1 + B_2) = EncN(B_1) + EncN(B_2)$

$EncN(B_1 + B_2) := (B_1 + \gamma * \beta)\ mod\ n + (B_2 + \gamma * \beta)\ mod\ n$

$EncN(B_1 . B_2) = EncN(B_1) . EncN(B_2)$

$= (B_1 + \gamma * \beta)\ mod\ (n) + (B_2 + \gamma * \beta)\ mod\ n$

Cipher Text CT

{

$\alpha, \beta, \gamma,$ H, $EncN(B_1 + B_2) = EncN(B_1 . B_2)$

};

This CT will be decrypted only those wireless node who has exact matching credentials as authorization.

Node Data Decryption Process:
Input(Cipher Text CT, Secret Key):

Cipher Text CT

{

$\alpha, \beta, \gamma,$ H, $EncN(B_1 + B_2) = EncN(B_1 . B_2)$

};

$$\psi(B_1) := EncN(B_1) = EncN(B_1) = (B_1 + \gamma * \beta) \bmod n$$

$$\psi(B_2) := EncN(B_2) = EncN(B_2) = (B_2 + \gamma * \beta) \bmod n$$

$$EncN(B_1 + B_2) = EncN(B_1) + EncN(B_2);$$

$$EncN(B_1 + B_2) := (B_1 + \gamma * \beta) \bmod (n) + (B_2 + \gamma * \beta) \bmod n$$

$$EncN(B_1 . B_2) = EncN(B_1) . EncN(B_2)$$

$$:= (B_1 + \gamma * \beta) \bmod (n) . (B_2 + \gamma * \beta) \bmod n$$

$$DecN(EncD(I_1 + I_2)) := (EncN\psi(B_1) + \psi(B_2)) \bmod \alpha$$

$$:= ((\psi(B_1) + \gamma * \beta) \bmod n + (\psi(B_2) + \gamma * \beta) \bmod n) \bmod \alpha$$

$$:= B_1 + B_2 \quad (1)$$

$$DecN(EncD(I_1 . I_2)) := (EncN\psi(B_1) . \psi(B_2)) := EncN(\psi(B_1) . EncN(\psi(B_2)) \bmod \alpha;$$

$$:= ((\psi(B_1) + \gamma * \beta) \bmod n . (\psi(B_2) + \gamma * \beta) \bmod n) \bmod \alpha$$

$$:= B_1 . B_2 \quad (2)$$

Solving eq-(1) and eq (2) we will get B_1 and B_2.

In encryption process, encrypted data along with credentials are sent to the receiver node. Receiver runs the same algorithm in reverse order to decrypt the data using the cipher text and the key. It the receiver node matches the integrity with the sender's integrity then the authentication process is successful otherwise it fails and resends its ACK to the sender.

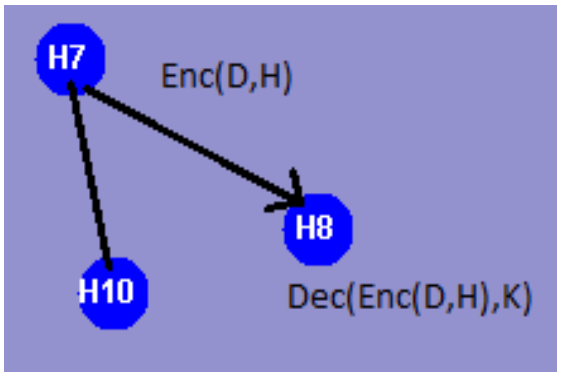

Figure 3. Node to node communication in secured way

For instance, source node H7 communicates with the destination node H8 as shown in Figure 3. Here node H7 sends the encrypted data which contains the integrity value H and the node data D to node H8.

4. Performance Analysis

4.1 Security Resistance in the Proposed Model

1) HELLO Flood Attack

Here, the attackers send HELLO packet in order to compel the server using its resources. According to our approach, the sensor nodes are responsible to receive and send data to the cluster head dynamically. The whole data flow of the network is monitored and saved at the base station. The base station directs every node to communicate, only after the successful authentication of that specific node. Our proposed technique is secure from Hello Flood attack. Additionally, our technique is also immune to Selective Forwarding attack.

2) Denial-of-Service Attack

Denial-Of-Service attack aims to block the network service to some specific nodes. Attackers send packets to occupy the network bandwidth, which restricts the user accessing the network at that time. This issue can be resolved through some changes in the traditional approaches, those are:- 1) The cluster head must be changed dynamically, after completion of every transmission. 2) A log must be maintained at the cluster head storing all details of member nodes.

3) Compromised Cluster Head Attack

This type of attack occurs, when an attacker combines data out of all cluster nodes by pretending as cluster head. The attacker thoroughly analyses data and retrieves his required information out of those. According to our presented approach, cluster head transmits data in encrypted format from cluster nodes and base station. No decryption occurs at this phase of transmission. Additionally, our proposed encryption scheme contains node location, round index and the distance among node-cluster head. This adds extended security to WSNs applications, as the attacker needs to know the entire network operations along with the whole network topology. Therefore, it becomes much difficult to break this security.

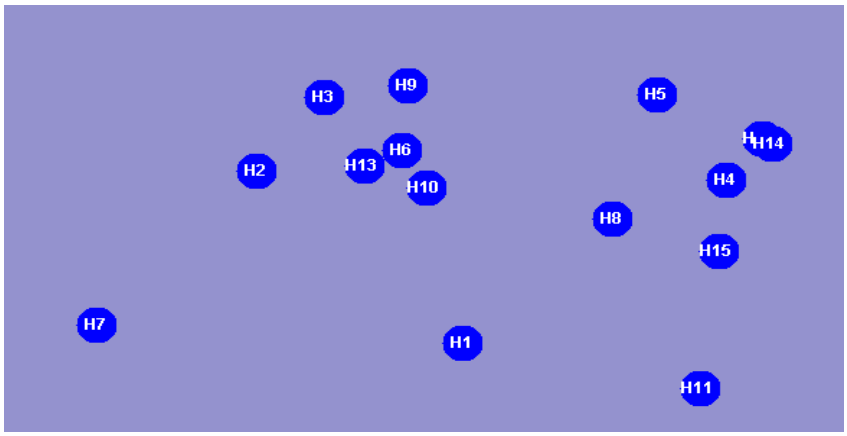

Figure 4. Wireless nodes simulation

Figure 4 describes the initialization of wireless sensor nodes in the dynamic network. Initially, 15 wireless nodes are initialized for data communication.

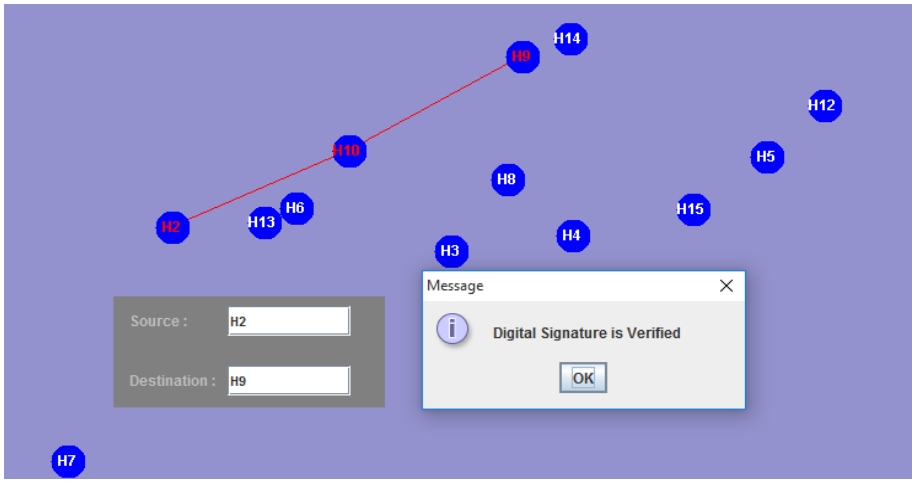

Figure 5. Node authentication verification from node 2 to node 9

Figure 5, describes the data communication between Node 2 to Node 9. A source node 2 encrypts the data and sends its credentials to the receiver node 9. Node 9 verifies its credential signature and then decrypts the data.

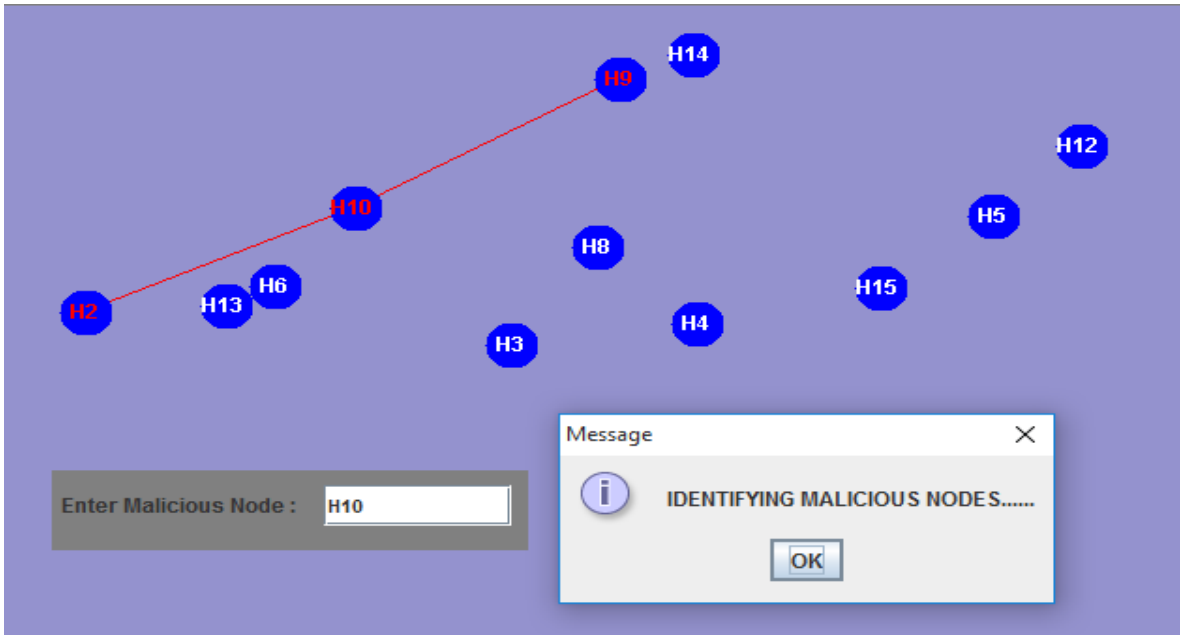

Figure 6. Detecting malicious node in the wireless network

Figure 6 represents the malicious node detection procedure. As shown in the figure, Node 10 enters into the network as a malicious node. During the data communication, each node has to prove its authentication to decrypt the data. Here, Node 10 fails to decrypt the data due to incorrect integrity verification.

Nodes	MD5 Based Scheme	Linear Chaotic	Proposed Integrity algorithm
10	0.897	0.8763	0.987
20	0.823	0.8953	0.997
30	0.819	0.9134	0.9839
40	0.854	0.9593	0.9964
50	0.831	0.9593	0.9897

Table 1. The performance of proposed model and the traditional model in terms of Integrity verification accuracy

Table 1 describes the accuracy of the integrity verification during the authentication process. From the table, it is clear that proposed model has a high rate of accuracy for malicious node detection during the authentication process.

5. Conclusion

In this paper, we proposed a novel integrity based secured authentication model for wireless sensor networks. Our model effectively authenticates the security defense against malicious attacks in WSN by implementing neighbor node integrity

Datasize(bytes)	MD5+ABE	MD5+KPABE	MD5+CPABE	MD5+ECC	ProposedModel
#500	7938	5938	5892	5636	5032
#1000	12443	10498	9893	10354	9935
#1500	19386	19758	18967	17958	16975
#2000	26884	25976	24976	22976	19758
#2500	37333	36977	34532	32976	29758

Table 2. Performance analysis of Average authentication time of proposed model with the traditional models

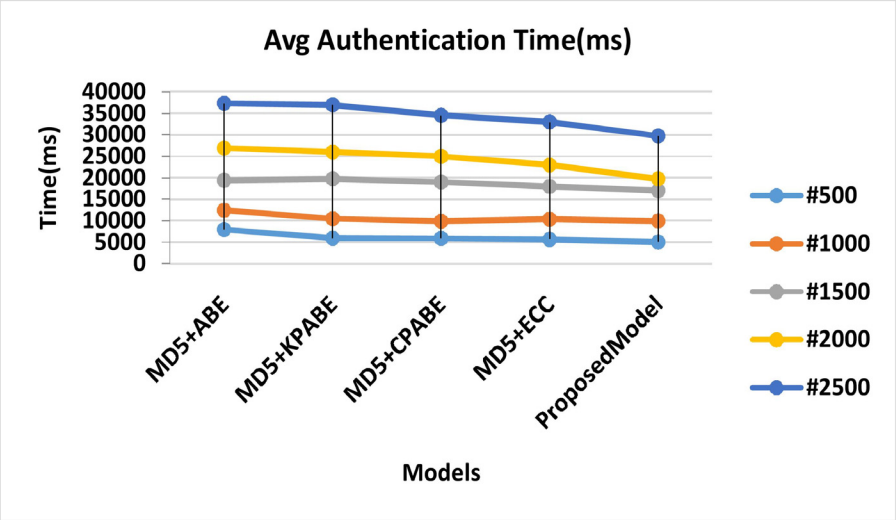

Figure 7. Performance analysis of Average authentication time of proposed model with the traditional models

verification process between the communication nodes. The entire model is presented in two phases – sender side data encryption with integrity embedding phase and receiver side data decryption with integrity verification phase. The performance of the proposed model is also evaluated in terms of attacks detection accuracy and average authentication time. Experimental results proved that the proposed authentication model has low communication cost and low storage overhead compared to traditional authentication models. In future, this model may be improved to integrate a new security parameter to the integrity and security authentication to create a more security solution for dynamic WSN environments.

References

[1] Yang, F. Y., Jan, J. K. (2004).An enhanced and secure protocol for authenticated key exchange", http://eprint .iacr.org/2004 / 270.

[2] Yiu, S., Terry, T., Colin, B. (2003). Provably Secure Mobile Key Exchange: Applying the Canetti-Krawczyk Approach, ACISP'2003, Berlin, Heidelberg: Springer-Verlag, p. 166–179.

[3] Kim, M., Jo, H., Kim, S., Won, D. (2009). Security weakness in a provable secure authentication protocol given forward secure session key, ser. Lecture Notes in Computer Science, 5593, p. 204–211.

[4] Chang, C. C, Le, H. D. (2016). A provably secure, efficient and flexible authentication scheme for ad hoc wireless sensor networks. *IEEE Transactions on Wireless Communications*, 15 (1) 357–366.

[5] He, D., Zeadally, S., Kumar, N., Lee, J. H. (2016). Anonymous Authentication for Wireless Body Area Networks With Provable

Security. *IEEE Systems Journal*.

[6] He, D., Kumar, N., Shen, H., Lee, J. H. (2016). One-to-many Authentication for Access Control in Mobile Pay-TV Systems. *Science China-Information Sciences* 59 (5) 1–14.

[7] Huyen, N. T. T., Jo, M., Nguyen, T. D., Huh, E. N. (2012). A beneficial analysis of deployment knowledge for key distribution in wireless sensor networks. *Security and Communication Networks*; 5 (5) 485–495.

[8] Das, A. K. (2016). A secure and robust temporal credential based three-factor user authentication scheme for wireless sensor networks. *Peer-to-peer Networking and Applications*; 9 (1) 223–244.

[9] Jiang, Q., Ma, J., Lu, X., Tian, Y. (2015). An efficient two-factor user authentication scheme with unlink ability for wireless sensor networks. *Peer-to-peer Networking and Applications*; 8 (6) 1070–1081.

[10] Chandrasekaran, B., Balakrishnan, R. (2016). Attribute Based Encryption Using Quadratic Residue for the Big Data in Cloud Environment, *In*: *Proceedings of the International Conference on Informatics and Analytics. ACM*.

[11] Kaci, A., Bouabana-Tebibel, T. (2014). Access Control Reinforcement over Searchable Encryption, IEEE IRI 2014, August 13-15, 2014, San Francisco, California, USA, p.130-137.

[12] Li, J., Shi, Y., Zhang, Y. (2015). Searchable cipher text-policy attribute-based encryption with revocation in cloud storage, *International Journal Of Communication Systems International Joirnal of Communication System*.

[13] Li, L., Chen, X., Jiang, H. (2016). P-CP-ABE: Parallelizing Cipher text-Policy Attribute-Based Encryption for Clouds, *In*:17th IEEE/ACIS International Conference on. IEEE, p.1-6.

[14] Wang, S., Zhou, J., Liu, J. K., Yu, J., Chen, J., Xie, W. (2016). "An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing, *IEEE Transactions on Information Forensics and Security* 11 (6) 1265-1277.