SECURE TRANSMISSION OF DATA BETWEEN NODES AND GATEWAY IN INTERNET OF THINGS

Dr. Nasreen Fathima Associate Professor, Department of Computer Science and Engineering, ATME College of Engineering, Mysuru, (Affiliated to Visvesvaraya Technological University, Belagavi)
M S Sunitha Patel Assistant Professor, Department of Computer Science and Engineering, ATME College of Engineering, Mysuru, (Affiliated to Visvesvaraya Technological University, Belagavi)

Abstract

The core idea behind developing 'Internet-of-Things (IoT)' applications- is to serve humanity with a better quality of life. It is realized that wireless technologies are the key-enabler for actualizing the underlying fundamental propositions of IoT in reality. However, different applications in the IoT ecosystem aim to provide higher degree connectivity among users with faster execution workflow considering future generation digital cellular communication standards. Despite having potential strength factors, the exploration is still active in investigating the scope of implementation towards ensuring better security management in a complex communication environment like IoT. The proposed research study uses an experimental approach for securing the transmission between communicating IoT devices (I-Node) and Gateway/Internet host (I-Host) in IoT eco-system. The framework modeling adopts a numerical implementation approach to design and represent the system's entire building blocks.

Keywords: Secure data Transmission, Digital Signature, Encryption, Sensors.

Introduction

As IoT eco-system envisioned to include diverse forms of application areas[1][10] and incorporation of promising cutting-edge technologies, the development of robust security schema that can cope with dynamic traffic scenario and user demands in IoT is essential. If the research trend from the past decade is observed, then it can be seen that the approach taken into consideration of the majority of the existing technique lacks efficiency either with respect to computation or communication[2][3][4][5].

Statement of the Problem

There exist several problems which are explored from the conventional literature and briefed as follows:

i. The existing trend of security protocol mostly adopts complex mathematical cryptographic techniques. One of the most popular and frequently adopted techniques is elliptical curve cryptography (ECC), which has higher routing dependency[12][13] and can result in a communication burden. The excessive generation of prime fields in ECC leads to computational inefficiency, which negatively influences the overall communication performance, which has not been extensively reported.

ii. Very few approaches are found in the recent past that have incorporated digital signature schema for authenticating/verifying the digital message stream from I-Node.

iii. Security threats for key-based attacks[21] and analysis have also not been extensively carried out. It is also observed that implications of iterative security approaches generate resource consumption overhead while applied to the routing and data aggregation phase in IoT[23].

iv. Incorporation of a combined digital signature approach with public-key cryptography has been less likely explored towards authenticating I-Node digital data[24][25][26].

v. Conventional security approaches do not consider dynamic scenarios where I-Node mobility can take place with respect to the time and implications of key-based attacks. The behavioral analysis of security approaches is not much concerned against new forms of adversaries considering key and signature-based security schema.

Objectives of the study

Thereby the proposed system aim to

- To design a robust security framework capable of offering privacy preservation of data.
- Joint management of key-based approach and signature scheme for IoT.
- Maintaining a balanced performance between resource consumption and non-iterative execution workflow modeling of public-key encryption.

Review of Literature

Existing researchers have presented various approaches in order to offer a security solution towards various vulnerable situations in IoT. Software-Defined Network is proven to contribute extended security solution over an IoT as witnessed in work carried out by Liu et al. [6]. The authors have presented a mechanism to transmit data securely using an undirected graph. Existing literature has also used attribute-based encryption towards security, as seen in the work of Ambrosin et al. [7]. Ciphering the application-based data is found to offer a reduction of complexity when it is compared to the existing DTLS scheme, as seen in the work of Ban et al. [8]. The work of Kumarage et al. [9] has carried out investigation towards linking security with mining of data.

The vulnerability of the physical layer due to issues of eavesdropping can be resisted using a distinct relay strategy using multi-hop, as claimed in the work of Xu et al. [19]. Yalcin et al. [18] have used elliptical curve cryptography for offering security using a synthesis approach. The existing system has also witnessed the usage of encryption and manipulation of data towards strengthening the security system of an IoT, as seen in the work of Schurgot et al.[11]. Usages of probability theory, as well as transformation-based approaches, are proven to offer better control of eavesdropping issues in an IoT. Existing solutions towards resisting threat has been constructed using threat mapping model. A better security solution has been offered using secret keys of smaller sizes, which can withhold the computational complexity as witnessed in the work of Premnath and Hass [16]. The solution presented by Porambage et al. [17] has used the group key using a hash function where the security is further strengthened by using a digital signature. The existing system has also discussed the usage of trust management by Mendoza & Kleinschmidt [18]; however, the study emphasized stopping one kind of attack. The influence of data dropping attack is studied by Li et al. [19] considering a different form of security issues in a wireless network. Apart from stopping adversaries, there are also study carried out towards controlling the overhead of security as briefed in the work of Kim et al. [20]. The existing system has also reported of various approaches contributing towards strengthening security system in IoT (Hou & Yeh [21], Dong et al. [22], Chi et al. [24]), Elliptical curve cryptography, attack-specific solution (Zhang et al. [15]), accomplishing interoperation . Hence, there are different forms of solutions towards boosting the security strength of IoT. In reality, all these solutions are applicable when the research work is carried out in a similar environment, and they are in much recent state of research. At present, there is no specific standard claimed to offer efficient security that is demanded in the IoT environment.

Proposed System Design and Analysis

The prime aim of the system design and modeling is to represent a computing system for IoT security which can be defined as a function Y ←f(x,y) where x and y are different input operational parameters. The system design modeling for the security framework design adopts public-key cryptography, and the prime reason behind this is that public-key cryptography offers optimal supportability among a set of I-Node. The system representation initially considers a set of IoT sensor nodes, which is denoted with I-Node. Also, it has considered a set of I-Host, which are often referred to as an Internet host. Here the system modeling applies a clustering paradigm with dynamic I-Nodes where it subsequently communicates with I-Host of IoT with the progressive communication cycle. The proposed work's prime objective is to attain the privacy preservation of digital data in terms of both confidentiality and integrity. For this purpose, only the captured data by I-Node undergoes through signature and key-based data authentication schema and is subjected to the ciphering process. The encrypted data in the subsequent stages of routing and communication will be forwarded from I-Node → I-Host. The numerical modeling associated with the proposed system design consists of algorithm execution procedures to accomplish novel public-key cryptography to attain data integrity. The system's design phase introduces two different layers of security protocols, such as 1) Security Protocol-1 and 2) Security Protocol -2. The architectural overview of the designed framework is represented as in Figure 1.

As shown in Figure 1, the entire framework consists of two different protocols for data authentication and integrity validation through a different set of security parameters. Here the security system related to protocol-1 implements a novel approach of light-weight public-key cryptography where the msg which get transmitted between I-Node and I-Host undergoes through a ciphering process considering joint management of digital signature and key-based encryption schema[23][26]. It is numerically modeled keeping the resource constraints into consideration, i.e., the execution workflow of the security protocol in I-Node should not consume more resources which makes the system vulnerable as over- utilized resources can lead to higher energy consumption and adversary can take advantage of that situation and can mislead the flow of transmitted msg.

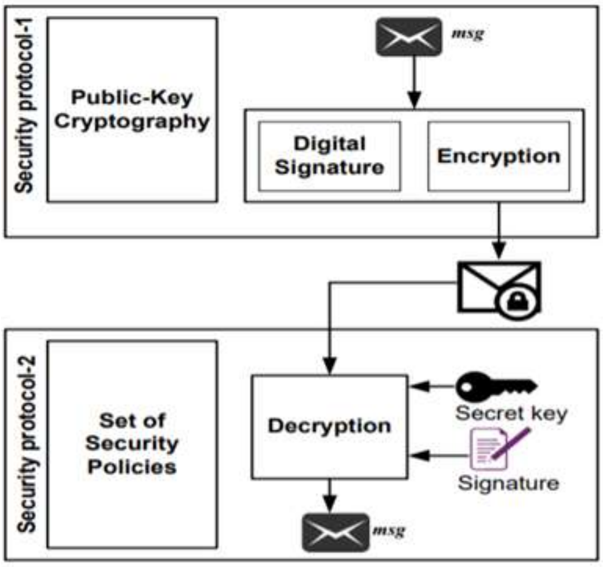

Figure 1 Architectural overview of the overall framework modeling

In the long run, it also affects communication performance with the heavier computational burden. The rule set corresponding to security protocol-2 is meant for secret key computation and signature verification to validate the integrity of the msg. This computational operation of decryption takes place at the receiver node, which here refers to I-Host, the gateway node in IoT.

The core idea behind the system's implementation strategy is to formulate secure communication between I-Node and I-Host with a cluster formation and grouping structure of node and I-Host deployment. Here, each I-Node is considered dynamic means each node will have mobility and can change clusters at any point in time, making the entire IoT communication scenario dynamic.

Set-up: Deployment of IoT sensor nodes for the construction of the network**.** During the IoT sensor node deployment process, the computation step initially performs node registration to accumulate a few significant attributes. This includes sensor node type (T1 | T2) in terms of computational capabilities along with that it also assesses initial location coordinates (Lc []).

In this computation phase, the system initializes a set of network parameters for n number of IoT sensor nodes **(nSIoT).** The parameters include simulation area α (1×1), T_1 (1×1), T_2 (1×1), number of IoT gateway systems **(nG$_{IoT}$).**

The computation for localization of each IoT sensor node is considered in a way where it ensures that every T1 and T2 node get placed within the vicinity of α (1×1). The system analytically modeled in a way where the IoT-based sensor network construction takes place in a random pattern of heterogeneous deployment mode. The randomization of T1 provides a new matrix r (T1) which can be shown as follows.

$$|\vec{r}(T_1)| = \begin{bmatrix} T_1(1,1) \\ T_1(2,1) \\ T_1(3,1) \\ . \\ . \\ . \\ T_1(nS_{IoT},1) \end{bmatrix}(nS_{IoT} \times 1)$$

After the computation of r(T1), the process also incorporates a variable called β to deploy IoT sensor nodes as uniform as possible for different sub-regions. To compute the x coordinate for each SIoT, the following mathematical expression is modeled.

$$\text{x(i)} = \sum_{i=1}^{nS_{IoT}} \beta + (\alpha - 2 \times \beta) \times r(T_1(i)) \quad \text{...eq. (.1)}$$

The computation of eq. (1) provides a matrix x(i) that stores all the x coordinates of respective SIoT. The matrix structure of x(i) is as follows:

$$\text{x(i)} = \begin{bmatrix} x(1,1) \\ x(2,1) \\ x(3,1) \\ . \\ . \\ . \\ x(nS_{IoT},1) \end{bmatrix}(nS_{IoT} \times 1)$$

Similarly, the computation assesses y(i), which stands for the matrix, that holds the numerical value corresponding to the y coordinate of each SIoT. The mathematical expression to do this is as follows:

$$\text{y(i)} = \sum_{i=1}^{nS_{IoT}} \beta + (\alpha - 2 \times \beta) \times r(T_1(i)) \quad \text{...eq.(2)}$$

The computed column vector of y(i) can be represented as follows:

$$\text{y(i)} = \begin{bmatrix} y(1,1) \\ y(2,1) \\ y(3,1) \\ . \\ . \\ . \\ y(nS_{IoT},1) \end{bmatrix}(nS_{IoT} \times 1)$$

Finally, the system generates a random pattern of orientation for constructing the IoT based sensor network. Figure 2 exhibits the overall network overview for a set of nodes.

Here, the IoT gateway's role is to aggregate and accumulate the sensor-generated information and further process the data towards the Internet and cloud computing systems. Here T1 indicates the type of SIoT which are having higher computing capabilities as compared to T2.

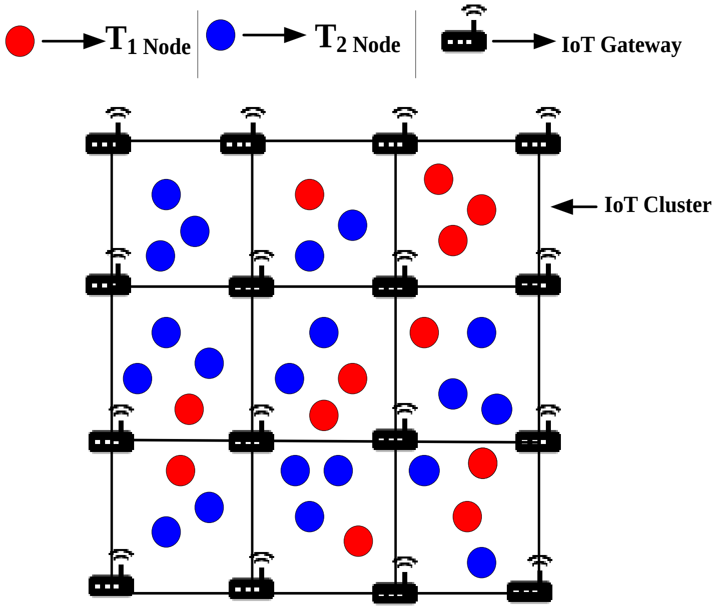

Figure 2 IoT Sensor Node Deployment Scenario

Incorporation of Layer-1 Security: Obtaining system parameters

In this level of security modeling, the IoT gateway plays a very crucial role. It generates system parameters based on k bit prime number Ɛ.

Incorporation of Layer-1 Security: Defining security attributes

The IoT gateway in this phase of computation initially defines a set of security attributes such as Δ_1, Δ_2, Δ_3, Δ_4. The IoT gateway also initializes a secret gateway key, which is denoted with **$G_{Secret\text{-}Key}$.** Further, the system computes public key attributes **(Pub_{key})** by executing the following mathematical expression.

$$Pub_{key}\,(1\times1) = G_{Secret\text{-}Key}\,(1\times1) \times \Delta_4\,(1\times1) \quad \ldots eq.(3)$$

Incorporation of Layer-1 Security

Formulated Encoder and its Design Specification from an analytical viewpoint. To design encoding attributes E = {E_0, E_1, E_2, E_3} the system has derived 4 different mathematical equations using the above-highlighted security attributes which are as follows:

$$E_0\,(1\times1) \leftarrow r(1\times1) \times \Delta_3^2 \quad \ldots eq.\ (4)$$

$$E_1(1\times1) \leftarrow \Delta_3^3 \times r(1\times1) \times \Delta_3 \quad \ldots eq.\ (5)$$

$$E_2\,(1\times1)\,,\, E_3(1\times) \leftarrow \Delta_3 \times r(1\times1) \times \Delta_3 \times r(1\times1) \times \Delta_3 \times r(1\times1) \times \Delta_3 \quad \ldots eq.(6)$$

Incorporation of Layer-1 Security:

Concatenation of secret parameters Finally, the IoT gateway system concatenates all the secret parameters and stores into a matrix as C_{SP}[] for the future set of task evaluation.

Generation of Secret Key

This computation takes place in the IoT gateway system where initially, two different row vectors are generated, such as idx(T_1) and idx(T_2), which are basically index of type-1 and type-2 nodes.

$$\text{Here idx}(T_1) = [t_1(1,1)\,,\, t_1(1,2)\ \ldots\ldots\ldots\ldots t_1(1,T_1)]_{(1\times T1)}$$

$$\text{And idx}(T_2) = [t_2(1,1)\,,\, t_2(1,2)\ \ldots\ldots\ldots\ldots t_2(1,T_1)]_{(1\times T2)}$$

Now the total number of deployed IoT sensor nodes can be computed with the following derived eq. (7)

$$nS_{IoT} = \sum_{i=1}^{n} T_1 + T_2 + \ldots\ldots\ldots + T_n \quad \ldots eq.(7)$$

In further steps, each of the nodes can have a provision to select and choose a specific secret key attribute **(S_k1),** which is computed by executing the eq. 8 and 9.

$$S_{k1} \leftarrow 1 + \Omega \times r(T_1) \text{ ...eq.(8)}$$

Eq. 8 implies that in this level of secret key computation, the values are considered between 1 to (Ω+1). The randomized pattern of computation in each execution generates a new set of values by assessing the function **r(T₁).** Eq. 9 further computes another level of the secret key, i.e., S_{k2}

$$S_{k2} \leftarrow S_{k1} \times \Delta_4 \text{ ...eq.(9)}$$

The trusted authority component **(TAC),** which belongs to the IoT gateway system in this phase, determines another variable of security key attribute S_{k3}. The computation happens by executing the above-mentioned eq. 8. As it incorporates random r() function, therefore the values are newly generated and stored into S_{k3}.

The system further initializes the generation of partial public and private keys, which are denoted as P_{pp}, P_{pk}.

$$S_{k4} \leftarrow S_{k3} \times \Delta_4 \quad \text{...eq.(10)}$$

$$S_{k5} \leftarrow S_{k3} + mod(A, \varepsilon) \text{ ...eq.(4.11)}$$

$$\text{where } A = (S_{k1} \times E_0 \times (idx(T_1) + S_{k4} + S_{k2})$$

- **Computation of private key (pK):** It employs transpose operation over the elements of S_{k5} attributes along with S_{k1}, Further these two components are stored into a matrix form of **pK ←** **[** S_{k5}' || S_{k1}'].

$$\mathbf{pK} = \begin{bmatrix} pK_{1,1} & pK_{1,2} \\ pK_{2,1} & pK_{2,2} \\ pK_{3,1} & pK_{3,2} \\ . & . \\ . & . \\ pK_{T_1,1} & pK_{T_1,2} \end{bmatrix} (T_1 \times 2)$$

- **Computation of public key (pubK):** Similarly **pubK** get computed by transposing and concatenating S_{k2}' and S_{k4}', This notion of computation is numerically represented as: **pubK ←** [S_{k2}' || S_{k4}']

$$\mathbf{pubK} = \begin{bmatrix} pubK_{1,1} & pubK_{1,2} \\ pubK_{2,1} & pubK_{2,2} \\ pubK_{3,1} & pubK_{3,2} \\ . & . \\ . & . \\ pubK_{T_1,1} & pubK_{T_1,2} \end{bmatrix} (T_1 \times 2)$$

After computation of private and public key components , the process further define communication range C_r for each IoT sensor node which is expressed with

$$C_r = \frac{\alpha\,(1 \times 1)}{\text{nGIoT}} \text{ ...eq.(11)}$$

The process is defined in a way where other IoT gateway system gathers all the information regarding its neighbor nodes, which consist of coordinates and distance vector d_v[].

Here the process initially extract coordinate of a particular IoT sensor node $S_{IoT}(x(i),y(i))$ and calculate the distance between $S_{IoT}(x(i),y(i))$ and other IoT sensor nodes. It incorporates the notion of Euclidian distance to compute the distance vector. The following eq. 12 exhibits the formula regarding Euclidian distance.

$$d_v(P_1.P_2) \leftarrow \sqrt{(p_1(x) - P_2(x))^2 + (P_1(y) - p_2(y))^2} \text{ ...eq.(12)}$$

The notion of the above eq. 4.12 is incorporated to find out the distance between one $S_{IoT}(x(i),y(i))$, and other IoT sensor nodes. The process also validates the C_r of each IoT sensor node and also ensures its neighbors if $d_v(P_1.P_2) \le C_r$. P_1 here indicates the coordinate of IoT sensor node 1 and P_2 here shows the coordinate of IoT sensor node 2. Then finally, it can be visualized as follows:

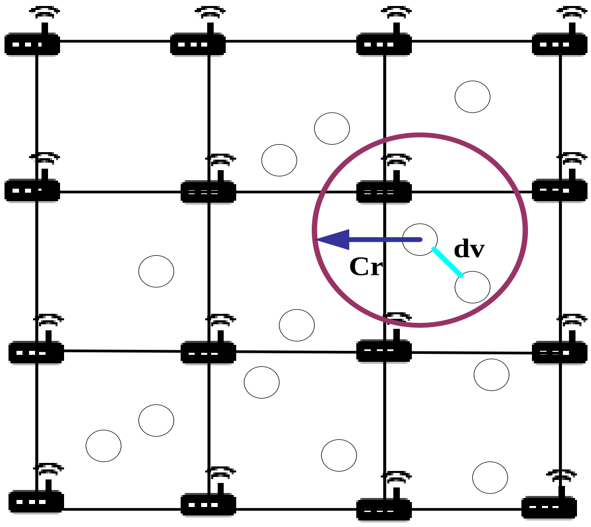

Figure 3 Defining communication range of each nodes w.r.t distance computation

Connectivity establishments among nodes: In this phase of the study, link establishment happens between two nodes where a node broadcasts an advertisement message to its eligible neighbors.

For each eligible neighbor node, the process initially creates a security variable $S_{k6} \leftarrow \Omega \times \Delta_4$, and then establish all possible links between the node to the eligible neighbors. The system creates a matrix named link$_{mat}$[], which stores all the information corresponding to the connection established between 1→ many nodes. Another security attribute called S_{k7} is computed with the following mathematical expression:

$$S_{k7} \leftarrow \Omega \times E_0 \times eligN \times \Delta_4 \times Pub_{key} + mod((\Omega \times eligN), \mathcal{E})) \quad \text{eq. 13}$$

here eligN is number of eligible nodes to perform communication

During the registration process, the IoT gateway systems share a public key certificate with all the eligible nodes authorized to communicate. Therefore using that public key certificate, each node generates its respective secret key attributes. Then finally, the S_{key} can be computed as:

$$S_{key} \leftarrow E_1 \times S_{k6} \times S_{k7} \times \Omega \times \Delta_4 \times eligN \; \ldots\text{eq.(14)}$$

Further, the sender node also computes the propagated signal (P_{signal}), the data (μ) attributes. It encapsulates it into a new variable Pkt = [P_{signal} μ], the final encapsulated packet can be formed as Pkt = [P_{signal} μ S_{k6}]. Finally, when the data packet reaches the destination IoT sensor node, then it de-capsulate it using the partial secret key $S_{k6} \in S_{key.}$

$$S_{k7} \leftarrow r(1,1) \times S_{k6}$$

Finally it computes the propagation signal as follows:

$$P_{signal} \leftarrow E_2 \times S_{k6} \times r(1,1) \times S_{k7} \times \alpha \times r(1,1) \times eligN \; \ldots\text{eq.(4.15)}$$

The system finally authenticates the data packet at the IoT gateway system using secret key pools, consisting of a set of copies of secret keys already distributed partially among the member nodes. During packet transmission from node to IoT gateway, the secret key is retained based on certain conditions. It is declared as an invalid secret key, and the privacy of the data preserver. Finally, the system implementation procedure proceeds to secure cluster construction within a dynamic scenario where for a specific number of simulation cycles, I-Node communicates with its respective group head that is I-Host.

Algorithm Implementation strategic Modeling

The algorithm in this phase of the study is numerically modeled to secure the data transmission between I-Node and I-Host considering a clustering mechanism in IoT systems dynamic applications. Here the above computation of secret key and digital signature-based pkt/msg verification is represented with simplified steps of execution modeling. The proposed study considers four different types of secret key attributes: i) non-indexed Skey, ii) I-Node sensor secret key, iii) Integrated key and iv) group/cluster key for msg authentication and authorization of I-Node. During the primary layer of implementation, the system considers best and optimal key generation processing in dynamic IoT applications considering public-key encryption. In the second layer of implementation, the system computes the digital signature based data authentication followed by the key establishment, construction, and distribution, considering the public key encryption strategy. Finally, in the third layer of security approach, the system performs intrusion detection and prevention to resist maximum possible threats that arise due to key-based attacks regardless of its strategic execution scenario. The system modeling and its core implementation modules offer a better solution approach to deal with any forms of key-based attacks that more likely occur during the data aggregation phase in IoT. The prime idea is to secure the communication between I-Node to I-GNode, which is a gateway or cluster head. Also, it should provide a higher layer of security between the communication of I-Node to I-Host. The following steps show how the algorithm is numerically modeled to carry out the dynamic IoT environment's execution process.

Framework Design Requirements

The overall framework design requirements consider two different types of I-Nodes, where 2 types of I-Node are defined considering computational characteristics. Here 1 type of I-Node is defined with maximum computational capability **(maxI-Node),** and another type of I-Node is defined with minimum computational capability that is **(minI-Node).** Thereby the total number of I-Node/ (nS_{IoT}) is the total summation of these two types of I-Node. Here the maxI-Node can become eligible for the superior node, which is also referred here as cluster-head/gateway (I-GNode). Here I-GNode and I-Node both can securely communicate with I-Host. Here one condition is followed by being a practical assumption that the number of I-GNode will be lesser as compared to the number of I-Node. Both the nodes within the IoT ecosystem are allocated with the unique identifier tags I-Node(tag). The key-management schema is designed in a way where the computed secret key **(S_{key})** is uniformly shared between I-Node. Here the final secret key computation takes place considering the computation of non-indexed S_{key}, which are computed considering eq. (4.12) and eq. (4.13) as shown in the previous section. The system also finds a group-key (gKey), which is allocated to the I-GNode only. The system also considers a joint key attribute during the data aggregation process.

The flow of the algorithm goes as follows, where in the first level of the execution flow, the system considers the secret key generation as already discussed above. The second layer of the security protocol further focuses on the generation of a novel digital signature attribute from the security viewpoint. Here the system maintains forward and backward secrecy to maintain the confidentiality of the data being exchanged between the I-Node and I-GNode and I-Host and vice-versa. Here the in the initial computational step, the system represented in the form of algorithm execution flow takes the number of I-Node and number of I-Host into consideration and generates S_{key} and signature ***(sig)*** after processing the execution pipeline. The system also defines 4 different types of security attributes where a1 represents a finite field, a2 represents the pattern of prime fields, a3 represents the monogenous group, and finally, a4 represents point generator.

Further, the system constructs encoder distinctly from the security attribute a3. Finally appending of these security attributes take place as SecA ← {a, E, pubK}. Further the steps of execution also incorporates computation of variant security parameters such as

i) selection of prime number,
ii) computing of the matrix corresponds to a tuple of security attribute,
iii) computation of I-Host secret key and
iv) Public key computation, respectively.

Here the based encoders are also utilized to compute the specific length of the symmetric key. Finally, I-Host computes all these entities to construct the *sig* considering all these key attributes for pkt authentication and verification purpose. Further, the system again computes private or secret key attributes and public key attributes. Here the private key computation takes place considering half of the pKey and pubKey attributes from the minI-Node. Finally, the system generates final sKey considering the encoder e0 along with a prime number. This sKey also gets allocated to the I-Host. After this process, the I-Host computes a distinct identity of the minI-Node and maxI-Node. During the communication process, all the I-Node computes confidential numerical values to compute the Skey. Finally, with the assistance of trusted authority, half of the Skey is validated through I-Host and shared by the I-Host to the minI-Node, and they validate the Skey and compute the full-length secret key. Once I-host completes the secret key generation process, then the system computes the matrix of legitimate I-Node and validates I-Node with respective node identity along with Skey. Finally, the algorithm computes a digital signature (*sig*) in a unique way where it computes 6 prime distinct entities. The function g(i) computes the signature with j where j is the prime number. Further, the weighted attribute val1 and cumulative hash function value val2 are compared to generate the Skey. Further proposed system also secure the beacon exchange between I-Node and I-GNode and I-GNode to I-Host.

Algorithm Design Strategy for key management, digital signature generation, and clustering

```
Input: Number(I-Node, I-Host)
Output: $S_{key}$ , sig
Start
1.  Initialize Number(I-Node, I-Host)
2.  For i ← 1 to I-Node/ ($nS_{IoT}$)
        a.  SimA ← rand(x,y)
        b.  Deploy: maxI-Node , min-I-Node , I-Host
        c.  Define security attribute: a ← [ a1 , a2, a3, a4]
        d.  Compute public key attributes pubK ← [$S_{k2}'$ || $S_{k4}'$]  //considering I-host  secret
            key and point generator a4
        e.  Construct encoders E = [e0 , e1 , e3, e4] ← func(a3)
        f.  SecA ← {a, E, pubK}
        g.  Compute key ← [pkey , pubKey]
        h.  Compute sig ← g(j)
                i.  If val1 = val2
                        1.  Obtain: key
                ii. End
        g. CH ← ArgMin(dist) , maxI-Node → id
3. End
End
```

The above algorithm steps clearly show how the proposed system accomplishes a joint secure key and digital signature-based pkt authentication to maintain the data's privacy in terms of both integrity and confidentiality. The system's numerical design and modeling clearly accomplish a cost-effective clustering of **I-Node**, where **I-GNode** is elected as **CH**. I-Node authentication also takes place during clustering where I-GNode is elected dynamically. I-Host validates the I-GNode and their respective data considering the Skey and its respective id. The system modeling justifies that it is robust against any types of key-based attacks in IoT, which is further validated with comparative analysis in the next section.

Experimental Results Produced from Extensive Numerical Analysis

The numerical analysis produced outcome with respect to two prime performance metrics such as

i. Energy consumption with respect to Pause Time and

ii. Energy Consumption with respect to Update Frequency where velocity **(vel)** of each I-Node ranges between 1 m/s to 16 m/s.

For the extensive analysis purpose, the framework design also considers a set of I-Host, which are considered 4, 9, 16, and 25. And also the stimulation parameters include a set of additional parameters which are listed in the following Table 1.

Table No.1: Simulation parameters and their respective numerical values for experimental/simulation purpose

Simulation parameters	Numerical values bunded with a range.	Numerical values considered: for test scenario(comparative)
Number of I-Node (sensors) for IoT	100-1000	100
Number of I-Host/Gateway	4, 9, 16, 25	16

UpdateFeq(val)	1 to 20 Hz	5 Hz
PauseTime(val)	0 to 1000 sec	500 sec
Number of the Simulation cycle	200 -800	200
Simulation area	(1000 × 1000) m^2	(1000 × 1000) m^2

Table 2 shows the numerical values of simulation parameters considered during the execution modeling of the security system in IoT. The numerical modeling of the formulated system is further simulated under the variable condition of network and communication constraints to understand the system's behavior where dynamic I-Node securely communicates with I-Host.

Table No.2: Analysis of Energy consumption metric for cluster key update

	Energy Consumption For Cluster Key Update				
Updated Frequency	**Vel = 1 m/s**	**Vel = 2m/s**	**Vel = 4/s**	**Vel = 8/s**	**Vel = 16/s**
0	1.212	1.904	3.044	4.892	8.632
2	1.236	1.876	2.976	4.676	8.424
4	1.268	1.784	2.864	4.448	3.98
6	1.228	1.824	2.796	3.364	3.112
8	1.2	1.72	2.528	2.572	2.444
10	1.168	1.708	1.996	2	2
12	1.12	1.62	1.968	1.832	1.648
14	1.156	1.48	1.6	1.6	1.6
16	1.088	1.436	1.596	1.484	1.364
18	1.068	1.16	1.2	1.2	1.2
20	1.024	1.16	1.2	1.2	1.2

Descriptive Statistics of the Data points	**Std**	**Var**	**Mean**
Vel = 1 m/s	0.0776	0.0060	1.1607
Vel = 2m/s	0.2659	0.0707	1.6065
Vel = 4/s	0.7086	0.5021	2.1607
Vel = 8/s	1.4366	2.0637	2.6607
Vel = 16/s	2.7523	7.5749	3.2367

The analysis of the energy consumption for cluster key update is performed with respect to two distinct metrics for comparison where UpdateFrequency increasing values are taken as independent values corresponds to an independent variable during the simulation and the impact of it on the energy performance of the system is measured for five different velocities of I-Node ranges between 1 m/s to 16 m/s. Here update frequency refers to the count of times the secret key Skey of the I-GNode is updated during the clustering process. Here I-Nodes are taken as vulnerable nodes from the security viewpoint. However, the analysis and descriptive statistics computation of these data points show that initial energy consumption is highest when vel is set to 16 m/s. In the case of 1m/s, it is initially found lowest. Still, eventually, for different velocity conditions, all the curves corresponding to energy consumption come closer, indicating a marginal difference in energy consumption performance, as shown in Figure 4.

Figure 4 visual outcome clearly shows that the key-management is effectively incorporated and well-managed with frequent updating process of the key with increasing values of update frequency whenever an I-Node joins or leaves the IoT ecosystem. This indicates that regardless of I-Node mobility, the system ensures better energy performance as it decreases with increasing values of Update Frequency. It leads to maximizing overall network lifetime with the maximized operation of algorithm execution for key update generation and sig-based msg authentication.

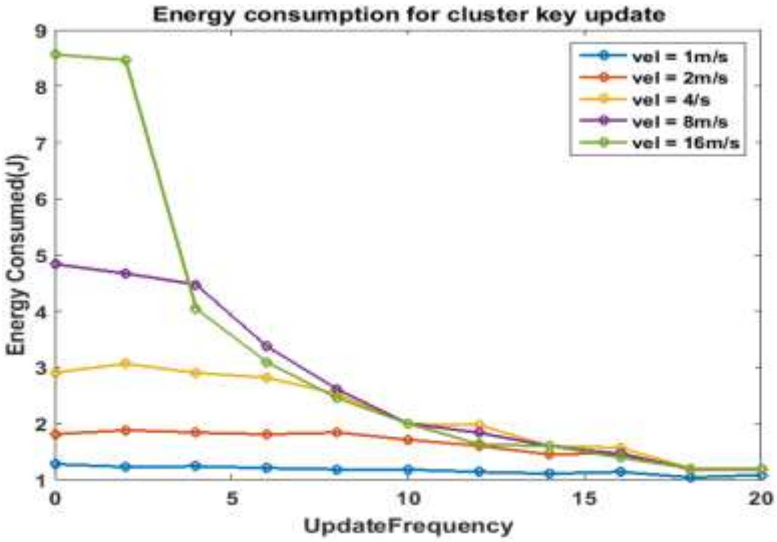

Figure 4. Energy consumption metric estimation with respect to UpdateFrequency

Table 3 also indicates another metric validation, i.e., energy consumption for the key establishment with respect to PauseTime. Here PauseTime or Wait Time refers to the time instance duration spent before discarding the secret key from I-Host when an I-Node leaves a cluster or group. The numerical analysis with respect to I-Node's increasing velocity shows that here also in every test instance, the energy performance is quite superior, and the energy consumption curve decreases with increasing velocity. The statistical inferencing from the above Table 3 also shows that from the computation of Standard deviation **(Std)** and variance **(Var)** it is quite clear that despite node mobility and dynamicity in IoT environment, the formulated approach attain better energy performance without compromising the data integrity and confidentiality and also protect data privacy from different forms of key-based attacks.

Table No.3: Analysis of Energy consumption metric for cluster key Establishment

	Energy Consumption For Key establishment				
Pause time	**Vel = 1 m/s**	**Vel = 2m/s**	**Vel = 4/s**	**Vel = 8/s**	**Vel = 16/s**
0	91.44	116	159.6	248.4	343.8
100	85.32	109	143.3	179.3	165.4
200	87.96	107.9	140.1	153	123.6
300	78.32	106.9	130	132.3	107
400	89.96	106.6	119	136.4	90.28
500	86.16	104.8	122.7	120.3	89.88
600	92.8	105	118	132.1	88.2

Descriptive Statistics Of the data points	**Std**	**Var**	**Mean**
Vel = 1 m/s	4.8418	23.4426	87.4229
Vel = 2m/s	3.8169	14.5690	108.0286
Vel = 4/s	15.2738	233.2895	133.2429
Vel = 8/s	44.4737	1.9779e+03	157.4000
Vel = 16/s	92.2782	8.5153e+03	144.0229

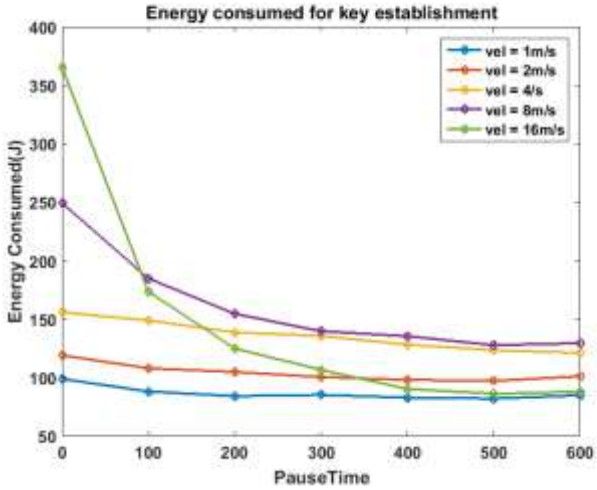

Figure 5. Energy consumption metric estimation with respect to PauseTime

The visual outcome of the energy consumption metric for the key establishment is also assessed considering the PauseTime. It is found that with increasing PauseTime, the curve corresponds to energy consumption decreases with respect to the variance of the velocity of I-Node. The overall performance analysis clearly shows that the proposed system not only ensures better energy performance but also ensures higher-level security due to effective joint management of key and signature-based data authentication. The study also performed a comparative theoretical analysis with similar studies of [12][13] and [14], which are highly cited in the past and also addressed similar problems with Elliptical Curve Cryptography. The following table shows the performance analysis comparison highlights.

Table No.4: Comparative Analysis from the theoretical viewpoint

Factors	**Proposed**	**Existing**
Key Generation	Finite Field	Elliptical Curve
Usage of Digital Signature	Simplified	Complex
Iterative	No	Yes
Resource Evaluation	Yes	No

The comparative analysis is made after analyzing the baseline technical manuscripts thoroughly. The outcome of the inference cumulatively shows that as compared to the existing system overall performance of the formulated approach is quite superior from both energy, security, and computational performance and also due to simplified steps of execution. The proposed system offers I-Node protection from different key-based attacks, and also it can be well-suited for other forms of attacks in the IoT environment. The processing time analysis also shows that the overall processing time in the proposed system is obtained as 0.35512 seconds for obtaining the security attributes, whereas in the case of an existing system where plain digital signature and an elliptical curve are used consumes approximate processing time of 3.76221 seconds. Hence, it is quite clear that the proposed system accomplishes better security performance by maintaining a good balance between communication and computation costs.

Conclusion

This study introduces a novel and robust security approach that adopts the potential features of public-key encryption and digital signature-based data authentication modeling. The uniqueness of the security policy is that it implicates the design and development of simple and cost-effective security solutions based on key attributes and authorizes data and I-Node with a progressive round of communication. Another uniqueness of the system is that it considers I-Node as a dynamic that can join and leave a cluster any time as in IoT; most of the nodes are sensor-driven and can have mobility. However, here I-Host is considered to be static. The key generation procedure is applied to generate a secret key attribute through which the msg transmitted from I-Node to I-Host via I-GNode should get adequately encrypted.

Moreover, while receiving the encrypted data, the I-Host applies digital signature-based verification to check the confidentiality and authority of the data. The experimental outcome with respect to distinct performance metrics shows that it accomplishes superior energy performance. The comparative analysis, in the end, shows that the formulated approach attain better security performance and attain significant computational efficiency due to its simplified approach and execution pipeline.

References

1. Amjad Gawanmeh, Sazia Parvin, Joel J. P. C. Rodrigues, Kashif Saleem (2019) "Smart Devices, Applications, and Protocols for the IoT", Engineering Science Reference.

2. Y. Yang, L. Wu, G. Yin, L. Li and H. Zhao (2017), "A Survey on Security and Privacy Issues in Internet-of-Things," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250-1258, Oct. 2017.

3. M. A. M.Sadeeq, S. R. M. Zeebaree, R. Qashi, S. H. Ahmed and K. Jacksi (2018) "Internet of Things Security: A Survey," International Conference on Advanced Science and Engineering (ICOASE), Duhok, pp. 162-166.

4. S. Deshmukh and S. S. Sonavane (2017), "Security protocols for Internet of Things: A survey," 2017 International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2), Chennai, pp. 71-74.

5. A. Oracevic, S. Dilek and S. Ozdemir (2017), "Security in internet of things: A survey," 2017 International Symposium on Networks, Computers and Communications (ISNCC), Marrakech, pp. 1-6.

6. Y. Liu, Y. Kuang, Y. Xiao and G. Xu (2018), "SDN-Based Data Transfer Security for Internet of Things," in IEEE Internet of Things Journal, vol. 5, no. 1, pp. 257-268.

7. M. Ambrosin et al.,(2016), "On the Feasibility of Attribute-Based Encryption on Internet of Things Devices," in IEEE Micro, vol. 36, no. 6, pp. 25-35.

8. Hyo Jin Ban, Jaeduck Choi, and Namhi Kang (2016), "Fine-Grained Support of Security Services for Resource Constrained Internet of Things", Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks.

9. H. Kumarage, I. Khalil, A. Alabdulatif, Z. Tari and X. Yi (2016), "Secure Data Analytics for Cloud-Integrated Internet of Things Applications," in IEEE Cloud Computing, vol. 3, no. 2, pp. 46-56.

10. T. Yalçin (2016), "Compact ECDSA engine for IoT applications," in Electronics Letters, vol. 52, no. 15, pp. 1310-1312.

11. M. R. Schurgot, D. A. Shinberg and L. G. Greenwald (2015), "Experiments with security and privacy in IoT networks," 2015 IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks

12. Z. Liu, H. Seo, J. Großschädl and H. Kim (2016), "Efficient Implementation of NIST-Compliant Elliptic Curve Cryptography for 8-bit AVR-Based Sensor Nodes," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 7, pp. 1385-1397.

13. Z. Liu and H. Seo (2019), "IoT-NUMS: Evaluating NUMS Elliptic Curve Cryptography for IoT Platforms," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 3, pp. 720-729.

14. S. Ding, C. Li and H. Li (2018), "A Novel Efficient Pairing-Free CP-ABE Based on Elliptic Curve Cryptography for IoT," in IEEE Access, vol. 6, pp. 27336-27345.

15. Y. Zhang, Y. Shen, H. Wang, J. Yong and X. Jiang (2016), "On Secure Wireless Communications for IoT Under Eavesdropper Collusion," in IEEE Transactions on Automation Science and Engineering, vol. 13, no. 3, pp. 1281-1293.

16. S. N. Premnath and Z. J. Haas, "Security and Privacy in the Internet-of-Things Under Time-and-Budget-Limited Adversary Model," in IEEE Wireless Communications Letters, vol. 4, no. 3, pp. 277-280, June 2015.

17. P. Porambage, A. Braeken, C. Schmitt, A. Gurtov, M. Ylianttila and B. Stiller (2015), "Group Key Establishment for Enabling Secure Multicast Communication in Wireless Sensor Networks Deployed for IoT Applications," in IEEE Access, vol. 3, no. , pp. 1503-1511.

18. Carolina V. L. Mendoza and João H. Kleinschmidt(2015), "Mitigating On-Off Attacks in the Internet of Things Using a Distributed Trust Management Scheme", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks.

19. Xuran Li, Hao Wang, Hong-Ning Dai, Yuanyuan Wang, and Qinglin Zhao(2016), "An Analytical Study on Eavesdropping Attacks in Wireless Nets of Things", Hindawi Publishing Corporation Mobile Information Systems.

20. Sung-Ki Kim, Byung-Gyu Kim, and Byoung-Joon Min (2015), "Reducing Security Overhead to Enhance Service Delivery in Jini IoT", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks.

21. Jia-Li Hou and Kuo-Hui Yeh (2015), "Novel Authentication Schemes for IoT Based Healthcare Systems", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks.

22. Qingkuan Dong, Jiaqing Tong, and Yuan Chen (2015), "Cloud-Based RFID Mutual Authentication Protocol without Leaking Location Privacy to the Cloud", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks.

23. N. Fathima, R. Banu, and G. F. A. Ahammed (2019), "Modeling of secure communication in internet-of-things for resisting potential intrusion," Advances in Intelligent Systems and Computing, 2019, vol. 1047, doi: 10.1007/978-3-030-31362-3_38.

24. Ling Chi, Liang Hu, Hongtu Li, and Jianfeng Chu (2014), "Analysis and Improvement of a Robust User Authentication Framework for Ubiquitous Sensor Networks", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks.

25. N. Fathima, R. Banu, and G. F. A. Ahammed (2020), "Framework for Secure Transmission between Communicating Nodes with the Internet Host in IoT" International Journal of Disaster Recovery and Business Continuity Vol. 11, No. 1, pp. 1370-1380

26. Z. Liu and H. Seo (2019), "IoT-NUMS: Evaluating NUMS Ellipti Curve Cryptography for IoT Platforms," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 3, pp. 720-729.