Novel Secure Validation Scheme to Assess Device Legitimacy in Internet of Things

Ayasha[1]
Research Scholar, Periyar Univerity, Salem, India
Assistant Professor, Department of Computer Science
MGR College, Hosur, Krishnagiri-Dist, Tamilnadu, India

M Savitha Devi[2]
Assistant Professor & Head, Department of Computer Science, Periyar University Constituent College of Arts & Science Harur, Dharmapuri, Tamilnadu, India

***Abstract*—The increasing security concerns in Internet-of-Things (IoT) have led the researchers to evolve up with multiple levels of the research-based solution towards identifying and protecting the lethal threats. After reviewing the existing literature, it is found that existing approaches are highly specific toward stopping threats via predefined threat information. Hence, the proposed system introduces a new computational model capable of building up a flexible validation model for evaluating the legitimacy of the IoT nodes. The proposed system develops an algorithm that uses a simplified generation of secret keys, performs encryption, and generates validation tokens to ensure a higher degree of privacy and data integrity. The proposed model also contributes towards a unique energy allocation approach to ensure better energy conservation while performing security operations. The simulated study outcome shows better security and data transmission performance compared to the existing scheme.**

***Keywords*—Internet of things; security; validation; privacy; integrity; attacks**

I. Introduction

Internet of Things (IoT) offers more extensive coverage of different connected physical objects or machines, which are also known as things linked to a broader version of the network, i.e.,the internet [1]. Such physical objects are contributed by various technologies, software, hardware, actuators, and sensors, mainly with the objective of data transmission over the internet [2]. Data plays a significant role in IoT as this concept has evolved by integrating multiple technologies, e.g., automation, control system, wireless sensor network, ubiquitous computing, analytics, artificial intelligence [3]. This concept mainly targetsdeveloping a smart city by enabling more extensive connections of multiple and different types of machines. This causes a severe and increasing threat to security and privacy issues. There are various security concerns in the IoT environment connected explicitly with IoT devices and exchanged data. The first problem is its existing protection mechanism based on weaker password forms typically hard-coded and embedded within the device [4]. The second practical problem is associated with insufficient compliance of IoT devices manufacturers, which leads to insecure transfer and storage of data, usage of older operating environment and software, absence of robust updating mechanism, issues related to hardware, and hard-coded password. The next problem is related to a significantly lesser extent of awareness within the users, making the user morevulnerable in threat detection. Problems also exist due to the usage of insecure firmware. Due to this issue, the system suffers from brief downtime when the data is stored outside the cloud environment by the IoT device while performing updating operations. The existing physical devices are not secured from the external threat, which is not defined by the firewall system. Moreover, it is not feasible to imply a sophisticated security protocol running within the smart appliances or IoT devices due to their limitation of resource constraints and processing capability constraints. The usage of botnets by the attacker can significantly affect many IoT devices connected. Hence, during Distributed Denial-of-Service attacks in IoT, many connected appliances can be adversely affected. Apart from this, eavesdropping, industrial espionage, hijacking are some of the potential threats in IoT that have not yet met the robust security solution. There are various dedicated research-based solutions to deal with security concerns in IoT [5]-[9]. The conventional security solution of an IoT depends on Secure Socket Layer, Transport layer security, Datagram Transport Layer Solution, Quick UDP internet connection, secure MQTT, IP Sec [10].

Therefore, the research problem of proposed study is to address the limitation of conventional security scheme that may offer resistance but fails to offer full-proof validation of intention of any threat in large scale deployment over IoT. This problem is computationally challenging to implement whereas there is an increasing evolution of network devices as well as smart appliance for accessing services over IoT. Hence, this acts as motivating factor towards security for IoT devices.Therefore, this manuscript offers a solution to this issue by presenting a unique and lightweight validation scheme designed, unlike any existing approach. The prime objective of the proposed solution is to develop a computational framework that can perform secure validation towards securing all forms of IoT devices.The proposed model can identify the malicious intention of IoT nodes and offers a simplified encryption mechanism to mitigate the undefined threat in IoT. The paper also contributes to a novel energy computation scheme that compliments secure validation. The organization of the proposed paper is as follows: Section II discusses different taxonomies of existing security validation in IoT, followed by outlining research problems in Section III. Section IV discusses proposed research methodology while algorithm design is discussed in Section V. Section VI presents discussion while Result evaluation is illustrated in Section VII, while conclusive remarks are stated in Section VIII.

II. Related Work

At present, various schemes contribute towards security validation associated with identifying IoT devices while performing data forwarding.

- Blockchain-based Approaches: Blockchain is increasingly used in the majority of existing security approaches. The work presented by Hosen et al. [11] used context-aware blockchain validation. The approach also uses a software-defined network in the form of middleware to better control security operations in IoT. Banerjee et al. [12] have developed a blockchain-based authentication mechanism considering the key agreement protocol. The model is used in an implantable device that makes secure communication with the servers in the cloud. Blockchain is also reported to carry out authentication of cross-domain in IoT, as witnessed in the work of Ali et al. [13]. The researcher has presented a decentralized scheme for delegating permission and offer control over the structure of IoT. Further, the scheme also facilitates validating the local blockchain using the proof-of-Authentication and Integrity mechanism.

- Key Management-based Approaches: This is the most frequently used security scheme in IoT, where the emphasis is all about generation, storage, updating of secret keys among IoT devices. The computational model presented by Wang et al. [14] has presented a validation scheme for certificates used in IoT nodes. The prime idea is to assess the trust factor of IoT nodes. Xia et al. [15] have used a chaotic map to develop a key management scheme for authentication. The validation is carried out using informal security analysis along with the real-or-random model. Park et al. [16] have emphasized developing independent verification systems to offer untraceability and anonymity.

Further, the study has also used Burrows-Abadi-Needham logic to establish a secure bridge for mutual authentication servers and IoT devices. Shim et al. [17] have presented a study to assess a validation scheme towards anonymity issues in IoT. This security scheme is focused on the certificate's signature scheme to resist attacks towards secret keys and public keys. Another key-based protocol for validation is constructed by Saleem et al. [18], mainly targeting secure communication among cloud servers, roadside units, fog servers, and vehicles. Mahmood et al. [19] have developed key management based on distributed multiparty to carry out a compelling validation of nodes in IoT. The technique makes use of a chaotic map along with an on-way hashing approach for securing keying operation among all the core nodes and trusted servers. Public-key encryption and its different variant are witnessed to cover the IoT devices from most known threats. Such adoption of logic was reported in He and Zeadally [20],where elliptical curve encryption is used while validating RFID devices in IoT. The study outcome has found its security suitability on healthcare applications mainly. The work discussed by Yang et al. [21] has emphasized achieving forward secrecy in order to protect the session keys. For this purpose, a dynamic session key is presented,strengthening the credential management system in industrial-based IoTwithout any dependencies towards using primitives of public-key encryption.

- Policy-based Authentication:This scheme constructs a predefined policy to resist security threats. The security model of Banerjee et al. [22] has used a hashfunction with a defined security policy for offering validation for the regular/malicious IoT nodes. The study has also used a logical operator (bitwise exclusive OR) andan unclonable security function to compliment the device security. A similar approach of validation was also presented by Yanambaka et al. [23]. Existing studies have reported the usage of the message authentication scheme in order to construct a security policy in order to stop forgeability attacks in IoT. The model developed by Li et al. [24] has used identity-based encryption using signatures to strengthen privacy in IoT communication.

- Trust-based Security: These schemes are mainly meant for trust computation for ensuring the validation of IoT nodes. Rani et al. [25] have used game theory in order to evaluate trust in IoT. The work of Azad et al. [26] has used homomorphic encryption for securing the trust score in a decentralized manner. Xia et al. [27] have implemented a scheme for storage security using the trust factor to control accessibility. Almogren et al. [28] have used fuzzy logic for resisting Sybil attack and thereby developed a trust management scheme. The existing system has also witnessed other trust-related schemes by Truong et al.[29], Awan et al.[30], Fang et al.[31], Awan et al. [32], Wang et al. [33], Han et al. [34], etc.

- Unique Approaches: The work carried out by Amato et al. [35] has presented a unique technique based on workflow languages as well as semantics used for validating the inbuilt security characteristic of IoT devices. Another unique approach is presented by Ko etal. [36], where a validation scheme is designed using a tree that connects with variable security services with signature. The model assists the user in carrying out validation of the genuine sources anda relationship with the server. The existing system has also witnessed usinga cross-layer-based approach to offer an authentication scheme in IoT. The study carried out by Lee et al. [37] is mainly towards validation of user over physical layer as well as implementing encryption for large scale IoT deployment. The study makes use of the physical attributes in order to carry out preemptive-based authentication. Another unique approach witnessed in security validation in IoT is based on a group-based scheme, as witnessed in Aydin et al. [38]. The study has mainly targeted to resist man-in-middle attacks and replay attacks.The protocol also emphasized energy saving while carrying out group-based validation of many IoT nodes in a decentralized scheme.

The prominent research gap is existing approaches doesn’t offer lightweight encryption supportive of decentralized environment in IoTwith biased attacker identification policy. The next section outlines the problems associated with existing approaches and their methods towards validation.

III. Limitation / Research Problem

From the prior section, it has been seen that there are various approaches towards secure validation of an IoT device. After analyzing existing literature, apart from a valuable perspective in its security method and outcomes, there are also exploratory studies towards the limiting factors. This section outlines the limiting factors associated with the existing scheme as follows:

- Issues of decentralization: To offer more security coverage to large-scale IoT deployment, it is necessary to ensure the security scheme is decentralized. However, existing blockchain and key agreement-based schemes using a trust are more on a centralized security scheme and very much less towards decentralized implications. However, some work has used decentralized schemes, emphasizing delay control is not witnessed in existing schemes.

- Usage of Sophisticated Encryption: The encryption scheme is majority iterative and uses complex mathematical operations to ensure a better trapdoor function. However, the existing usage of encryption is quite voluminous, which will introduce a computational burden while trying to transmit data over the dense and more extensive network in IoT. Apart from this, sophisticated encryption will also saturate the resources to a higher level, and it is unlikely for the resource-constrained IoT nodes to sustain a more extended data transmission period.

- Unstructured Communication Scheme:The majority of existing secure data transmission scheme in IoT permits the data being captured from IoT nodes and directly forward to the gateway node. Such schemes offer higher resource fluctuation and challenge to control threats in case of multiple attackers in IoT. The impact of threat also becomes maximum. Such schemes cannot offer resistance from distributed denial of service attacks and man-in-middle attacks for large-scale deployment in IoT.

- Biased Identification Policies: Existing schemes are developed considering apriori information about attackers. Even the assessment is carried out using the same attackers. Such schemes will offer protection only from a predefined set of attackers and will never be able to identify if the attacker changes its strategy differing from what is coded within the firmware of the IoT nodes. A malicious node eventually does not attack when introduced in the environment; hence, existing security validation techniques will fail to identify dynamic attackers. The key management techniques are developed on an equal basis where there are fewer options for offering multi-stage encryption with a lightweight operation.

Apart from the above-stated problems, the existing scheme is not meant to cover up a set of integrated IoT attacks over a large scale. Apart from this, there is less consideration of resources used during validation during secure transmission. Therefore, the problem statement is "Developing a secure validation approach considering dynamic attack balancing with resource demands is challenging computational task in IoT." The next section outlines the solution towards this problem.

IV. Research Methodology

The proposed methodology addresses the limitation of existing approaches presented in prior section. The issues of decentralization is solved by presenting a lightweight encryption operation supportive of decentralized environment in IoT. The limitation of usage of sophisticated encryption is solved by parallel assessment of energy along with generation of secret key. The problem of unstructured communication scheme is addressed by developing a specific topology of an IoT which organization device and its respective communication with a gateway node. The problem of biased identification policies is addressed by performing secure modelling of local and global IoT. Local IoT would mean a network with a single application, while global IoT would mean forming a centralized network with multiple (and diverse) applications. Therefore, the proposed system uses a domain-based communication system where the domain will refer to a particular local IoT device where a heterogeneous domain performs its communication via a gateway node. Initially, simple modelling is being carried out by defining actors in local IoT (datacenter, target IoT, sensors) and global IoT (network of all the datacenters). A novel authentication mechanism is presented among all the possible actorsresiding within the local and global IoT domain by incorporating challenge and response-based approaches. A sophisticated validation module will be designed to validate the legitimacy of the requestor node. The research methodology adopted is analytical-based, as shown in Fig. 1.

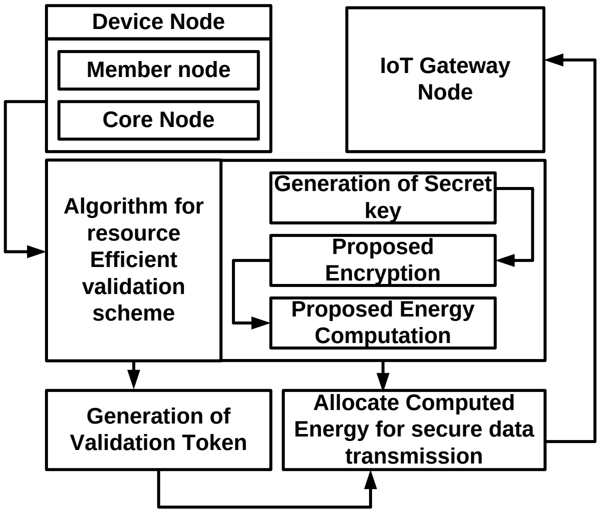
Device Node
Member node
Core Node
IoT Gateway Node
Algorithm for resource Efficient validation scheme
Generation of Secret key
Proposed Encryption
Proposed Energy Computation
Generation of Validation Token
Allocate Computed Energy for secure data transmission

Fig. 1. Tentative Research Methodologies for Phase-II.

The proposed system will formulate an algorithm for ensuring both forward and backward secrecy to safeguard the presented authentication framework for any possible threats. The system will use cipher-text-based encryption and novel energy computation to strengthen the authentication mechanism with lower resource consumption. The novelty of this model is its validation process which is meant to mitigate dynamic threats in large-scale IoT more effectively and in a decentralized manner to offer more security coverage. The next section discusses algorithm design and implementation towards the model.

V. Algorithm Design

The primary concern of the proposed system is to construct a unique validation scheme that could be used for assessing the authenticity of the IoT nodes. Owing to the last deployment scenario in an IoT, it is required to ensure that this scheme should also be resourced efficiently, balancing with the security demands. The proposed algorithm performs this dual-task in combining the security features with resource efficiency features. The steps of the proposed algorithm are as follows:

Algorithm for Resource-Efficient Validation Scheme

```
Input: $n, A, s, e, p$
Output: $v_{tok}, E$
Start
1. init $n, A, s, e, p$
2. For i=1:n
3.     $n_{mem} \leftarrow msk$
4.     $[d, e, n] \leftarrow f_1(msk, NP)$
5.     $n_{core} = A_{ix}(G_i(r < T_i))$
6.     $[v, ix] \leftarrow arg_{min}(dist)$
7.     $[v_{tok}] \leftarrow f_2(msg, enc_i, n_i)$
8.     $E_{tx} = f_3(dist, PL*cm)$
9.     $E(n_{core}(i)] \leftarrow E(n_{core}(i)) - E_{tx}$
10. End
End
```

The algorithm takes the input of *n* (IoT nodes), *A* (simulation area), *s* (gateway node), *e* (initialized Energy), *p* (probability of core IoT node) that upon processing yields and outcome of v_{tok} (generation of validation token) and*E* (computed Energy). The proposed algorithm initializes a master key *msk* and allocates it to a structured memory system n_{mem} of a node (Line-3). The next essential step of the proposed algorithm is to apply a customized function $f_1(x)$, responsible for carrying out a secret key generation. The internal steps of $f_1(x)$ are as follows: The function takes the input of master key *msk*, and nearest prime number *NP* and it generates three attributes memory structure of decryption *d*, memory structure of encryption *e*, and IoT nodes *n* (Line-4). Following are further steps:

- The IoT nodes *n* is computed by-product of master key *msk* and nearest prime number *NP*.
- An internal security attribute is constructed *Φ*, computed as *Φ*=(msk-1)(NP-1).
- The greatest common divisor is computed concerning random numbers for *NP* and obtained internal security attribute *Φ*.
- The value of this scheme is obtained by applying the modulus of the product of *d* and *e* and *Φ*.

The obtained information of attributes *d*, *e*, and *n* are further updated in the memory systems, accessed by legitimate IoT devices on a memory-sharing basis. In order to offer better control of the communication in large-scale IoT device deployment, the proposed system introduces a threshold-based provisioning scheme for the selection of core IoT nodes n_{core}(Line-5). The proposed mathematical expression of this threshold is as follow:

$$T = \frac{p}{\Delta p} . \Delta E \tag{1}$$

In the above expression (1), three dependable parameters are used in computation, i.e., p, Δp, and ΔE. The first variable,*p*, represents the probability that one of the IoT devices will be provisioned as a core IoT node authorized to forward the data to the gateway node. The second variable Δp represents $(1-p(|1/p|)).E/E_{init}$, where *E* and E_{init} represent total and initialized Energy, respectively. The selection of core IoT node n_{core} is selected considering matrix A_{ix} which retains all active nodes with *E* more than zero and any candidate IoT node randomly selected number less than T_i (Line-5). It should be noted that the variables*T* and T_i are different as the former is represented by mathematical expression (1) while the latter is represented as $T_i = E(G_i)$. It will mean that T_i is the threshold considered for all the randomly selected candidate nodes G_i which has sufficient residual Energy. The next task is to compute the distance *dist* between all the candidate IoT devices with the core IoT device (Line-6). The proposed system computes the minimum distance and obtains its value *v* and coordinates *ix* (Line-6). The variable *ix* is further used for updating the core IoT device. The next part of the algorithmic step is to perform encryption using an explicit function $f_2(x)$. Following are the internal operation of this encryption function:

- The function $f_2(x)$ takes the input of message *msg*, encryption attribute enc_i, and IoT device $n_{i,}$ which yields an outcome of validation token v_{tok} (Line-7).
- The first step is to compare the length of the message *msg* with the unit value. If it is found more than the unit value, then the size of the message is reduced to 32 bit.
- A simplified encoding is carried out for the encrypted attributed enc_i by converting decimal to binarized value.
- The function further compares the value of obtained encoded value from the prior step with the unit value. If the size of the encoded value is found more than the unit value, then it further put forward a condition where the value of the encoded attribute is equated to the unit value. The coefficient c is computed as,

$$c = |(c^2, n) * msg, n|, \text{ c=1} \tag{2}$$

$$c = |(c^2, n)| \tag{3}$$

The expression (2) is implemented if the encoded value is equal to the unit value, while expression (3) is implemented if the encoded value equals zero. The outcome, by either condition, generates coefficient c, which is a validation token vtok (Line-7). This completes the operation of the proposed encryption.After the encryption is carried out, the next emphasis is given to control the energy dissipation. The proposed system implements the final function f_3(x), which mainly targets to reduce the dissipated Energy while forwarded the encrypted data from the core IoT nodes to the gateway node (Line-8). Following are the internal steps being carried out towards energy control function f_3(x):

- This function takes the input of distance *dist*, length of data *PL*, and domain member *cm*. The proposed system considers domain-based communication where the domain represents a group of similar IoT devices. Each domain consists of two categories of nodes, i.e., domain member *cm* and core node n_{core}. The elementary information is captured by domain member *cm* and is then routed to core node n_{core} while the core node $\mathrm{n}_{\mathrm{core}}$ forwards all the data collected to the gateway node. The proposed model implements a standard energy computation of hierarchical communication scheme [39] for computing transmittance energy.
- The energy model used in this part of the implementation emphasizes the distance attribute. The core idea is to ensure that the distance between two communicating nodes is kept as minimal as possible. A higher distance will eventually lead to excessive energy drainage. Hence, a greedy approach is applied to ensure that nodes with minimum distance criteria perform data transmission to the gateway node.
- While performing the energy computation, the energy control function f_3(x) considers practical energy factors, e.g.,Energy required for antenna to carry out transmission within an IoT device, Energy required to amplify the signal, length of data to be transmitted, and distance. Further, the function initializes the Energy required to transmit validation token $\mathrm{v}_{\mathrm{tok}}$. This operation can be carried out for both active and passive modes of validation.
- The active mode of validation is when the validation is required instantaneously by the user, while the passive mode of validation is when the validation of the security token can be done later. The difference is that an active mode of validation is carried out before the data is transmitted, while a passive mode of validation is carried out when the data starts receiving at different network elements in an IoT environment. The active mode of validation can be carried out in case of a known attack, while the passive validation model can be carried out if the attacker strategy is unknown to the user. In both cases, safety is ensured. Therefore, the total energy consumption will bea summation of Energy required in performing either mode of validation of $\mathrm{v}_{\mathrm{tok}}$.

After the cumulative energy E is computed, the proposed system performs a reduction of Energy. This is carried out by obtaining the appropriate Energy obtained by subtracting the total Energy of the core IoT device with allocated transmitted Energy (Line-9). Unlike any existing energy modelling, the novelty factor is thatthe proposed system does not allocate static Energy, but it computes the exact necessary Energy and allocates it after performing the encryption steps. The next section discusses the discussion followed by results evaluation.

VI. Discussion

At present, there are scattered and multi-variants forms of security approaches to ensure that accessibility towards the IoT device is always carried out in secured manner. There are reported claims of benefits observed in existing approaches too in this regards on the basis of reviews carried out in Section II. However, a closer look into the review of literature shows that there is no potential connectivity among the existing techniques, which will mean that hybridization of multiple techniques are extremely challenging with existing approaches. The prime reason behind this is the dependencies of research environment, specification of implementation, and applicability are highly narrowed scope. Hence, there is no scope of integrating conventional security approaches towards assessing the legitimacy of the devices. This calls for evolution of the novel idea presented in this paper, where the idea is to address the identified research problem / limitation outlined in Section III.

A closer look into existing approaches shows that they are yet not much supportive of decentralized environment. This problem is directly addressed by implementing a key generation approach discussed in Section V considering completely distributed communication among IoT nodes in the form of cluster. Unlike any conventional IoT system, where there are only two roles of nodes i.e. IoT node and IoT gateway node, the proposed system offers two more distinct roles i.e. member node and core node, which is designed from the operational features of sensor network in IoT environment. The benefit of this scheme will be i) highly supported of decentralized environment considering local and global IoT system, ii) highly structured communication among different roles of device nodes and IoT gateway node, iii) conservation of energy due to structured communication system. Apart from this, the security strength of proposed system is further leveraged by inclusion of validation token which ensures the legitimacy of the node to participate in data communication process.Another interesting contribution of proposed methodology that separates it from existing approaches are its formulation of validation technique and all its attributes involved in it. Majority of the attributes used in the formulation of algorithm discussed in Section V i.e. distance, nodes, master key, message, encryption attribute, etc. are readily available from neighborhood node or hop table. No extensive computation is required to assess the validation token except few conditional checks being carried out. This significant reduces the computational burden and make the system highly scalable in peak traffic load in IoT for secure validation. Result evaluation is discussed next.

VII. Evaluation

This section illustrates the outcome obtained by implementing the secured validation in IoT. It is to be noted that the proposed system introduces a flexible validation scheme contributing towards secure communication in IoT.

A. Simulation Parameters

The proposed system is scripted in MATLAB on a regular 64-bit machine with a Core i5 processor. The study is evaluated considering 100-500 IoT devices deployed in an arbitrary position in a simulation area of 1000 x 1000 m^2 considering the variable location of the gateway node. The initialized Energy of IoT nodes is considered 10 Joule with a 5% probability score for a member IoT node to become the core access node in IoT. The proposed study also consider variable energy attributes, e.g., theEnergy utilized for data transmission by IoT nodes as 5nj/bits, Energy required to amplify signals by wireless IoT nodes as 100 pJ/bit for every squared meter of simulation area,Energy utilized for generating and assessing validation token as 80 μJ/validation tokens, Energy required for assessing validation token in active mode as 13μJ/validation tokens, Energy required for assessing validation token in passive mode as 5μJ/validation tokens, the size of the data packet is 1000 bytes. The consideration of the values has been considered according to the standard ranges observed from existing literature and standard secured hierarchical protocols.

B. Simulation Environment

The first step of the implementation is to deploy a generalized IoT environment consisting of member IoT devices, core IoT devices, and a gateway node. A domain-specific communication is carried out where the member IoT nodes forward the data to core IoT nodes which further aggregates the data and forward it to either gateway node directly or forward to its nearest neighboring core node. The direct transmission to the gateway node is carried out if the distance between the core node and gateway resides in the proximity of each other. Otherwise, multi-hop transmission is carried out via other core nodes to the gateway node. Assuming the presence of attackers, the analysis is carried out as the proposed system is designed to resist any form of key-based and routing intrusion associated with identity-based theft attacks in the IoT environment. The communication is permitted to continue for 7000 simulation rounds till all the IoT nodes are depleted of their Energy.

C. Performance Evaluation

For an effective benchmarking system, the proposed system consider the existing system of the secured hierarchical protocol [39], which acts as baseline security of IoT device. The prime justification of adopting this existing system for benchmarking is as follows: i) sensors and actuators are an integral part of an IoT environment in the form of IoT devices compliant with security protocols applied for sensory application. Hence, secure hierarchical protocols [39] offer a balance between security and energy efficiency, which suits the proposed objectives too, ii) it offers a standard mathematical formulation to compute Energy considering various energyattributes. In order to facilitate equivalent testbeds, similar energy parameters are also selected to carry out the proposed implementation. This will offer a fair outcome in a similar test environment for both proposed and existing systems. For more granular analysis, the proposed system is assessed for both its active and passive state of verification of validation tokens. The performance parameters selected for the analysis are rounds required to complete validation, number of sustained nodes, delay, throughput, resource, fluctuation, and overall energy depletion.

D. Impact of the Proposed System on Transmission

This section discusses the simulation outcome involved for each performance parameter.

1) Validation round: The first performance parameter to assess is validation rounds, computed by observing the total number of rounds required for both proposed and existing systems to complete the validation.

Fig. 2 highlights the simulated outcome of observed validation rounds where the proposed system is observed to found lesser validation rounds thanthe existing system. The proposed system with passive state *Prop(P)* is found to occupy less validation time than that of active state *Prop(A)*. The prime reason behind this validation inactive state includes end-to-end node validation, which is not in the case of the passive state. On the other hand, existing Secured Hierarchical protocol *Exist(SecHier)* carry out iterative validation till all the IoT node depletes its complete Energy. Hence, the existing approach is found to offer more validation time compared to the existing system.

2) Number of sustained nodes: Basically, sustained nodes will mean the number of IoT devices found to possess specific cut-off Energy. A sample analysis has been carried out for 100 IoT devices, and the outcome is found to be precisely similar even if the number of nodes is increased. While the simulation is carried out, observed values for several nodes with optimal residual Energy are obtained to achieve the graphical outcome stated in Fig. 3.

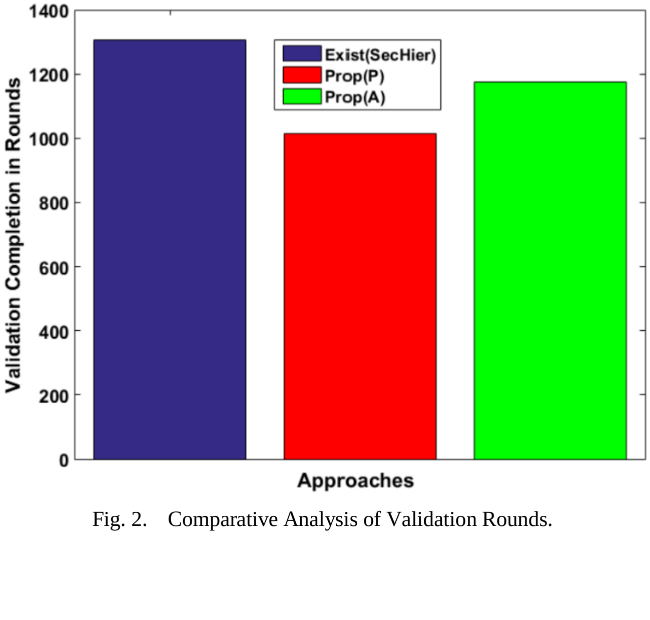

Fig. 2. Comparative Analysis of Validation Rounds.

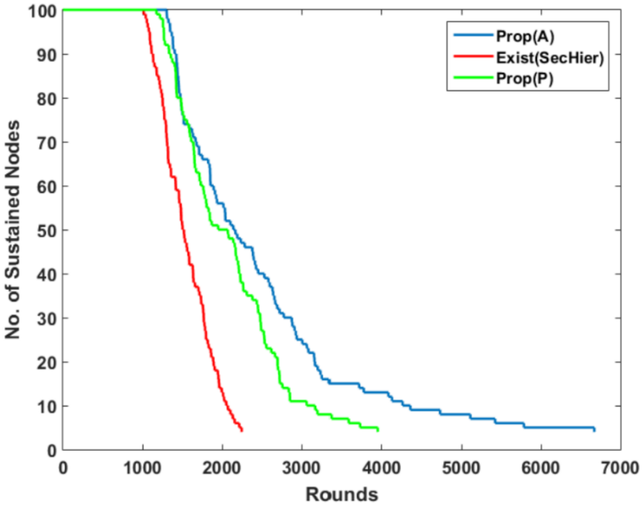

Fig. 3. Comparative Analysis of Number of Sustained Node.

According to the trend of curves in Fig. 3, both the version of the proposed system offers more sustained nodes for increasing rounds of simulation in contrast to the existing scheme. The existing scheme lets all the IoT devices perform secured data transmission using a conventional public encryption scheme. This will demand more memory dependencies toward each IoT node, which results in a more saturated state of a gradually increasing number of IoT devices, which results in faster drainage of Energy; hence, existing system collapse even before completion of 50% of simulation rounds. On the other hand, the proposed scheme with a passive state offers more sustainability, but due to not considering end-to-end node validation, each node must be finalized 100% of validation. However, the proposed scheme with active mode has a memory sharing feature that lets all nodes perform 100% of validation simultaneously compared to an existing system with a passive state. Hence, the passive state is ideal for medium-scale deployment, while the active scale is ideal for large-scale deployment of IoT.

3) Delay: The proposed system considers end-to-end delay, which is consumed time for transmitting the packet from transmitting IoT device in one domain to the gateway node inclusive of all the relay nodes within it. Delay is one of the essential parameters to judge the possibility of various attacks (e.g., flooding-type attacks, man-in-middle attacks). Delay is an eventual part of large-scale IoT communicationdue to various intrinsic and extrinsic factors in IoT. The intrinsic factors will be the data packet size, the number of available IoT devices, the distance between two transmission points, and the job saturation state of each relay node. The extrinsic factor will be interference caused by communication, densityof IoT nodes, battery life of each node, queuing process adopted, etc. An effective security logic should optimize the delay performance so that with an effective delay score, the transmission of the packet could be carried out securely and for the more extended extensible period of data transmission between IoT nodes and gateway nodes.

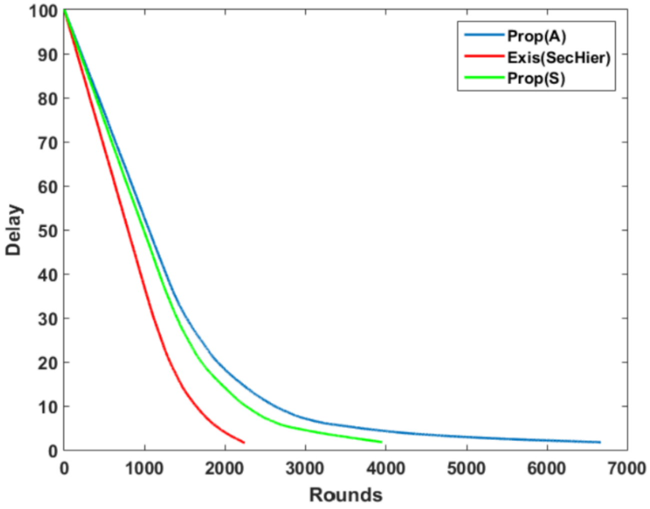

Fig. 4. Comparative Analysis of Delay.

Fig. 4 highlights the simulated outcome of delay. A closer look into this outcome will show that the proposed system offers extensible delay performance, which permits data transmission till maximum simulation rounds, unlike existing approaches. The justification of this outcome is similar to that of the number of sustainable nodes.

4) Throughput: This performance parameter is computed as the number of arrived packets from transmitting nodes to the actual destination node with the inclusion of all relay nodes. An effective security protocol should offer better throughput performance to ensure that its security scheme does not hamper the data transmission performance.

Fig. 5 exhibits that the proposed system offers better throughput performance compared to the existing scheme. The prime reason is that the existing scheme doesn't offer sustainable nodes to carry out data transmission, whereas the proposed scheme offers more sustainable nodes, resulting in better throughput performance. The idea is to balance Energy, data transmission, and internal security operation at the same time.

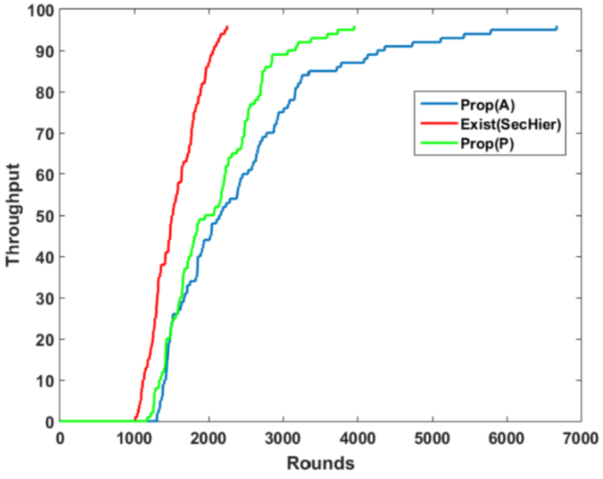

Fig. 5. Comparative Analysis of Throughput.

5) Resource fluctuation: An efficient security protocol should offer consistent resource utilization to retain more IoT nodes to carry out secure transmission.

However, resource demands can fluctuate depending on the random allocation of the data packet and the different dynamics present within the IoT environment. The standard variance parameter computes this parameter in statistics associated with transmittance energy. Fig. 6 highlights that the proposed system offers slightly more resource fluctuation (5-10%) thanthe existing approach. The contribution of this scheme is that although it offers little more resource fluctuation, it still manages to use maximum IoT nodes till the end of the simulation, whereas the existing scheme fails to do so. Hence, although the existing scheme offers lesser resource fluctuation, it can still not be deployed over a large-scale application in IoT.

6) Energy depletion: The proposed system makes use of expression used in its algorithm to compute the Energy. The outcome of Fig. 7 highlights better energy retention of the proposed system over more simulation rounds.

E. Impact of Proposed System on Security

The proposed algorithm offers a significant level of security in IoT. The lightweight cryptographic operation carried out in the proposed system offers better confidentiality as well as data integrity. On the other hand, the usage of validation tokens can ensure the better form of non-repudiation and authenticity factor associated with transmission in large-scale deployment in IoT. The security analysis towards different variants of attacks in IoT are briefed as follows:

- Resilience towards passive form of intrusion: The encryption method used in the proposed system benefits the system due to performing computation over a ciphered packet with non-dependencies towards performing initial decryption. This operation result leads to encrypted data, which, when subjected to decryption, will lead to a unique identical outcome. Hence, it can be used to preserve privacy for the computation and outsourced storage in the data center. The significant beneficial factor of the proposed system is that IoT nodes perform encryption and forward the data to a gateway that further forwards it to the datacenter, encrypting it. Therefore, any form of the passive intruder will notcompromise the transmitted data without possessing the decrypted key, which is further computed and not stored in any device.

- Resilience towards active form of intrusion: In most such attacks, the target victim will be the core IoT node as the relay node due to the restricted operation by the member IoT devices in a domain-based communication system. As the intruder will not have possession of a legitimate validation token in order to perform concatenation with the beacon to be broadcasted in a wireless environment by IoT nodes, it will be impossible for an intruder to act as a gateway node or even the core IoT node in order to launch an attack. Hence, any possibility of identity-based theft is not possible by an attacker while it offers higher resistance towards selective forwarding attack and sinkhole attack in IoT, which the existing protocols cannot stop. Further, along with the usage of validation tokens and memory sharing among the IoT nodes, the proposed system also offers protection against flooding attacks.

- Resilience to device compromise intrusion: In case of device compromise intrusion, the victim IoT device acts usually but will carry out malicious intention towards each transmission and data processing activity. Assuming that a victim node acts as a member node or relay node, there are still requirements under a validation check by generating a secret key. It is unlikely that the victim node will generate the secret key obeying the proposed protocol, and hence the secret key generation before encryption by the victim node will eventually fail to comply. This will itself stop all communication with the victim node and updatethe trust value of the victim node. Hence, even if the victim node is present inside the network, they will never participate in any data processing or data transmission in IoT. Dependency on multiple parameters will also stop the victim node from carrying out this computation.

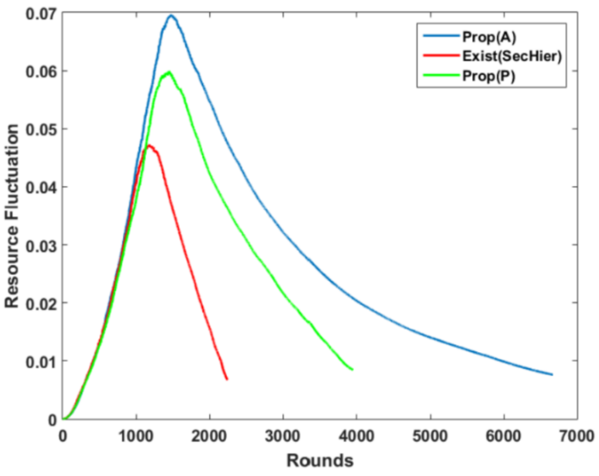

Fig. 6. Comparative Analysis of Resource Fluctuation.

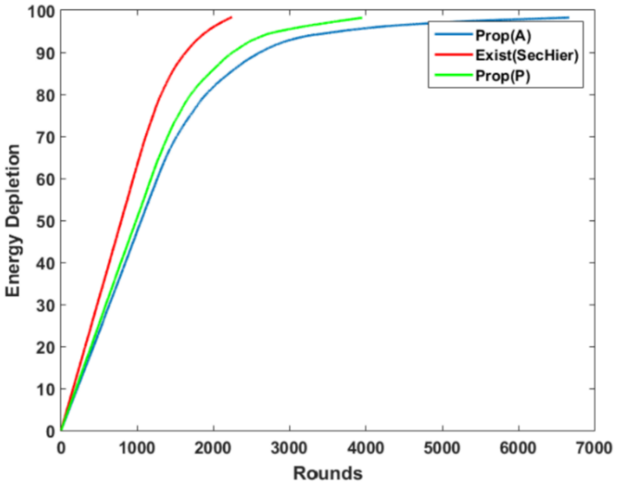

Fig. 7. Comparative Analysis of Energy Depletion.

VIII. Conclusion

IoT security has been a critical concern forthe past few years, which has not yet met with an effective solution. The existing solution is based on predefined knowledge of the attacker to circumvent the defined threats. Such a scheme is not capable to even identify the attacker when they alter their strategy. Hence, this paper offers a solution by presenting a secure validation technique thatidentifies the malicious intention of an IoT device and protects the data. It should be noted that proposed system is assessed over a formulated IoT environment scripted in MATLAB where data packets are programmatically generated based on arbitrary traffic load in order to map with practical world use-cases. Hence, the proposed system is applicable for any form of data or traffic environment over IoT, which increases the scope of implementation. This is one significant novelty factor unlike existing systems which mainly uses data traces. Apart from this, another novelty of proposed system is introduction of roles of IoT device to understand the demands of security and communication system over decentralized environment unlike existing approaches. The inclusion of local and global IoT will also contribute to novelty factor of proposed system.

Following are the contribution/novelty of the proposed system, viz.

- The proposed system introduces a secure validation that is capable of performing in both active and passive states of communication in IoT.
- The proposed system performs validation of the encrypted data by applying validation token along with the packets, further followed by secret keys in order to offer more layers of security.
- The proposed system does not make use of any complex or sophisticated encryption operation, and hence it is capable of conserving maximized sustainable IoT devices for a longer time.
- A unique energy computation is carried out in proposed system which ensures allocated of appropriate Energy required for transmitting encrypted data to the gateway node, unlike any existing techniques where static Energy is allocated every time in data transmission.

References

[1] Goundar, J. Avanija, G. Sunitha, K.R.Madhavi, S.B.Bhushan, "Innovations in the Industrial Internet of Things (IIoT) and Smart Factory", IGI Global {ublisher of Timely Knowledge, 2021.

[2] B. Marr, "Tech Trends in Practice The 25 Technologies that are Driving the 4th Industrial Revolution", Wiley, pp. 304, 2020.

[3] G. Kaur, P. Tomar, and M. Tanque, "Artificial Intelligence to Solve Pervasive Internet of Things Issues", Academic Press, 2020.

[4] D. Yu, L. Zhang, Y. Chen, Y. Ma, and J. Chen, "Large-Scale IoT Devices Firmware Identification Based on Weak Password," in IEEE Access, vol. 8, pp. 7981-7992, 2020, doi: 10.1109/ACCESS.2020.2964646.

[5] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," in IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2702-2733, thirdquarter 2019, doi: 10.1109/COMST.2019.2910750.

[6] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646-1685, thirdquarter 2020, doi: 10.1109/COMST.2020.2988293.

[7] F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8182-8201, Oct. 2019, doi: 10.1109/JIOT.2019.2935189.

[8] I. Farris, T. Taleb, Y. Khettab and J. Song, "A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems," in IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 812-837, Firstquarter 2019, doi: 10.1109/COMST.2018.2862350.

[9] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani and J. Lim, "Security, Privacy and Trust for Smart Mobile- Internet of Things (M-IoT): A Survey," in IEEE Access, vol. 8, pp. 167123-167163, 2020, doi: 10.1109/ACCESS.2020.3022661.

[10] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis." Sensors 20, no. 13 (2020): 3625.

[11] A. S. M. S. Hosen et al., "Blockchain-Based Transaction Validation Protocol for a Secure Distributed IoT Network," in IEEE Access, vol. 8, pp. 117266-117277, 2020, doi: 10.1109/ACCESS.2020.3004486.

[12] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, J. J. P. C. Rodrigues and Y. Park, "Physically Secure Lightweight Anonymous User Authentication Protocol for Internet of Things Using Physically Unclonable Functions," in IEEE Access, vol. 7, pp. 85627-85644, 2019, doi: 10.1109/ACCESS.2019.2926578.

[13] G. Ali et al., "xDBAuth: Blockchain-Based Cross-Domain Authentication and Authorization Framework for Internet of Things," in IEEE Access, vol. 8, pp. 58800-58816, 2020, doi: 10.1109/ACCESS.2020.2982542.

[14] M. Wang, C. Qian, X. Li, S. Shi, and S. Chen, "Collaborative Validation of Public-Key Certificates for IoT by Distributed Caching," in IEEE/ACM Transactions on Networking, vol. 29, no. 1, pp. 92-105, Feb. 2021, doi: 10.1109/TNET.2020.3029135.

[15] J. Xia, G. Cheng, S. Gu and D. Guo, "Secure and Trust-Oriented Edge Storage for Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4049-4060, May 2020, doi: 10.1109/JIOT.2019.2962070.

[16] K. Park et al., "LAKS-NVT: Provably Secure and Lightweight Authentication and Key Agreement Scheme Without Verification Table in Medical Internet of Things," in IEEE Access, vol. 8, pp. 119387-119404, 2020, doi: 10.1109/ACCESS.2020.3005592.

[17] K. -A. Shim, "Universal Forgery Attacks on Remote Authentication Schemes for Wireless Body Area Networks Based on Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9211-9212, Oct. 2019, doi: 10.1109/JIOT.2019.2922701.

[18] M. A. Saleem, K. Mahmood, and S. Kumari, "Comments on "AKM-IoV: Authenticated Key Management Protocol in Fog Computing-Based Internet of Vehicles Deployment"," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4671-4675, May 2020, doi: 10.1109/JIOT.2020.2975207.

[19] Z. Mahmood, A. Ullah, and H. Ning, "Distributed Multiparty Key Management for Efficient Authentication in the Internet of Things," in IEEE Access, vol. 6, pp. 29460-29473, 2018, doi: 10.1109/ACCESS.2018.2840131.

[20] D. He and S. Zeadally, "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography," in IEEE Internet of Things Journal, vol. 2, no. 1, pp. 72-83, Feb. 2015, doi: 10.1109/JIOT.2014.2360121.

[21] Z. Yang, J. He, Y. Tian, and J. Zhou, "Faster Authenticated Key Agreement With Perfect Forward Secrecy for Industrial Internet-of-Things," in IEEE Transactions on Industrial Informatics, vol. 16, no. 10, pp. 6584-6596, Oct. 2020, doi: 10.1109/TII.2019.2963328.

[22] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, J. J. P. C. Rodrigues and Y. Park, "Physically Secure Lightweight Anonymous User Authentication Protocol for Internet of Things Using Physically Unclonable Functions," in IEEE Access, vol. 7, pp. 85627-85644, 2019, doi: 10.1109/ACCESS.2019.2926578.

[23] V. P. Yanambaka, S. P. Mohanty, E. Kougianos and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication on the Internet of Medical Things," in IEEE Transactions on Consumer Electronics, vol. 65, no. 3, pp. 388-397, Aug. 2019, doi: 10.1109/TCE.2019.2926192.

[24] J. Li, Z. Zhang, L. Hui, and Z. Zhou, "A Novel Message Authentication Scheme With Absolute Privacy for the Internet of Things Networks," in IEEE Access, vol. 8, pp. 39689-39699, 2020, doi: 10.1109/ACCESS.2020.2976161.

[25] R. Rani, S. Kumar, and U. Dohare, "Trust Evaluation for Light Weight Security in Sensor Enabled Internet of Things: Game Theory Oriented Approach," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8421-8432, Oct. 2019, doi: 10.1109/JIOT.2019.2917763.

[26] M. A. Azad, S. Bag, F. Hao and A. Shalaginov, "Decentralized Self-Enforcing Trust Management System for Social Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 4, pp. 2690-2703, April 2020, doi: 10.1109/JIOT.2019.2962282.

[27] J. Xia, G. Cheng, S. Gu and D. Guo, "Secure and Trust-Oriented Edge Storage for Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4049-4060, May 2020, doi: 10.1109/JIOT.2019.2962070.

[28] A. Almogren, I. Mohiuddin, I. U. Din, H. Almajed and N. Guizani, "FTM-IoMT: Fuzzy-Based Trust Management for Preventing Sybil Attacks in Internet of Medical Things," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4485-4497, 15 March15, 2021, doi: 10.1109/JIOT.2020.3027440.

[29] N. B. Truong, G. M. Lee, T. Um and M. Mackay, "Trust Evaluation Mechanism for User Recruitment in Mobile Crowd-Sensing in the Internet of Things," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 10, pp. 2705-2719, Oct. 2019, doi: 10.1109/TIFS.2019.2903659.

[30] K. A. Awan, I. U. Din, M. Zareei, M. Talha, M. Guizani and S. U. Jadoon, "HoliTrust-A Holistic Cross-Domain Trust Management Mechanism for Service-Centric Internet of Things," in IEEE Access, vol. 7, pp. 52191-52201, 2019, doi: 10.1109/ACCESS.2019.2912469.

[31] W. Fang, M. Xu, C. Zhu, W. Han, W. Zhang and J. J. P. C. Rodrigues, "FETMS: Fast and Efficient Trust Management Scheme for Information-Centric Networking in the Internet of Things," in IEEE Access, vol. 7, pp. 13476-13485, 2019, doi: 10.1109/ACCESS.2019.2892712.

[32] K. A. Awan, I. Ud Din, A. Almogren, M. Guizani, A. Altameem, and S. U. Jadoon, "RobustTrust – A Pro-Privacy Robust Distributed Trust Management Mechanism for Internet of Things," in IEEE Access, vol. 7, pp. 62095-62106, 2019, doi: 10.1109/ACCESS.2019.2916340.

[33] T. Wang, H. Luo, W. Jia, A. Liu, and M. Xie, "MTES: An Intelligent Trust Evaluation Scheme in Sensor-Cloud-Enabled Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2054-2062, March 2020, doi: 10.1109/TII.2019.2930286.

[34] S. Han, M. Gu, B. Yang, J. Lin, H. Hong and M. Kong, "A Secure Trust-Based Key Distribution With Self-Healing for Internet of Things," in IEEE Access, vol. 7, pp. 114060-114076, 2019, doi: 10.1109/ACCESS.2019.2935797.

[35] F. Amato, V. Casola, G. Cozzolino, A. De Benedictis and F. Moscato, "Exploiting Workflow Languages and Semantics for Validation of Security Policies in IoT Composite Services," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4655-4665, May 2020, doi: 10.1109/JIOT.2019.2960316.

[36] H. Ko, J. Jin, and S. L. Keoh, "Secure Service Virtualization in IoT by Dynamic Service Dependency Verification," in IEEE Internet of Things Journal, vol. 3, no. 6, pp. 1006-1014, Dec. 2016, doi: 10.1109/JIOT.2016.2545926.

[37] Y. Lee, J. Yoon, J. Choi, and E. Hwang, "A Novel Cross-Layer Authentication Protocol for the Internet of Things," in IEEE Access, vol. 8, pp. 196135-196150, 2020, doi: 10.1109/ACCESS.2020.3033562.

[38] Y. Aydin, G. K. Kurt, E. Ozdemir and H. Yanikomeroglu, "A Flexible and Lightweight Group Authentication Scheme," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10277-10287, Oct. 2020, doi: 10.1109/JIOT.2020.3004300.

[39] M. Elshrkawey, S.M. Elsherif, and M. E. Wahed, "An enhancement approach for reducing the energy consumption in wireless sensor networks." Journal of King Saud University-Computer and Information Sciences, vol.30, no. 2, pp.259-267, 2018.