International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 1, February 2020, pp. 1092~1100
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i1.pp1092-1100

Novel authentication framework for securing communication in internet-of-things

Shamshekhar S. Patil[1], Arun Biradar[2]
[1]Department of Computer Science & Engineering, Dr. AIT, India
[2]Department of Computer Science Engineering, East West Institute of Technology, India

Article Info

Article history:

Received Aug 6, 2019
Revised Oct 4, 2019
Accepted Oct 15, 2019

Keywords:

Attacks
Encryption
Internet-of-Things
Intrusion
Security

ABSTRACT

Internet-of-Things (IoT) offers a big boon towards a massive network of connected devices and is considered to offer coverage to an exponential number of the smart appliance in the very near future. Owing to the nascent stage of evolution of IoT, it is shrouded by security loopholes because of various reasons. Review of existing research-based solution highlights the usage of conventional cryptographic-based solution over the traditional mechanism of data forwarding process between IoT nodes and gateway. The proposed system presents a novel solution to this problem by a model that is capable of performing a highly secured and cost-effective authentication process. The proposed system introduces Authentication Using Signature (AUS) as well as Security with Complexity Reduction (SCR) for the purpose to resist participation of any form of unknown threats. The outcome of the model shows better security strength with faster response time and energy saving of the IoT nodes.

Corresponding Author:

Shamshekhar S. Patil,
Department of Computer Science & Engineering,
Dr. Ambedkar Institute Of Technology (Dr. AIT),
Bengaluru, India.
Email: shamshekhar.patil@dr-ait.org

1. INTRODUCTION

Internet-of-Things (IoT) has been slowly capturing the global network integrated with cloud-based services that are characterized by a massive network of different smart appliances [1, 2]. As it connects different forms of devices, it is liable to use various forms and types of communication medium in order to ensure connectivity and data transmission [3, 4]. One of the biggest threats in IoT is the security challenges which have various reasons. At present, there is a billion number of IoT devices that are globally interconnected, and this score of devices is anticipated to exponentially increase in the next few years. Unfortunately, such massive numbers of existing commercial devices are not assessed for lethal security threats in manufacturing companies. Existing producers of IoT devices offer security in terms of updates only for a shorter period of time, which is incapable of resisting lethal threats.

Another significant problem in IoT security is the common threat of Distributed Denial-of-Services [5]. As the IoT nodes are connected via cloud services; therefore, it is eventual that the adversarial affecting cloud ecosystem could also easily affect the devices networks without much effort. Data privacy is another significant problem in IoT as the devices consistently capture the data, processes it, and transmits it to another IoT device [6, 7]. The challenging part in this is that the data of the user are highly distributed and shared among each other, which violate the privacy rights of the user data [8]. Apart from this usage of machine learning and automation is another factor which enhances the features of IoT device with respect to data analytics, but it also invites various security threats. The usage of artificial intelligence is quite inevitable as IoT deals with millions of connected devices [9]. Majority of such tools are highly autonomous, which

contradicts the essential functions of various enterprise applications. At present, there are various existing approaches that have been evolved up discussing the security aspects associated with IoT [10]. A closer look at the existing approaches shows that they are highly specific towards addressing a particular form of the adversary in IoT. Unfortunately, such study approaches could only explain its effectiveness over a certain set of problems, and their applicability is extremely limited to a few sets of attack only. Hence, such approaches are in nascent stages of research and development and require more intensive investigation. Apart from this, there is another problem associated with topology of an IoT which says that IoT nodes are always required to perform uplink transmission via IoT gateway node that carries out translational services. The problem using this conventional topology is that there is much involvement of time factor, which gives an opportunity to man-in-middle attack to launch an attack. Apart from this, the energy consumption of the IoT nodes will also be high if any complex cryptographic protocol (e.g., Rivest-Shamir Algorithm) runs in its underlying architecture. As the IoT nodes are resource constrained nodes; hence, execution of complex cryptographic algorithm will further drain out the energy of such nodes. Such an implementation cycle offers problems in both security as well as data delivery performances. Therefore, there is a deliberate need of an effective system that can investigate the change of such inherent mechanism of data packet forwarding process such that both security, as well as data delivery performance, should increase. Therefore, the proposed system presents a novel analytical model that is responsible for introducing a secured authentication system, a novel mechanism of the communication process from IoT nodes, and significant saving of energy of the nodes.

There are various existing approaches that have offered discussion about the security approaches in IoT [11]. Most recently, Das et al. [12] have used elliptical curve cryptography in order to offer access control in the IoT environment. The works of Han et al. [13] have presented security modeling using a software-defined network. Approach using shuffling of addresses has been carried out by Nizzi et al. [14] for minimizing the network overhead. The work of Siboni et al. [15] has presented a framework that can be used for assessment of security strength connected with IoT. The authors have also used machine learning process in order to carry out this work. Wang et al. [16] have discussed security approaches using the physical layer in order to incorporate the precise level of secrecy with better adaptability to network alteration. Significance of security and trust is discussed by Hudson [17]. Device authentication problem has been discussed by Hao et al. [18] where the physical layer has been used while Li et al. [19] has used trust factor as a part of the evaluation process.

Privacy is another concern in the IoT system, especially when it handles the massive scale of data and the work of Sollins [20] has presented a conceptual solution for this. Wazid et al. [21] have discussed a key management scheme for promoting the autonomous assessment of security strength. Secure transmission of data using a software-defined network was also proven to offer better security, as seen in the work of Liu et al. [22]. The agent-based mechanism was also used in IoT and cloud ecosystem as MANET finds its ultimate deployment over this. The recent works carried out by Magarino et al. [23] have used agent-based approach for facilitating massive mining data. Another recent work of Fortino et al. [24] has discussed how agent-based mechanism can be embedded with smart objects in the IoT environment. The work of Gargees and Scott [25] has presented a technique for facilitating data structurization over IoT media in order to extract the pattern of communication. However, such studies are more data-oriented and less on security. Another work carried out by Fortino et al. [26] have discussed that hybridizing the characteristics of agents has multiple benefits of communication system assessment in an IoT. The work carried out by Hsieh et al. [27] has constructed the design of an agent using the event-driven approach for constructing the communication mechanism in IoT. The agent-based mechanism was also used in IoT and cloud ecosystem as MANET finds its ultimate deployment over this. Another recent work of Fortino et al. [28] has discussed how agent-based mechanism can be embedded with smart objects in the IoT environment. The work of Gargees and Scott [29] has presented a technique for facilitating data structurization over IoT media in order to extract the pattern of communication. However, such studies are more data-oriented and less on security. The study carried out by Santos et al. [30] has discussed the usage of software agents, along with the incorporation of intelligence. The work carried out by Hsieh et al. [31] has constructed the design of an agent using the event-driven approach for constructing the communication mechanism in IoT. The existing system offers a certain level of advance as well as a certain level of limitation too that are found to affect security features in IoT. The next section discusses the research problems of existing approaches.

Significant research problems are as follows:

a. Adoption of advanced and extensive cryptographic algorithm usage is too high in the existing system without much emphasis on lightweight-based security approach.
b. Existing concepts are bound by the hardware-based architecture of an IoT whereas there is no much attempt toward computational modeling of secure routing scheme in it.

c. Existing approaches to forwarding the data to a fixed IoT gateway suffers from traffic management problem, the energy problem, as well as complex problems.
d. Attack-specific solutions in the existing system are less practical while they do not apply to other dynamic scenarios of attacks in IoT.

Therefore, the problem statement of the proposed study can be stated as "*Developing a computational framework where an enhanced and robust authentication mechanism is constructed in order to offer a significant level of secrecy in IoT communication system*."

This part of the study is a continuation of the prior model [32] towards securing the IoT environment. The proposed work is introducing a robust authentication mechanism as well as a novel communication system in IoT. The prime agenda of the proposed system is to ensure that no illegitimate member in the IoT environment could ever participate in the data dissemination process. The developed flow of the proposed system is showcased in Figure 1.

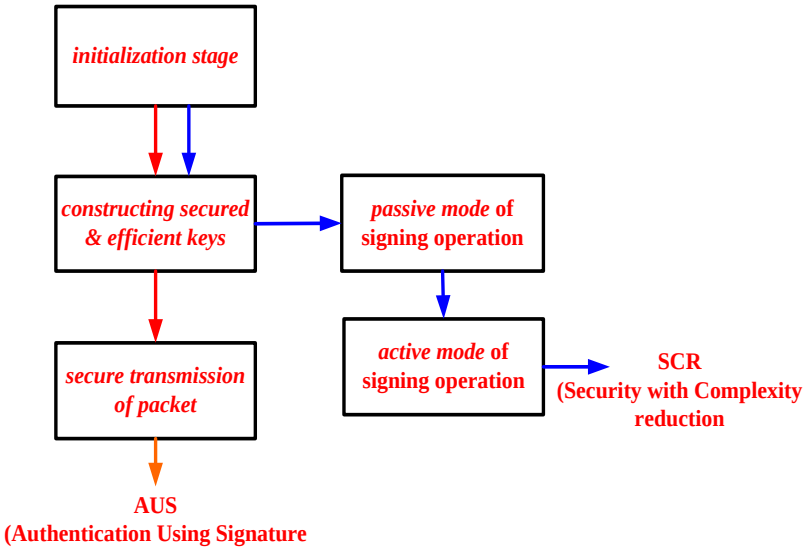


Figure 1. Proposed schema

The above diagram Figure 1 highlights that the proposed system is classified into two modules on the basis of the operation. The first module of AUS (Authentication Using signature) is used for generating the digital Signature while the second module of SCR (Security with Complexity Reduction) is responsible for authenticating the generated messages. The proposed system identifies the strength of using a digital signature, which offers faster security checks as well as cost-effective security incorporation. The module of AUS has three stages of operation while the second module of SCR has four stages of operation where the first and second stage of the operation is common with AUS while the third and fourth stage of the operation is distinct operation in SCR. Apart from this, the proposed system is developed over analytical research methodology where the framework is mainly inclined toward including multi-tier stages of the generation of unique keys in such a way that even if anyone set of keys is compromised, the attacker will never be able to perform decryption. Another uniqueness of the proposed system is that it offers energy saving by introducing a novel concept where the local gateway nodes are selected dynamically, unlike existing system where the IoT devices straight forward message to IoT gateway. The proposed system also introduces IoT access nodes that take input of all the data from distributed IoT gateways.

2. SYSTEM IMPLEMENTATION

The proposed concept is designed on the basis of the problems associated with the current communication architecture of the IoT gateway system. According to the existing system, the IoT nodes (which are essentially sensory application) forward their data to the IoT gateway node and then all IoT gateway node forwards the data to the access point that connects directly to cloud services as shown in Figure 2. The biggest challenge, in this case, will be to perform communication between the gateway node as well as all the IoT nodes has to compete to forward data to best gateway node on the basis of distance.

This process is a highly computational expensive process and is not secured as there are all possibilities that some forged data is introduced to the gateway node also and thereby make the entities vulnerable. Therefore, the main novelty of the proposed system is that gateway node is considered as an internal entity and is selected by the IoT devices along with the inclusion of security feature to incorporate secure communication system as shown in Figure 2.

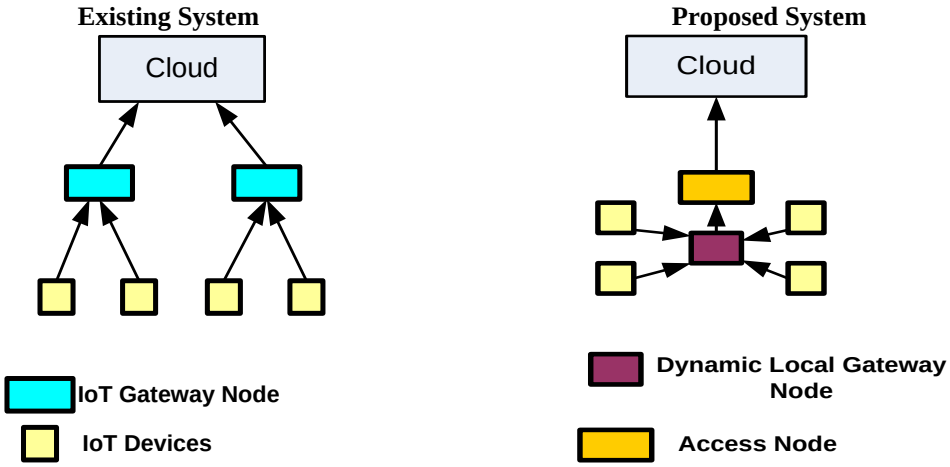


Figure 2. Novelty of proposed design scheme

2.1. System strategy

The primary strategy of the proposed system is to introduce the security protocol into two parts viz. i) performing authentication using Signature and ii) minimize computational complexity associated with operation. The secondary strategy is to perform authentication of all the data by jointly using the signature and key management scheme while making it lightweight operation by assuming a user-defined variable construct to be public keys. The tertiary strategy is to apply public encryption with an assurance that private key will be generated and is not required to be forwarded for decryption, which makes the process further lightweight as well as faster validation scheme. Apart from these strategies, the core strategy is carried out for further two operations viz. i) Operation-1: The first operation in the proposed system is associated with performing Authentication Using Signature (AUS). Here, the access node is configured followed by extraction of key and signing process of digital Signature for the transmitting nodes. ii) Operation-2: The second operation is associated with the offering of Security with Complexity Reduction (SCR), and it consists of similar steps of operation as that of Operation-1 with a difference of inclusion of performing signing operation in an active/passive mode of network. Figure 3 pictorially discusses the steps of operation in AUS and SCR.

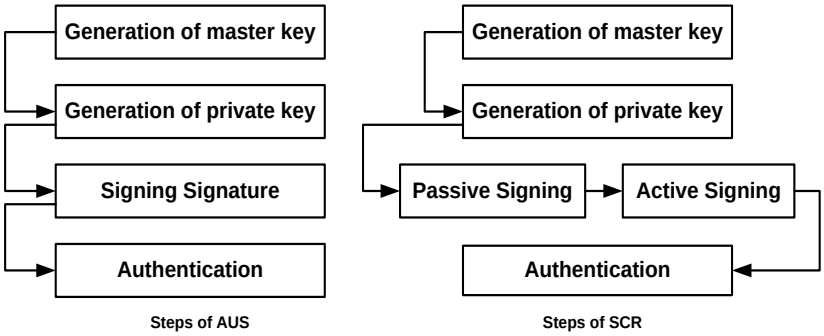


Figure 3. Flow of AUS and SCR

2.2. System implementation

The discussion of the system implementation is carried out with respect to core modules involved in the proposed system as follows:

2.2.1. AUS (authentication using signature)

The first phase of this module implementation is *initialization stage* where i) homomorphic encryption is applied in order to cipher the packet to be forwarded, ii) construct a generator for secret key using stochastical approach, iii) usage of simplified hashing operation, iv) selection of master secret key randomly, and v) performing preloading operation of all the system parameters. The second phase of this module implementation is *constructing secured & efficient keys* where the following operation takes place e.g., i) obtaining private key from the master matrix (from initialization step), ii) performing signing process of the digital Signature randomly, and iii) authentication on the basis of the time stamp to check the freshness of the obtained message. Upon finding the correct time, the IoT node performs the computation to find if the obtained message is originated from the legitimate user. The third and last phase of this module implementation is to perform *secure transmission of the packet*. Following are the sequence of the operation carried out in this implementation phase viz. i) the generation of the signal is carried out using time stamp T_1 (from leaf IoT node to access points) and user-defined information of the IoT node. In parallel, the internal communication of specific IoT domain is secured by generating Signature using different time stamp T_2 (from dynamic local IoT gateway node to access points). In this process, an embedded packet about the identity-information of the IoT node, a pseudonym, as well as updated T_2 information is transmitted by the accessnode to the IoT nodes. This information set will be utilized for performing a signing operation as well as performing authentication. The next step is to perform a computation of a dynamic threshold score which will be used as a decisive parameter if the IoT device to be selected to execute the role of the dynamic local gateway node. However, there is a criterion of choosing an IoT node to act as a dynamic local IoT gateway node. The proposed system compares the value of the dynamic threshold with the anticipated probability of an IoT node to become a dynamic local IoT gateway node. It the anticipated value is found less, the IoT node is declared to act the role of dynamic local IoT gateway node. An IoT node then transmits a beacon to the adjacent nodes where the beacon is appended with the digital signature. In the next step, an IoT node that chooses to act as a leaf node will now select its dynamic local IoT gateway node on the selection criteria of highest strength of signal associated with the beacon forwarded by the newly elected dynamic local IoT gateway node. In the next step, a dynamic local IoT gateway node transmits an instruction where the transmitted data should be further appended with digital Signature in next round of communication. This new instruction message includes provisioning of identity information of dynamic local IoT gateway node and T_1 information. After this phase of operation, the captured information from the IoT node is transmitted to the access node via a dynamic local IoT gateway node as shown in Figure 4.

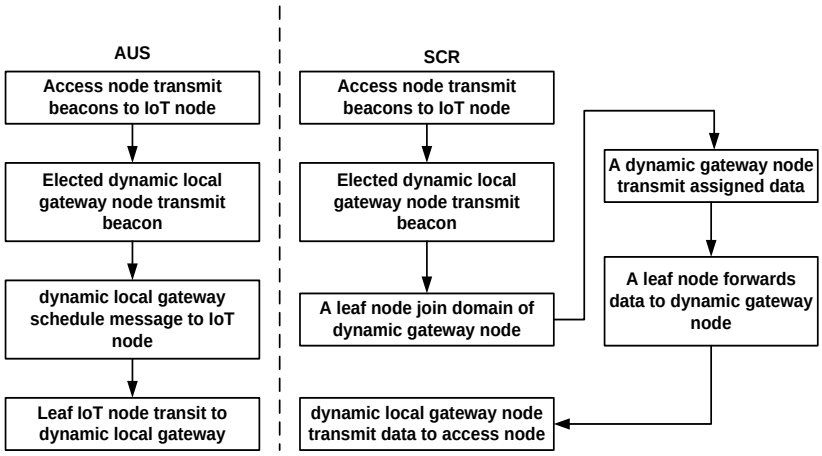


Figure 4. implementing authentication using signature

2.2.2. SCR (security with complexity reduction)

This is the second part of the implementation that is meant for minimizing the possible complexity that could arise owing to the inclusion of digital Signature. The process of SCR is nearly equivalent to that of AUS with a slight difference in the process of key management in SCR. Following are the steps of operation

viz. i) the first implementation is *initialization phase* which is same as that of AUS where an encryption key is generated followed by random generation of the secret key and hashing operation is applied on the top of it. ii) the second implementation is *constructing secured & efficient keys* which slightly different process happens as compared to AUS e.g., i) the first sub-operation is to obtaining private secret key prior to applying digital Signature, ii) the second sub-operation in SCR is very new where a *passive mode* of signing operation is introduced. According to this, an IoT node generates a random value along with instantaneous data and reposits it for the purpose of signing. This operation can be carried out only by IoT node or by access node only. iii) the third sub-operation in SCR is called an *active mode* of signing where a dynamic signature is computed by the IoT node on the basis of the ciphered data and Signature obtained in the prior sub-operation stage. The transmitting node then forwards the packet to the destination IoT device using this Signature of active mode, iv) this is the authentication step where all the received messages are subjected to authentication on the basis of the timestamp. Upon finding the correct timestamp, the IoT device (destination node) performs the computation to evaluate if the obtained data are legitimate or not. This is followed by forwarding the packet to the next IoT node and continues until it is upload over the cloud via an access point.

Algorithm for Authentication

Input: n (IoT nodes), a (geographical area of deployment), l_{ap} (location of access point), e (initial node energy), p (probability of local dynamic gateway)
Output: Sig (generated Signature)
Start
1. init n, a $l_{ap,}$ e, p
2. *mem* struc$\leftarrow m_{key}$
3. For i=1:n
4. (keys)$\rightarrow k_{gen}(m_{sk}, n_{prime})$
5. $\alpha=n_{nd}(\theta)$
6. select α with arg_{min}(dis)
7. $Sig_{gen}\rightarrow f(m, k)$
8. End
End

The proposed algorithm takes the input of n (IoT nodes), a (geographical area of deployment), lap (location of access point), e (initial node energy), p (probability of local dynamic gateway) which after processing yields the outcome of Sig (generated signature) that is basically used for authentication. The algorithm shows that after initialization of parameters is done (Line-1), it constructs a memory structure where the master key mkey is retained (Line-2). The proposed algorithm considers all the IoT nodes (Line-3) and executes its primary initialization of parameters for random key generation (Line-4). A function kgen is constructed that takes the input of master secret key msk and prime number nprime in order to generate private keys (Line-4). The proposed system then applies the concept of AUS, which performs a selection of dynamic local IoT gateway node where only the node which is non-draining of energy is considered nnd (Line-5). The process also considers a parameter θ is introduced for ensured the inclusion of eligible IoT gateway node dynamically. Finally, the best IoT gateway node is selected locally on the basis of minimum distance (Line-6). The next process is to generate the signature sig using an encryption function f(x) considering the input argument of message m and encryption keys k (Line-7). Similar steps are iterated for the SCR approach with the inclusion of the active and passive mode of operation. The complete algorithm of SCR works on compile time and perform autonomous election of dynamic local IoT gateway node, and it doesn't require any packet to be transmitted in order to obtain information. The similar process of incorporation of the digital Signature used in AUS is also used in SCR except with the exception of the inclusion of the active mode of signature generation. The final step of the algorithm performs forwarding of the data to the access node that finally user can access it via cloud services. Hence, the proposed system offers a cost-effective security algorithm which is highly non-recursive in its operation and yields faster generation of the secret key. Apart from this, the proposed system offers perfect data security while performing transmission. The next section discusses the result obtained.

3. RESULT ANALYSIS

As the proposed system introduces an authentication method where encryption mechanism using signature generation (AUS) and signature validation (SCR), therefore, it is anticipated that there could be a consumption of energy eventually. Therefore, the proposed system considers being benchmarked with certain energy efficient system of existing literature connected with IoT. We find the work carried out by

Shen et al. [33] has proven the best possible energy efficiency in IoT, and therefore, we are going to compare our authentication approach to find how much it offers better performance over current standards. In order to perform a comparative analysis, only the core approach of Shen et al. [33] has been utilized over the same test environment of the proposed system. The analysis was carried out over 100-500 IoT nodes, while scripting is carried out on MATLAB.

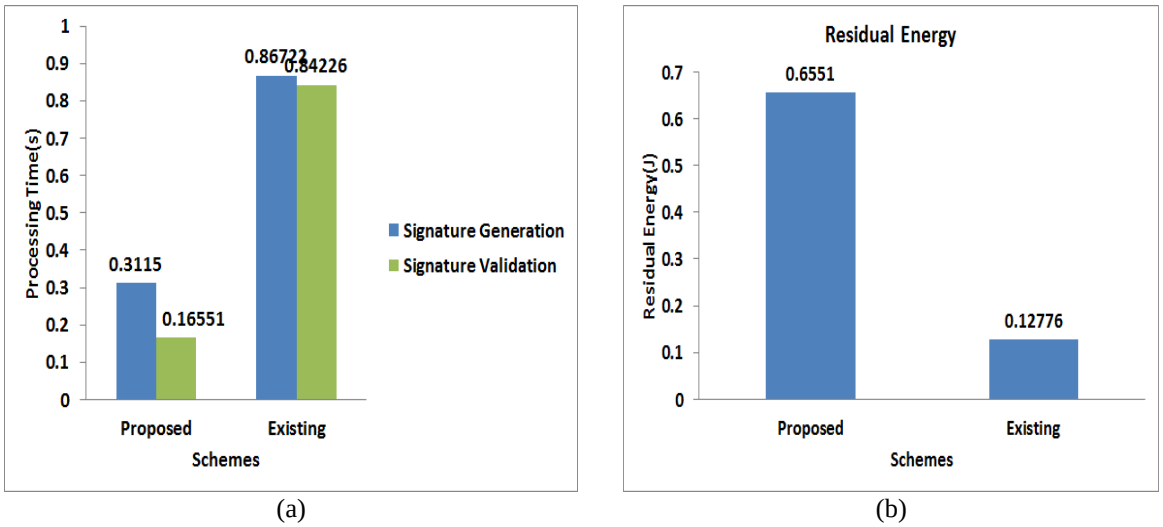
The inference of the obtained results is discussed as follows:

a. Security Performance Analysis

The proposed system is designed to resist different types of attacks e.g., wormhole attack, sinkhole attack, denial of service attacks, as well as physical attacks too. Irrespective of any types of attacks, the possibility of decrypting the ciphered message is not possible by any legitimate IoT nodes owing to the dependencies on authentication using digital Signature. Another interesting point is that usage of digital Signature has to be always computed, and there is no apriori information set in memory, and therefore, the Signature generated is highly secured, and its authentication policy (SCR) further gives proof of validation. Hence, it is not possible for an attacker to even gain even the encrypted data as the next module of authentication will fail the adversary as it will no have the model to compute the dependencies of validation model. Apart from this, we have not used any form of complex encryption usage for which reason; the processing time is found to be significantly low as compared with the existing system as shown in Figure 5(a). It can also be seen that the proposed system offer reduced time consumption to perform signature validation, and this protects the proposed system from a man-in-middle attack, also owing to faster response time.

b. Energy Performance Analysis

If a security algorithm is proven to be energy efficient that it can be claimed that it offers better network lifetime, which will directly contribute towards packet delivery performance too. It is essential that a maximum number of devices in IoT to retain maximum information as securing device-to-device connectivity will also require devices to have better resource availability. Hence, energy is a very important performance parameter. Normally, an IoT device consistently drain energy for two reasons viz. i) energy required for capturing, processing, and managing the data and ii) transmitting the data. The reason behind the fact that proposed system offers better energy conservation performance as because viz i) the proposed system is completely independent of location of IoT gateway as well as access node which is very much unlikely in existing system, and ii) the proposed system doesn't need to allocate maximum energy to perform processing of the data as the processing doesn't include complex cryptographic function. It will mean that the problem of performing a maximum number of processing over iterative steps in conventional cryptographic approach has been bypassed in the proposed system. Owing to this principle, the proposed system is found to offer energy efficiency as seen from the highest residual energy as shown in Figure 5(b).



(a) (b)

Figure 5. Comparative analysis (a) Processing time (b) Residual energy

4. CONCLUSION

The presented study has discussed that it is quite a difficult task to offer full-fledged security using a conventional mechanism of routing in IoT. It is because it neither offers security neither they are resource friendly. Moreover, the proposed study also discusses that replacement of existing communication technique by introducing an access node and different work principle of IoT nodes and devices could offer more comprehensive communication system to save energy. This, in turn, will support the workability of the encryption algorithm. Therefore, the contribution of the proposed system are as follows: i) in spite of forwarding the aggregated data from IoT nodes to static IoT gateway, the proposed system enables IoT nodes to dynamically select another IoT node to play the role of the gateway node. This principle offers good energy saving that is required to support encryption policy, ii) the proposed system introduces a novel authentication system using digital Signature where in spite of allocation static signature, the system chooses to generate it based on the traffic condition of the IoT nodes, and iii) the proposed system offers faster processing time as well as is energy efficient as compared to existing algorithms in IoT.

REFERENCES

[1] Qusay F. Hassan, *Internet of Things A to Z: Technologies and Applications*, John Wiley & Sons, 2018.
[2] Nasreddine Bouhaï, Imad Saleh, *Internet of Things: Evolutions and Innovations*, John wiley & sons, 2017.
[3] Mahboub, Aziz, El Mokhtar En-Naimi, Mounir Arioua, Hamid Barkouk, Younes El Assari, and Ahmed El Oualkadi. "An energy-efficient clustering protocol using fuzzy logic and network segmentation for heterogeneous WSN," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 4192-4203, 2019.
[4] Chetan, Rajani, and Ramesh Shahabadkar, "A comprehensive survey on exiting solution approaches towards security and privacy requirements of IoT," *International Journal of Electrical and Computer Engineering (IJECE)*," vol. 8, no. 4, pp. 2319, 2018.
[5] N. Vlajic and D. Zhou, "IoT as a Land of Opportunity for DDoS Hackers," *in Computer*, vol. 51, no. 7, pp. 26-34, Jul. 2018.
[6] T. Choudhury, A. Gupta, S. Pradhan, P. Kumar and Y. S. Rathore, "Privacy and Security of Cloud-Based Internet of Things (IoT)," *2017 3rd International Conference on Computational Intelligence and Networks (CINE)*, Odisha, pp. 40-45, 2017.
[7] J. Du, C. Jiang, E. Gelenbe, L. Xu, J. Li and Y. Ren, "Distributed Data Privacy Preservation in IoT Applications," *in IEEE Wireless Communications*, vol. 25, no. 6, pp. 68-76, Dec. 2018.
[8] C. Li and B. Palanisamy, "Privacy in Internet of Things: From Principles to Technologies," *in IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 488-505, Feb. 2019.
[9] Jeyanthi, N., and Thandeeswaran, R., "Security Breaches and Threat Prevention in the Internet of Things," *IGI Global*, 2017.
[10] M. A. M.Sadeeq, S. R. M. Zeebaree, R. Qashi, S. H. Ahmed and K. Jacksi, "Internet of Things Security: A Survey," *2018 International Conference on Advanced Science and Engineering (ICOASE)*, Duhok, pp. 162-166, 2018.
[11] Shamshekhar S. Patil, N. R. Sunitha, "Review of Research Approaches for Securing Communication in Internet of Things," *springer- Computer Science On-line Conference*, pp. 403-412, 2018.
[12] A. K. Das, M. Wazid, A. R. Yannam, J. J. P. C. Rodrigues and Y. Park, "Provably Secure ECC-Based Device Access Control and Key Agreement Protocol for IoT Environment," *in IEEE Access*, vol. 7, pp. 55382-55397, 2019.
[13] Z. Han, X. Li, K. Huang and Z. Feng, "A Software Defined Network-Based Security Assessment Framework for CloudIoT," *in IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1424-1434, Jun. 2018.
[14] F. Nizzi, T. Pecorella, F. Esposito, L. Pierucci and R. Fantacci, "IoT Security via Address Shuffling: The Easy Way," *in IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3764-3774, Apr. 2019.
[15] Ben Slimane, Yamina, and Khelifa Ben Ahmed, "Efficient End-to-End Secure Key Management Protocol for Internet of Things," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 6, pp. 3622-3631, 2017.
[16] D. Wang, B. Bai, K. Lei, W. Zhao, Y. Yang and Z. Han, "Enhancing Information Security via Physical Layer Approaches in Heterogeneous IoT With Multiple Access Mobile Edge Computing in Smart City," *in IEEE Access*, vol. 7, pp. 54508-54521, 2019.
[17] F. D. Hudson, "Enabling Trust and Security: TIPPSS for IoT," *in IT Professional*, vol. 20, no. 2, pp. 15-18, 2018.
[18] P. Hao, X. Wang and W. Shen, "A Collaborative PHY-Aided Technique for End-to-End IoT Device Authentication," *in IEEE Access*, vol. 6, pp. 42279-42293, 2018.
[19] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang and D. Chen, "Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security and Reputation Approach," *in IEEE Access*, vol. 7, pp. 9368-9383, 2019.
[20] K. R. Sollins, "IoT Big Data Security and Privacy Versus Innovation," *in IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1628-1635, Apr. 2019.
[21] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti and M. Jo, "Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks," *in IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 269-282, Feb. 2018.
[22] Y. Liu, Y. Kuang, Y. Xiao and G. Xu, "SDN-Based Data Transfer Security for Internet of Things," *in IEEE Internet of Things Journa*l, vol. 5, no. 1, pp. 257-268, Feb. 2018.
[23] García-Magariño, Iván, Raquel Lacuesta, and Jaime Lloret, "Agent-based simulation of smart beds with Internet-of-Things for exploring big data analytics," *IEEE Access*, vol. 6, pp. 366-379, 2018.

[24] Fortino, Giancarlo, Wilma Russo, Claudio Savaglio, Weiming Shen, and Mengchu Zhou, "Agent-oriented cooperative smart objects: From IoT system design to implementation," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 99, pp. 1-18, 2017.
[25] Gargees, Rasha S., and Grant J. Scott, "Dynamically Scalable Distributed Virtual Framework Based on Agents and Pub/Sub Pattern for IoT Media Data," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 599-613, 2019.
[26] Fortino, Giancarlo, Raffaele Gravina, Wilma Russo, and Claudio Savaglio. "Modeling and simulating Internet-of-Things systems: A hybrid agent-oriented approach," *Computing in Science & Engineering*, vol. 19, no. 5, pp. 68-76, 2017.
[27] Hsieh, Han-Chuan, Kai-Di Chang, Ling-Feng Wang, Jiann-Liang Chen, and Han-Chieh Chao, "ScriptIoT: A script framework for and internet-of-things applications," *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 628-636, 2015.
[28] Fortino, Giancarlo, Wilma Russo, Claudio Savaglio, Weiming Shen, and Mengchu Zhou, "Agent-oriented cooperative smart objects: From IoT system design to implementation," *IEEE Transactions on Systems*, Man, and Cybernetics: System, vol. 99, pp. 1-18, 2017.
[29] Gargees, Rasha S., and Grant J. Scott. "Dynamically Scalable Distributed Virtual Framework Based on Agents and Pub/Sub Pattern for IoT Media Data," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 599-613, 2019.
[30] Santos, João, Joel JPC Rodrigues, João Casal, Kashif Saleem, and Victor Denisov, "Intelligent personal assistants based on internet of things approaches," *IEEE Systems Journal*, vol. 12, no. 2, pp. 1793-1802, 2018.
[31] Hsieh, Han-Chuan, Kai-Di Chang, Ling-Feng Wang, Jiann-Liang Chen, and Han-Chieh Chao, "ScriptIoT: A script framework for and internet-of-things applications," *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 628-636, 2015.
[32] S. Patil, Shamshekhar and R. Sunitha, N., "A Novel, Lightweight, and Cost-Effective Mechanism to Secure the Sensor-Gateway Communication in IoT," *Cybernetics and Algorithms in Intelligent Systems*, pp. 403-412, 2019. 10.1007/978-3-319-91192-2_40.
[33] J. Shen, A. Wang, C. Wang, P. C. K. Hung and C. Lai, "An Efficient Centroid-Based Routing Protocol for Energy Management in WSN-Assisted IoT," *in IEEE Access*, vol. 5, pp. 18469-18479, 2017.

BIOGRAPHIES OF AUTHORS

Shamshekhar S. Patil received degree BE and M.Tech. in Computer Science & Engineering. He is research scholar under VTU Belgavi. He is working as Associate Professor in Dr. AIT Bangalore, Karnataka, India. Member of ISTE. His research interests include computer networks, Internet of Things security and sensor network security.

Dr. Arun Biradar received B.E., M.Tech., Ph.D. in Computer Science and Engineering. He is working as a Professor & Head, Department of Computer Science & Engineering, East West Institute of Technology, Bangalore, Karnataka, India. He has been published many papers in national and international journals & conferences. He is involved in organizing number of national and international conferences, workshops and other courses. He is a Member of ISTE, CSI and IEI. His main research interests are Wireless Ad-hoc Networks, Computer Networks, Genetic Algorithms, Software Engineering, IoT, Machine Learning, Cloud Computing.