International Journal of Electrical and Computer Engineering (IJECE)
Vol. 12, No. 3, June 2022, pp. 3298~3308
ISSN: 2088-8708, DOI: 10.11591/ijece.v12i3.pp3298-3308

A signature-based data security and authentication framework for internet of things applications

Nasreen Fathima[1], Reshma Banu[2], Guttur Fakruddin Ali Ahammed[3]
[1]Department of Computer Science and Engineering, ATME College of Engineering, Affiliated to Visvesvaraya Technological University, Belagavi, India
[2]Department of Information Science and Engineering, GSSS Institute of Engineering and Technology for Women, Mysuru, India
[3]Department of Computer Science Engineering, Visvesvaraya Technological University Post Graduate Centre, Mysuru, India

Article Info

Article history:

Received May 6, 2021
Revised Dec 20, 2021
Accepted Jan 11, 2022

Keywords:

Authentication
Digital signature
Encryption
Hashing
Internet of things
Public key

ABSTRACT

Internet of things (IoT) is the next big revolution in modernized network technologies connecting a massive number of heterogeneous smart appliances and physical objects. Owing to these technologies' novelty, various issues are characterized by security concerns are the most prioritized issue. A review of existing security approaches highlights that they are very particular about the solution towards a specific attack and cannot resist any unknown attacker. Therefore, this manuscript presents a novel computational model that introduces a unique authentication process using a simplified encryption strategy. The simulated study outcome shows that the proposed system offers efficient security and efficient data transmission performance in the presence of an unknown adversary. Hence, the study outcome exhibits better effects than frequently used security solutions when implemented in a vulnerable IoT environment.

Corresponding Author:

Nasreen Fathima
Department of Computer Science and Engineering, ATME College of Engineering, Affiliated to Visvesvaraya Technological University
VTU Main Rd, Visvesvaraya Technological University, Machhe, Belagavi, Karnataka 590018, India
Email: nasreen16fathima@gmail.com

1. INTRODUCTION

Internet of things (IoT) connects various physical objects using a sophisticated network chain [1]. An IoT is utilized in smart home appliances, elder-care, medical healthcare, transportation, vehicle-to-everything communication, home automation, and industrial application [2], [3]. However, with the massive connectivity of many heterogeneous devices and communication protocols, it is equally exposed to the highest degree of threat [4]. IoT's primary security attacks/issues are privacy, hardware issues, encryption of data, web interface, less network awareness, insecure software, side-channel attacks, and rogue IoT devices [5]. At present, various work is being carried out towards securing the communication system to resist multiple attacks [6]–[10], with each process having its advantages and limiting factors. Authentication is a standard method for ascertaining the legitimacy of any actor or event present within the communication area. The contribution of the proposed system is to formulate a proper authentication mechanism with an inclusion of critical practical constraints while performing data transmission in IoT. Different from existing approach, proposed system provides a significant balance in offering the algorithm's capability concerning the security and data transmission in IoT. The novelty of proposed system also resides in its authentication to offer enhanced scalability in its performance. Therefore, this paper contributes towards a novel computational model capable of performing secure authentication in IoT to resist a higher degree of threat and better resource retention within the resource-constrained IoT nodes. The paper's organization is section 1 discusses the study background and its problems.

The proposed solution followed by elaborating proposed method in section 2. The discussion of the obtained results is carried out in section 3. Finally, the conclusion is briefed in section 4.

Various works have been carried out towards a secure authentication mechanism in IoT [11]. Security is of utmost concern when it comes to using IoT in the automation system. Adopting a key agreement protocol using *public-key encryption* is proven to resist threats and use light-weight security operations [12]. Use of XOR function, concatenation, hashing, physically unclonable operation, elliptical curve encryption is reported to thwart common security intrusion. A study towards adopting a key agreement scheme independent of any verification table is showcased to offer light-weight authentication schemes [13]. The authentication process is strongly linked with access rights, which requires an explicit authentication scheme. In the paper, Xue *et al.* [14] have used a handover mechanism where the authentication is carried out by satellite making the operation quite faster. An authentication mechanism to strengthen the privacy factor is carried out by Lai *et al.* [15], which associates the secret key with a trusted server for boosting the privacy factor in IoT communication. IoT consists of static nodes and has mobile nodes, and authenticating mobile nodes is a complicated task. A study towards addressing such a problem is carried out by Zhang *et al.* [16], where authentication of vehicular nodes is carried out. Authentication of the message is carried out towards better privacy preservation, as seen in the work of Li *et al.* [17] and Vijayakumar *et al.* [18]. Furthermore, other studies towards similar privacy problems in authentication are carried out by Huang *et al.* [19], Hammi *et al.* [20], Shin *et al.* [21], Deeback *et al.* [22], and Zhang *et al.* [23]. Blockchain has been evolved as another robust security alternative for securing data and assisting in a better authentication process. Studies towards considering blockchain technology explicitly for authentication purpose is seen in the work [24]–[39]. The next section outlines research problems.

Various approaches are being carried out towards securing the communication addressing mainly authentication issues in an IoT. The associated problems in the existing system are: i) the existing studies have focused mainly on the encryption aspect while emphasizing effective resource utilization associated with resource-constrained IoT nodes; ii) the formation of the IoT nodes and its possible influence on the adversarial environment leading to the complex form of attacks are not addressed in existing studies; iii) adopting blockchain demands equal participation of servers for authentication, and it is highly centralized with less scalability over high-end deployment; iv) there is a lack of any studies which offer a simplified and cost-effective encryption approach. Usually, the encryption approach is quite iterative and leads to computational complexity; and v) existing security solutions are developed to address an intrusion's specific event, and hence its solution is not applicable when the means of attack are changed. Therefore, the existing solution offers less coverage towards maximum attacks in an IoT.

Different from any existing approaches that only focuses on security over predefined environment, the proposed system introduces a framework that can offer a robust authentication in the dynamic environment of an IoT. The present work extends our prior work that has introduced a computational model for securing the transmission between the sensor nodes and IoT using public-key encryption [40], [41]. This part of the implementation targets to evolve up with a scheme to offer resistivity against maximum threats. The proposed study considers two typical environments termed local and global IoT, where secure modeling is carried out. Each local IoT system consists of one specific application in a single domain. In contrast, all the local IoT system with heterogeneous communication schemes formulates together to generate a global IoT system. The global IoT system forms a centralized structure to facilitate communication. Hence, this environment defines a practical IoT deployment case and introduces various challenges to monitoring the security breach events in any one node residing within each domain; thereby defining an adversary environment unlike any existing system. From a practical perspective, all the data centers and sensors formed a local IoT system, while all the data centers' connectivity will create a global IoT system. The proposed method implements an authentication mechanism that helps secure all the actors involved in the communication of an IoT. The study uses a challenge and response to exchange information among the communicating nodes present within the environment. The model also incorporates both backward and forward secrecy towards the design of a light-weight encryption process. Figure 1 presents top-down architecture of proposed authentication mechanism where digital signature and key management plays a significant role. As a novel approach, the methodology presented is non-iterative.

The essential block of operation of the proposed system: i) local level of IoT: the proposed system considers a group of specific IoT devices that aggregates the data and forwards it to the datacenter. There is a different group in the simulation area where each group has a distinct underlying communication protocol of IoT. A specific IoT device is specifically elected within this communication group, which can take the data from other IoT devices and forward it to the gateway node. Such a node's election is carried out based on the highest level of resources within the IoT node. Hence, all the communication occurring within a single IoT node group is termed the given IoT environment's local level; ii) global level of IoT: each local level of IoT is required to be arranged effectively over an IoT environment to complete the process of data aggregation. The communication process is carried via a gateway node with all the aggregated data from the main collector IoT nodes from the local level and then forwards them to the data center's defined storage servers; and iii) data center: the proposed study considers the data center to collect various rack servers capable of distributed

storage. This module is connected to the gateway node via various network peripherals, e.g., switches and routers. All the incoming data are passed via a gateway node from normal IoT nodes and are stored in a distributed manner in this data center. Explicit metadata management and indexing mechanism are offered to ensure faster and accurate retrieval of data.

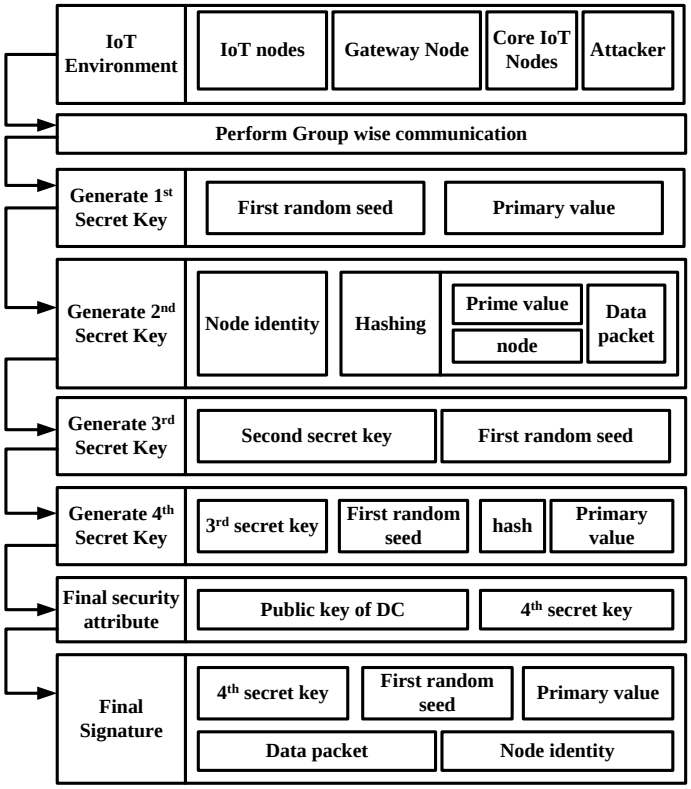

Figure 1. Proposed architecture of data security and authentication

All the operations mentioned above play a core role in carrying out communication. Owing to the possibilities of dynamic attacks of unknown types, the proposed system carries out this security operation mainly on the normal IoT nodes and then on the gateway node before disseminating and store the data over the distributed storage servers over the cloud environment, i.e., data center. The resource also plays an essential role in selecting the core IoT nodes that extract information from all the member nodes in a group. Only the nodes with higher residual energy are considered core IoT nodes, and hence the proposed system performs consistent monitoring of the nodes with higher residual resources. For security, the proposed system constructs a novel digital signature that is highly simplified in its operation. Unlike conventional public-key encryption, the proposed method performs the computation of both public key and private key. Another novelty of the proposed system is that the generated private key is subjected to four sequential rounds of the encoding process to develop a full backward and forward secrecy. A digital signature is caused by the proposed system used to sign the data to be forwarded to the destination node. Unlike an existing digital signature scheme, the proposed method does not have any extensive inclusion of the parameters. However, it only uses a simplified and smaller number of parameters, e.g., random seeds, multiple levels of the generation of secret keys, prime values, and a data packet. The design is carried out so that if attackers somehow bypass the protocol and capture the encoded data packet or the digital signature, they will not be capable enough to perform cryptanalysis to break the encoded data or the signed data packet. Simultaneously, the prime emphasis of the proposed system is to offer maximum resistivity from the maximum form of threats over an IoT environment. Finally, a verification process is carried out that assesses the data integrity using completely different conditions where the final secret key and excellent value's hash value is matched with the hash value of the 3rd level of secret key multiplied by the hash value of random seed of prime significance. Although this is a very simplified process, attackers will never retrace the encoding steps and can never access the dynamic data to attack. The following section discusses the algorithm implementation.

2. PROPOSED METHOD

The proposed system authenticates the legitimacy of the IoT nodes and gateway nodes and their data packets using a non-conventional public critical encryption method. The steps of the algorithm as shown in Figure 2. The algorithm uses a prime value *pv* considering two random seeds r_1 and r_2 (Line-2), considering all the IoT nodes *n* into consideration (Line-1). The proposed algorithm also finds a key authority, KA, which constructs two secret keys k_1 and k_2 (Line-3). The first secret key k_1 is carried out by multiplying the first random seed r_1 with prime value *pv* (Line-4). Unlike the conventional public-key encryption, where the public key is set as a default key, the proposed system computes the public key by multiplying the second random seed r_2 with prime value *pv* (Line-5). The proposed method also calculates the second secret key k2 where an explicit function $f_1(x)$ is applied over remaining IoT nodes, i.e. (i-*n*(id)) (Line-4), and it represents hashing operation. However, it does not use default hashing, but it generates hashing as $f_1(x)=pv\text{-}n(id)$. pkt. The generated second secret-key k_2 from Line-4 is further encoded to create the third secret-key k_3 (Line-6), where k_3 is the second secret key k_2 and first random seed r_1. Further encoding was carried out on this generated third secret key where the fourth secret key is generated by summing up third secret key k_3 and product of first random seed r_1, prime value *pv*, and hash *h* (Line-7). The algorithm then generates a signature s where a multiplicative function $f_2(x)$ is applied over the input arguments of data packet *pkt*, IoT nodes *n*(id), fourth secret key k_4, and product of first random seed r_1 with prime value *pv* (Line-8). Finally, the algorithm generates an ultimate secret attribute Tatt, a multiplicative function $f_2(x)$ of the newly computed public key of data center $pubkey_{DC}$ and fourth secret key k_4 (Line-9). This mechanism is used by the transmitting nodes where the data packets are signed before delivering it to the gateway node, and a similar principle is also applied for the gateway node when it wants to forward it to the data center. The proposed system also delivers the aggregated data using $Acc_{sig} \rightarrow (k_4, (r_1.pV), S)$ as the last encoding steps. A closer look into the entire algorithmic steps will show that it offers inter-dependency of multiple key parameters which offers higher degree of security as well as lower computational overhead owing to its progressive steps. This makes the algorithm feasible to be executed over resource-constrained IoT nodes with secure connectivity.

Algorithm for secure authentication of IoT nodes
Input: r_1/ r_2 (Random seeds)
Output: *flag* (notification message of secure connection)
Start
1. **For** i=1: *n*
2. *init*pv→(r_1, r_2)
3. KA→construct (k_1, k_2)
4. (k_1, k_2)→[(r_1.pv), f_1(1-n(id))]
5. $pubkey_{DC}$→(r_2.pv)
6. $k_3 \rightarrow k_2.r_1$
7. $k_4 \rightarrow k_3+(r_1.pv.h)$
8. S→f_2(pkt, *n*(id), k_4, (r_1. pv))
9. $T_{att} \rightarrow f_2(pubkey_{DC}, K_4)$
10. *flag*→secure *msg* communication.
11. **End**
End

Figure 2. Secure authentication of IoT nodes

3. RESULTS AND DISCUSSION

This section demonstrates the experimental results obtained from simulating the formulated mathematical expressions in a numerical computing environment. The study performed the entire workflow execution with mathematical computation in MATLAB. The simulation environment modeling, with parameters as shown in Table 1, depends on a system requirement with a minimum of 4 GB internal memory and a 1.2 GHz processing speed/clock frequency. It should be equipped with 64-bit Windows operating systems/x64-based processor architecture.

3.1. Simulation environment

The simulation environment for numerical framework modeling considers a comparison of different approaches to validate the performance of proposed approach which is now named as S-bAC. The simulation study is carried out for proposed approach S-bAC with both aggregation and un-aggregation test scenarios, and also the baseline approach of Challaet *et al.* [41] under two different conditions of aggregation and un-aggregation. The prime reason for the adoption of Challa *et al.* [41] is that 208 researchers adopt it as a standard implementation framework for secure data aggregation, which is higher than any existing standard

research work in similar topics. This is another set of novelty as majority of existing security approaches lacks comparisons. Table 1 highlights the experimental parameters used in proposed study.

Table 1. Experimental parameters for simulation

Simulation Parameters	Initialized Value
Number of IoT-devices (nIoT)	150
IoT: DC component placement coordinates (*x*,*y*)	(35,65)
Amount of Initial Energy for Activation of IoT-node in Joule	0.10
Number of IoT Gateway nodes	4
Maximum number iteration for workflow execution	500

3.2. Significance of accomplished result

The comparison of the formulated approach is performed with a baseline theoretical modeling of [41] concerning a performance metric consisting of two distinct parameters viz: i) outcome corresponds to the number of IoT-node that is no longer active with an increasing round of IoT communication cycle. That means that the number of IoT dead node computations with progressive communication cycle and ii) the assessment of remaining energy outcome into consideration with descriptive statistics computation. All the statistical effect corresponds to the simulation, and the behavioral outcome is further illustrated. It provides the reader much more insight into the trend of the variation for different performance metrics. To analyze the number of IoT dead nodes, the simulation in this phase of the study considers 80 rounds of the IoT communication cycle. The trend of the outcome is observed. The statistical mean, variance, and standard deviation trend are computed from that outcome, further discussed. Table 2 highlights mean computation of the numerical outcome obtained for dead IoT nodes for 4-different approaches viz: i) existing system with aggregation i.e., Agg [41], ii) proposed system with aggregation i.e., Agg-S-bAC, iii) existing system without aggregation i.e., UAgg [41], and iv) proposed system without aggregation i.e., UAgg-S-bAC.

Table 2. Numerical outcomes of statistical mean in comparative analysis-i

Approaches for Comparison	Quantified outcome of the Statistical Mean
Agg-Challaet *et al.* [41]	18.3750
Agg-S-bAC	12.3750
UAgg- Challaet *et al.* [41]	35.7500
UAgg- S-bAC	32.8750

The inferencing of the Table 2 shows that the maximum mean value is obtained in [41] when applied with the UAgg scenario. It shows that the number of dead nodes progressively increases with a growing communication cycle. Still, nodes start draining energy at early phases of communication, which is also happened in UAgg-S-bAC, where the mean value computed is 32.8750. However, in the case of Agg-Challaet [41] and Agg-S-bAC, the IoT nodes start deactivating themselves as a later phase when the IoT communication cycle reaches the 54^{th} round. However, among Agg [41] and Agg-S-bAC, Agg-S-bAC attains better performance outcomes means the node starts draining at further stages of the communication cycle. Agg-S-bAC outperforms Agg [41] and also other approaches to a greater extent.

Figure 3 shows the outcome of the statistical mean for both approaches. In the paper, Challa *et al.* [41] and S-bAC, both approaches are simulated under aggregation and un-aggregation conditions. It shows that Agg-S-bAC attains a minimum statistical mean value corresponding to IoT dead nodes that indicates that IoT nodes die with increasing rounds of communication cycle but at a slower pace. The mean computation values from the descriptive statistics viewpoint also show that it corresponds to the analysis of dead nodes, and here, the approach Agg-S-bAC attains better performance as due to the light-weight signature-based authentication schema it achieves considerable communication cost, which positively influences the energy performance of each IoT devices in both the local IoT and global IoT. Similarly, the study also performed a statistical variance assessment to check the S-bAC system's consistency while applied during the multi-hop data aggregation and aggregation phase. Table 3 highlights the statistical variance computation of the numerical outcome obtained for dead IoT nodes for 4-different approaches: Agg- [41], Agg-S-bAC, UAgg- [41], UAgg- S-bAC.

The result of the variance here indicates how far the data set corresponds to the outcome of IoT dead nodes spread out from the mean value. If the numerical value of variance is 0, then it indicates that all the data values are identical. Still, in the case of the proposed study, the highest value of variance corresponds to the number of IoT dead nodes found in UAgg [41] and the lowest value obtained for Agg-S-bAC. It shows that the outcome of Agg-S-bAC with the trend of the curve is closer to the mean statistical mean and do not indicate

data points are much more spread out over the curve of mean, which justifies that the Agg-S-bAC attains consistent data aggregation performance and chances of packet drops are also significantly lesser as each IoT node dies slowly with the progressive round of IoT communication cycle. Here the data points nearer to the mean indicate that the energy performance in the proposed S-bAC is relatively superior.

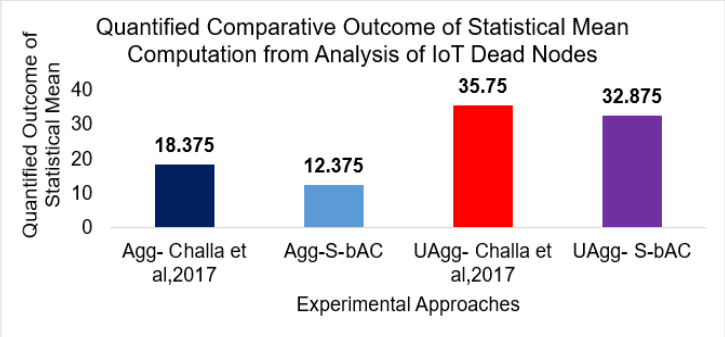

Figure 3. Visual outcome of the statistical mean computation for the number of IoT dead nodes

Table 3. Numerical outcomes of statistical variance in comparative analysis

Approaches for comparison	Quantified outcome of statistical variance
Agg- Challa *et al.* [41]	1.46e+03
Agg-S-bAC	837.6964
UAgg- Challa *et al.* [41]	3.13e+03
UAgg- S-bAC	2.84e+03

The visualization corresponds to statistical variance from the analysis of IoT dead nodes shown in Figure 4 with an extensive comparative study. It also shows that the existing approach of [41], while applied during the aggregation phase, also attains a better outcome of statistical variance, which marginally differs from the outcome of Agg-S-bAC. Here an overall analysis and interpretation show that Agg-S-bAC outperforms all the other approaches. Table 4 highlights standard deviation computation of the numerical outcome obtained for dead IoT nodes for 4-different approaches: Agg- [41], Agg-S-bAC, UAgg- [41], and UAgg- S-bAC.

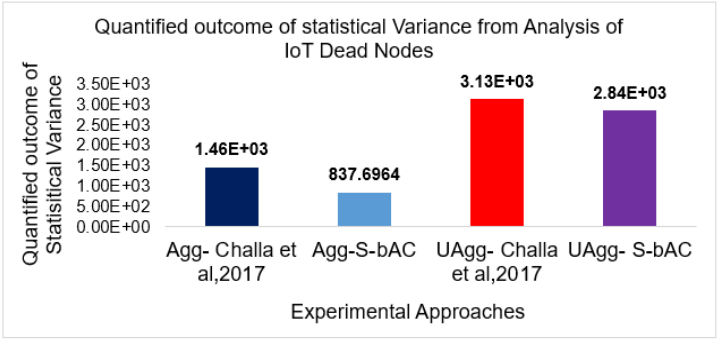

Figure 4. Visualization of statistical variance from analysis of dead IoT nodes w.r.t IoT communication cycle

Table 4 shows a comparative outcome among different approaches concerning the computed standard deviation. Here, standard deviation indicates how to spread out the data points corresponding to the IoT dead nodes are, and clear inferencing will reveal how the consistent performance of our proposed Agg-S-bAC and UAgg-S-bAC yields. The clear inferencing shows that the approach Agg-S-bAC attains superior data aggregation performance where the prime reason for accomplishing better data aggregation performance is that the formulated signature-based data authentication mechanism executes simplified steps and minimizes packet drops, leading to reducing the re-transmission counts. This, along with the simplified execution flow of

Agg-S-bAC, eventually resulted in better energy performance for which the IoT nodes die slowly and lately in the proposed concept. Whereas as already discussed above, in the context of variance, it is quite clear that a lower value of standard deviation indicates that data points are very close to the mean, which is found in the case of Agg-S-bAC whereas in both the techniques while applied for un-aggregation phase resulted in spread out of numerical values over the mean. It also indicates that the light-weight security mechanism of S-bAC accomplishes better security performance and enhanced energy performance.

Table 4. Numerical outcomes of standard deviation in comparative analysis

Approaches for comparison	The quantified outcome of standard deviation
Agg- [41]	3.82e+01
Agg-S-bAC	29.5584
UAgg- [41]	5.59e+01
UAgg- S-bAC	5.33e+01

The visual outcome of statistical standard deviation, as shown in Figure 5 shows that as compared to UAgg- [41], UAgg- S-bAC, both Agg-S-bAC and Agg- [41] resulted in the better and consistent outcome as in both the cases, IoT nodes slowly dies with increasing communication cycle. However, Agg-S-bAC attains superior performance among all. It incorporates the light-weight security mechanism and dynamic IoT gateway node election process, making the entire communication sustainable for a longer time in both local and global IoT communication scenarios. Table 5 highlights computation of the numerical outcome obtained for energy consumption for 4-different approaches: Agg- [41], Agg-S-bAC, UAgg- [41], UAgg- S-bAC.

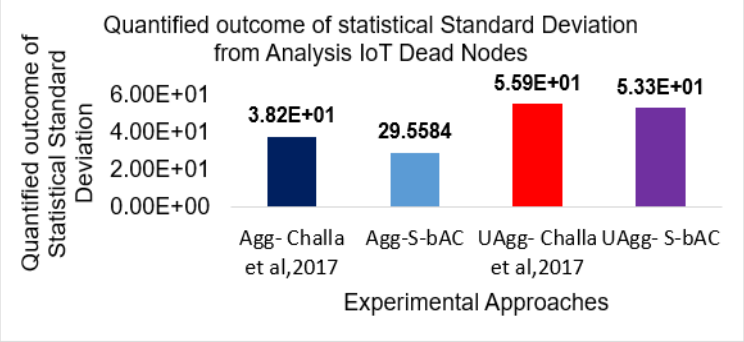

Figure 5. Visualization of statistical deviation from analysis of dead IoT nodes w.r.t IoT communication cycle

Table 5 shows the behavioral study of the different approaches for remaining energy performance corresponding to the statistical mean. In this case, also it can be seen that in the case of Agg-S-bAC, the remaining energy in each I-node is much more, whereas in the case of Agg- [41], the trend of remaining energy outcome marginally differs. However, both the approaches do not perform well while applied during the un-aggregation phases, as shown in Figure 6.

Figure 6 shows the visual outcome corresponds to the statistical mean computed from simulating the designed framework modeling for different execution workflow scenarios. As highlighted in Figure 4, it indicates that the light-weight execution workflow of S-bAC and the dynamic election of IoT gateway node has enhanced the energy-efficient data aggregation in Agg-S-bAC compared to the other experimental approaches. Table 6 highlights statistical variance computation of the numerical outcome obtained for Energy Consumption for 4-different approaches: Agg- [41], Agg-S-bAC, UAgg- [41], UAgg- S-bAC.

Table 5. Numerical outcomes of mean of energy in comparative analysis

Approaches for comparison	Quantified outcome of the statistical mean of energy
Agg- [41]	6.9639
Agg-S-bAC	7.1479
UAgg- [41]	6.2173
UAgg- S-bAC	6.3009

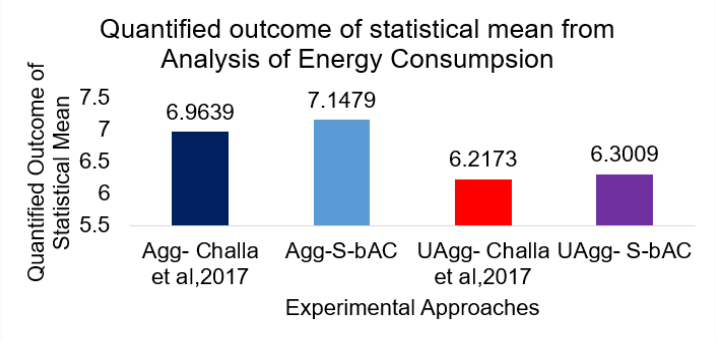

Figure 6. Visual outcome of the statistical mean computation for remaining energy of IoT-node

Table 6. Numerical outcomes of variance of energy in comparative analysis

Approaches for comparison	Quantified outcome of statistical variance of energy
Agg- [41]v	29.0117
Agg-S-bAC	27.7186
UAgg- [41]	31.1250
UAgg- S-bAC	30.7836

The analysis of statistical variance is also performed for four different types of approaches considering the formulated framework design where also it is observed that the trend of outcome corresponds to the remaining energy is relatively superior in the case of Agg-S-bAC among all the approaches, the prime reason behind the consistent performance is that the system converges towards secure data aggregation with the dynamic election of IoT gateway node which is energy efficient and do not generate much communication burden to the system.

Figure 7 shows the visual outcome of the statistical variance computation in this phase of the study, and the trend of outcome justifies that the proposed Agg-S-bAC outperforms all the other approaches not only with accomplishing high-level security requirements but also it attains better convergence solution with the dynamic election of IoT gateway node with a progressive round of communication cycle. Table 7 highlights standard deviation computation of the numerical outcome obtained for energy consumption for 4-different approaches: Agg- [41], Agg-S-bAC, UAgg- [41], UAgg- S-bAC.

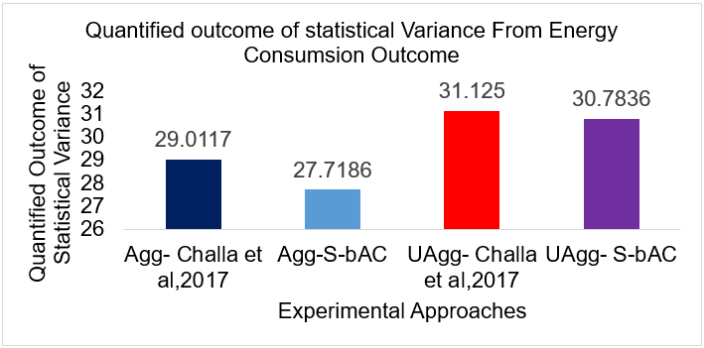

Figure 7. Visualization of statistical variance from the statistical analysis for energy consumption for 4-different approaches

Table 7. Numerical outcomes of standard deviation of energy in comparative analysis

Approaches for comparison	The quantified outcome of statistical standard deviation
Agg- [41]	5.3862
Agg-S-bAC	5.2649
UAgg- [41]	5.5790
UAgg- S-bAC	5.5483

The experimental analysis also further extended for computation and visualization of the outcome corresponds to the standard deviation where it can be seen that in both the cases of Agg- [41] and Agg-S-bAC, the numerical values obtained for standard deviation is 5.3862 and 5.2649, which indicates that the data points are not much spread out from the mean, on the other hand, which is relatively higher in the case of UAgg- [41] and UAgg- S-bAC. Thereby, it can also be claimed with the justification that the proposed approach Agg-S-bAC attains superior energy performance for low-cost operations of security implementation and ensures end-to-end data privacy in unknown adversaries in the context of both local and global IoT eco-system.

Figure 8 shows the standard deviation's visual outcome from the statistical analysis for the remaining energy computation for each IoT-Node. It clearly shows how the system performance of Agg-S-bAC ensures better energy performance with sustainable routing operations to a greater extent. Hence, it can be seen that proposed system offers a novel contribution towards evaluation process where statistical approach is used in comprehensive manner for assessing node performance when the proposed authentication algorithm is applied. Such approach of evaluation is not reported in existing studies and hence anticipates offering a better flexibility in framework construction in IoT.

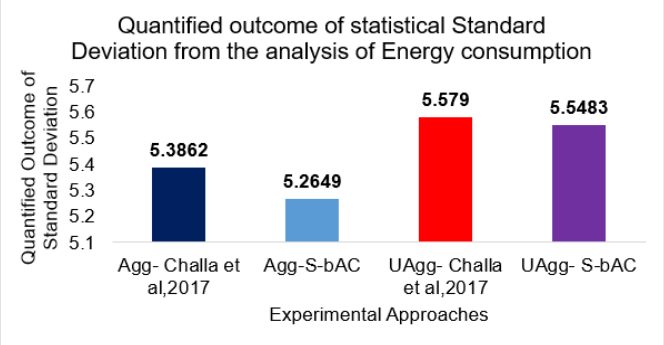

Figure 8. Visualization of standard deviation from the statistical analysis for energy consumption for 4-different approaches

4. CONCLUSION

This paper has discussed a novel signature-based secure authentication mechanism where a simplified encryption-based approach is used to validate the legitimacy of both IoT nodes and gateway nodes. The proposed system's novelty/contribution is: i) the proposed encryption method is characterized by less iteration and more progressive than any existing encryption method; ii) the proposed system retains a higher degree of resource retention in the presence of adversaries while performing security operations; iii) the proposed system's overall processing time is just 0.3765 seconds in the Core i3 processor. In comparison, the average of the existing system is 2.3998 seconds; and iv) the proposed system can resist most authentication and key-based attacks. The future work will be further towards optimizing the security operation for better security outcomes. Future work could be inclusion of more number of multiple attackers and dynamic threats present in communication environment. A strategically model can be further developed which is analyze malicious behavior on the basis of different resource attribute used in data transmission over an IoT.

REFERENCES

[1] K. Zhao and L. Ge, "A survey on the internet of things security," In *Ninth international conference on computational intelligence and security*, 2013, pp. 663-667, doi: 10.1109/CIS.2013.145.
[2] C. Valmohammadi, "Examining the perception of Iranian organizations on internet of things solutions and applications," *Industrial and Commercial Training*, vol. 48, no. 2, 2016, doi: 10.1108/ICT-07-2015-0045.
[3] K. K. Patel, S. M. Patel, and P. G. Scholar, "Internet of things-IoT: definition, characteristics, architecture, enabling technologies, application & future challenges," *International Journal of Engineering Science and Computing*, vol. 6, no. 5, 2016, doi: 10.4010/2016.1482.
[4] K. Gama, L. Touseau, and D. Donsez, "Combining heterogeneous service technologies for building an internet of things middleware," *Computer Communications*, vol. 35, no. 4, 2012, doi: 10.1016/j.comcom.2011.11.003.
[5] W. M. S. Stout and V. E. Urias, "Challenges to securing the internet of things," in *Proceedings - International Carnahan Conference on Security Technology*, 2016, vol. 0, doi: 10.1109/CCST.2016.7815675.
[6] S. L. Keoh, S. S. Kumar, and H. Tschofenig, "Securing the internet of things: A standardization perspective," *IEEE Internet of Things Journal*, vol. 1, no. 3, 2014, doi: 10.1109/JIOT.2014.2323395.
[7] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the internet of things," *Ad Hoc Networks*,

vol. 32, 2015, doi: 10.1016/j.adhoc.2015.01.006.
[8] M. Ammar, G. Russello, and B. Crispo, "Internet of things: a survey on the security of IoT frameworks," *Journal of Information Security and Applications*, vol. 38, 2018, doi: 10.1016/j.jisa.2017.11.002.
[9] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, 2017, doi: 10.1109/MIC.2017.37.
[10] L. Zhou and H. C. Chao, "Multimedia traffic security architecture for the internet of things," *IEEE Network*, vol. 25, no. 3, 2011, doi: 10.1109/MNET.2011.5772059.
[11] N. Fathima, R. Banu, and G. F. A. Ahammed, "An insight of existing research methods towards securing IoT communication system," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 9, no. 4, 2020, doi: 10.35940/ijitee.d1621.029420.
[12] S. Garg, K. Kaur, G. Kaddoum, and K. K. R. Choo, "Toward secure and provable authentication for internet of things: realizing industry 4.0," *IEEE Internet of Things Journal*, vol. 7, no. 5, 2020, doi: 10.1109/JIOT.2019.2942271.
[13] K. Park *et al.*, "LAKS-NVT: provably secure and lightweight authentication and key agreement scheme without verification table in medical internet of things," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3005592.
[14] K. Xue, W. Meng, S. Li, D. S. L. Wei, H. Zhou, and N. Yu, "A secure and efficient access and handover authentication protocol for internet of things in space information networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, 2019, doi: 10.1109/JIOT.2019.2902907.
[15] C. Lai, H. Li, X. Liang, R. Lu, K. Zhang, and X. Shen, "CPAL: A conditional privacy-preserving authentication with access linkability for roaming service," *IEEE Internet of Things Journal*, vol. 1, no. 1, 2014, doi: 10.1109/JIOT.2014.2306673.
[16] J. Zhang, H. Zhong, J. Cui, Y. Xu, and L. Liu, "An extensible and effective anonymous batch authentication scheme for smart vehicular networks," *IEEE Internet of Things Journal*, vol. 7, no. 4, 2020, doi: 10.1109/JIOT.2020.2970092.
[17] J. Li, Z. Zhang, L. Hui, and Z. Zhou, "A novel message authentication scheme with absolute privacy for the internet of things networks," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.2976161.
[18] P. Vijayakumar, M. S. Obaidat, M. Azees, S. H. Islam, and N. Kumar, "Efficient and secure anonymous authentication with location privacy for IoT-based WBANs," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, 2020, doi: 10.1109/TII.2019.2925071.
[19] P. Huang, L. Guo, M. Li, and Y. Fang, "Practical privacy-preserving ECG-based authentication for IoT-based healthcare," *IEEE Internet of Things Journal*, vol. 6, no. 5, 2019, doi: 10.1109/JIOT.2019.2929087.
[20] B. Hammi, A. Fayad, R. Khatoun, S. Zeadally, and Y. Begriche, "A lightweight ECC-based authentication scheme for internet of things (IoT)," *IEEE Systems Journal*, vol. 14, no. 3, 2020, doi: 10.1109/JSYST.2020.2970167.
[21] S. Shin and T. Kwon, "A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5G-integrated internet of things," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.2985719.
[22] B. D. Deebak, F. Al-Turjman, M. Aloqaily, and O. Alfandi, "An authentic-based privacy preservation protocol for smart e-healthcare systems in iot," *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2941575.
[23] X. Zhang, C. Liu, S. Poslad, and K. K. Chai, "A provable semi-outsourcing privacy preserving scheme for data transmission from IoT devices," *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2925403.
[24] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, and K. K. R. Choo, "HomeChain: a blockchain-based secure mutual authentication system for smart homes," *IEEE Internet of Things Journal*, vol. 7, no. 2, 2020, doi: 10.1109/JIOT.2019.2944400.
[25] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: a distributed and trusted authentication system," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, 2020, doi: 10.1109/TII.2019.2938001.
[26] Z. Cui *et al.*, "A hybrid blockchain-based identity authentication scheme for multi-WSN," *IEEE Transactions on Services Computing*, vol. 13, no. 2, 2020, doi: 10.1109/TSC.2020.2964537.
[27] A. Gauhar *et al.*, "XDBAuth: blockchain based cross domain authentication and authorization framework for internet of things," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.2982542.
[28] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. P. C. Rodrigues, and Y. Park, "BAKMP-IoMT: design of blockchain enabled authenticated key management protocol for internet of medical things deployment," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.2995917.
[29] W. Hu, Y. Hu, W. Yao, and H. Li, "A blockchain-based byzantine consensus algorithm for information authentication of the internet of vehicles," *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2941507.
[30] Y. Yao, X. Chang, J. Misic, V. B. Misic, and L. Li, "BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services," *IEEE Internet of Things Journal*, vol. 6, no. 2, 2019, doi: 10.1109/JIOT.2019.2892009.
[31] X. Wang, P. Zeng, N. Patterson, F. Jiang, and R. Doss, "An improved authentication scheme for internet of vehicles based on blockchain technology," *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2909004.
[32] F. Xie, H. Wen, J. Wu, S. Chen, W. Hou, and Y. Jiang, "Convolution based feature extraction for edge computing access authentication," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, 2020, doi: 10.1109/TNSE.2019.2957323.
[33] S. Chen *et al.*, "Radio frequency fingerprint-based intelligent mobile edge computing for internet of things authentication," *Sensors (Switzerland)*, vol. 19, no. 16, 2019, doi: 10.3390/s19163610.
[34] R. F. Liao *et al.*, "Security enhancement for mobile edge computing through physical layer authentication," *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2934122.
[35] Y. Chen *et al.*, "Clustering based physical-layer authentication in edge computing systems with asymmetric resources," *Sensors (Switzerland)*, vol. 19, no. 8, 2019, doi: 10.3390/s19081926.
[36] S. Chen *et al.*, "Internet of things based smart grids supported by intelligent edge computing," *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2920488.
[37] H. Song, J. Bai, Y. Yi, J. Wu, and L. Liu, "Artificial intelligence enabled internet of things: network architecture and spectrum access," *IEEE Computational Intelligence Magazine*, vol. 15, no. 1, 2020, doi: 10.1109/MCI.2019.2954643.
[38] J. Wu, S. Guo, H. Huang, W. Liu, and Y. Xiang, "Information and communications technologies for sustainable development goals: State-of-the-art, needs and perspectives," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 3, 2018, doi: 10.1109/COMST.2018.2812301.
[39] R. Atat, L. Liu, J. Wu, G. Li, C. Ye, and Y. Yang, "Big data meet cyber-physical systems: a panoramic survey," *IEEE Access*, vol. 6, 2018, doi: 10.1109/ACCESS.2018.2878681.
[40] N. Fathima, R. Banu, and G. F. A. Ahammed, "Modeling of secure communication in internet-of-things for resisting potential intrusion," in *Advances in Intelligent Systems and Computing*, 2019, vol. 1047, doi: 10.1007/978-3-030-31362-3_38.
[41] S. Challa *et al.*, "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, 2017, doi: 10.1109/ACCESS.2017.2676119.

BIOGRAPHIES OF AUTHORS

Nasreen Fathima received Ph.D. degree from Visvesvaraya Technological University, Belagavi, India in 2022. She has 17 years of teaching experience. She is currently working as Assistant Professor in the Department of Computer Science and Engineering at the Academy for Technological & Management Excellence College of Engineering, Mysuru, India. Her research areas are wireless networks and the Internet of Things. She has published four papers in International Conference, five papers in International Journal, and five papers in National Conference. She can be contacted at email: nasreen16fathima@gmail.com.

Reshma Banu Professor and HOD, ISE Dept at GSSSIETW, Mysuru. Has 19 yrs of Teaching and Research Experience. Won Best HOD of the year by CSI, Best Paper Award at CSI National Level, Best Accredited Student Branch" by CSI 2017, 2018 and 2019. Young Scientist Award from AUFAU, VIRA-2016. Delivered talks/guest lectures organized National competitions talk/Workshop/Conferences/FDP/session/Seminar/student convention. Received Fund for Best Projects Received VGST Grant, Karnataka, SMYSR. Fund by VTU TEQIP 1.3 in 2020.Organizing/Publication Chair for 5 IEEE International Conference on Electrical Electronics Communication Computer Technologies & Optimization Techniques 2016-2019 & 2021. Senior IEEE member, Session Chair/Reviewer for National/International conferences. Editorial Board member for various Journals. She can be contacted at email: reshma127banu@gmail.com.

Guttur Fakruddin Ali Ahammed received Ph.D. degree from Sri Krishna Devaraya University, Anantapur (A.P) in 2011. Presently he is guiding six Ph.D. scholars. He has 17 years of Academic, Research and Administrative experience and has published more than fifty research papers in National, International Journals and Conferences. He is currently working as an Associate Professor, in the Department of Computer Science & Engineering at VTU Centre for Post Graduate Study, Mysuru. He can be contacted at email: aliahammed78@gmail.com.