# A Novel and Integrated Architecture for Securing Communication in IoT

**Shamshekhar S. Patil, Arun Biradar**

***Abstract:** Although the IoT opens the door to endless possibilities, but it is also associated with many risks because all devices connected to the internet involve the use of data points. Therefore, it is essential to ensure IoT security and privacy. A review of existing research works highlights the usage of traditional security scheme based on cryptography for data transmission among IoT nodes and gateways. The proposed system proposes an integrated model that combines lightweight encryption technique with robust and cost-efficient authentication mechanism. The proposed system introduces digital signature-based authentication and complexity minimization in order to resist the involvement of any kind of unknown attacks. The simulation outcome of this model exhibits reliable security, faster response times and energy savings for IoT nodes.*

**Keywords***: Internet-of-Things, Security, Authentication, Encryption, Sensors, gateway*

## I. INTRODUCTION

The Internet has become a primary choice for many people to perform their work according to their own needs. People not rely on the Internet to share content, but they can also use the Internet for entertainment purposes, effectively accomplishing tasks and meeting their needs without relying on time and particular geographic locations. Another area is evolving due to the advantages of the Internet, which enables objects-(things) and machines to be interconnected and communicate over the Internet called the Internet of Things (IoT)[1-2]. The IoT ecosystem is a collection of smart (capability of storage and processing)-electronic devices that are interconnected by the Internet to provide efficient services to end-users. The core concept of the IoT is to automate the work that people use in their daily lives. The smart electronic devices are subjected to an object that has specific sensors engaged to it to sense and collect information from the physical world [3]. The information is stored at the local storage hub is then forwarded to cloud storage. Finally, authorized people use that information to take suitable and applicable actions. There are many applications like health care, home automation, transportation, infrastructure management, agriculture, and many more in which the concept of IoT has deployed that become smart and automate their work with the help of the Internet [4-5]. Applications supported by the IoTs typically handle sensitive data. Therefore, protecting such data from tampering, illegal disclosure, and protection from other security and privacy attacks is a significant concern for everyone. Since the functionality of IoT is highly dependent on the Internet and data that are shared over the Internet are quite vulnerable to many attackers on the Internet [6-7]. Therefore, data security and its privacy are the most important issues in the development of IoT. In addition, the IoT is vulnerable to well-known security attacks such as a denial of service (DoS), Man in the Middle-(MIM) attacks, cloning attacks, eavesdropping attacks, and routing attacks [8]. Many researchers and developers around the world are working hard to address various security issues associated with the IoT ecosystem [9]. However, ensuring adequate security in IoT-ecosystem is a challenging task due to the heterogeneity of the IoT. The IoTs is a fusion of different technologies that all have their own security and privacy flaws that need to be addressed in the underlying architecture of IoT. In addition, IoT devices are resource-constrained, and traditional cryptographic oriented security solutions cannot be implemented to such devices because performing the complex cryptographic operations can consume the whole energy of such constraint nodes. Also, such implementation operation can have a severe impact on the performance of both data transmission and security mechanisms, which makes them prone to information integrity and confidentiality associated issues [10]. Therefore, there is an urgent need to develop an efficient security protocol to provide identical security strength in the IoT ecosystem. Therefore, the proposed study aims to design an analytical model using a lightweight encryption technique and an efficient authentication operation, which is responsible for introducing a novel mechanism that provides secure communication without using much energy resources. The remaining part of this paper is arranged as follows: Section II discusses the existing literature where different techniques are discussed for IoT security. Section III illustrates research problem based on the review of literature. Section IV presents system design. Section V presents algorithm description. Section VI presents result of the proposed methodology and finally the conclusion of proposed system is presented in Section VII.

## II. LITERATURE SURVEY

This section presents a review of existing research methods towards securing the Internet of Things-(IoT). Shi et al. [11] focused on the encryption technique for executing signcryption operation and digital signatures.

**Revised Manuscript Received on December 30, 2019.**
***** Correspondence Author

**Shamshekhar S. Patil***, Associate Professor, Department of Computer Science & Engineering, Dr. AIT, Bengaluru, India. Email: shamshekhar.patil@dr-ait.org

**Arun Biradar,** Professor & Head, Department of Computer Science Engineering, East West Institute of Technology, Bengaluru, India.

This approach shows its effectiveness because it does not allow IoT-devices to disclose the confidentiality of data-packets and privacy of communication link information in the IoT system. The work done by Dao et al. [12], have tried to solve the problem associated with key management and agreement using special features and attributes from the social networks. The study of Das et al. [13], have adopted the concept of elliptic curve cryptography-(ECC) to enable access control mechanism in an IoT ecosystem. An extensive discussion about physical layer security is given in the study of Wang et al. [14] to achieve precise levels of confidentiality and improved adaptability to network changes. The study of Arshad et al. [15] introduced an approach for green IoT implementation for minimizing the energy consumption of equipment using the IoT and for maintaining environmental security. The study has discussed policies, common architecture, and recyclable materials of IoT. Wazid et al. [16] studied about the security approaches and presented a key management-oriented scheme to encourage autonomous evaluation of security strength. The work done by Santos et al. [17], have conducted an extensive analysis about software agents incorporated with intelligence mechanism. The study of Cheng et al. [18] studied the mobility functions and methods in the communications field that are limited by malware propagation, taking advantage of the new challenges associated with cyber security of IoT. Ransomware and its impact on IoT is investigated in the study of Yaqoob et al. [19]. The study has classified objective of ransomware, i.e. Crypto, Locker and Hybrid. Several infiltration techniques are presented and discussed, considering multiple attributes like botnets, social engineering, and IoT equipment as attack vector to launch malware into protected building. Zhou et al. [20] carried investigational analysis on network security and its impact on IoT. In this, the authors have introduced IoT function that included a unique set of features from IoT and differentiated it from other computing systems. These features can help developers to enhance the security and privacy flaws of IoT systems. There are various existing surveys and investigational analysis on security and privacy issues in the IoT eco-system. The work of Liu et al. [21] carried an extensive analysis on performance of routing based approach in large sensor networks. Here, the authors have reviewed the fundamental principal of routing and its control messages. The study of Fu et al. [22] focused on the opportunities and potential threats in special types of IoT-assisted application i.e. homes and hospitals. Similarly, the work of Roman et al. [23] carried an analysis highlighted various research challenges associated with security. Also the study has suggested possible solutions oriented on authentication, access control, and cryptographic based approaches. Wallgren et al. [24] conducted an extensive analysis of many routing attacks and compared their strength against such attack. Also, the authors have enhanced their survey work using a heartbeat technique to eliminate selective forwarding attacks. However, the presented work only discussed attacks that are totally associated with WSN. In addition, the study has not illustrated detailed information on mitigation methods. The authors of [25] have carried a survey on the location-based security issues in the IoT. A brief review of routing attacks and 6LoWPAN layers is conducted in the study of Pongle and Chavan in [26]. The study also discussed the various intrusion detection systems to eliminate routing associated security attacks. However, the authors have presented a brief discussion of the mitigation techniques, and it does not suggest current and novel recommendations. The study of Ngu et al. [27] mainly concentrated on security issues associated with IoT middleware and conducted a detailed review of the existing security mechanisms and their issues related. Patil, and Sunitha [28-29] also worked for introducing novel authentication mechanism with robust privacy preservation for IoT communication system. In this the authors have discussed about various attacks and their solutions. A comprehensive survey on routing security is offered by Airehrour et al. [30], and also, the authors here studied various reliable techniques used to reduce the possibility of routing attacks. However, the security discussed here is mostly suitable for WSNs, not for the IoT system. Another work by Alaba et al. [31] is subjected to routing attacks, but in this, the authors have not specifically discussed the different classes of attacks launched on the routing operation in the network. The study of Yang et al. [32] carried a review analysis on the existing previous surveys work, and based on that, the authors have explicitly classified different kinds of attacks in IoT infrastructure. In this, the study has described various aspects of research in IoT security, including security risks, threats, and unresolved issues, and also suggested some beneficial key points to support future research work.

## III. Research Problem

The following are the research problem associated with IoT security and privacy issues.

- Most of the existing security approaches for the IoT system are formulated according to the particular context of IoT infrastructure. The impact of attacks and security threats is mostly different in wireless sensor networks (WSN), and it has been observed that very few studies have investigated their impact over the Internet assisted communication system.
- Various existing schemes are found to be highly recursive, which is not practical to implement in energy constraints nodes. Therefore, this will result in an excessive reduction in resources from the sensor node, causing both communication and security standards to deteriorate.
- The use of advanced and complex cryptographic based security techniques is much greater in the existing studies without much focuses on lightweight-based security mechanisms.

Existing methods for data transmission to a particular IoT gateway generally associated with traffic management issues, energy efficiency issues, and complexity issues.

Hence, the problem statement for proposed study can be expressed as "*It is a challenging task to introduce an efficient computing framework in which an enhanced and powerful authentication mechanism can be built to provide top-level confidentiality in the IoT communication system*."

## IV. Proposed System

The proposed research work introduces an integration framework that is responsible for providing secure communication, and a strong authentication mechanism for IoT assisted applications.

The main motive of the proposed system is to guarantee that no illegal node or participants in the IoT ecosystem can participate in the operation of the data distribution and communication process.

The proposed implementation is conducted using an analytical approach that progressively provides efficient security mechanisms and consistent communication between wireless nodes and IoT gateway nodes. A schematic of the proposed system is illustrated in Figure 1. The overall design of the proposed system is built-in in a dual layer of security implementation.

The first layer of the implementation module presents a new mechanism for bootstrapping public keys, after registering sensor nodes within the IoT gateway. In this, elliptical curve cryptography (ECC) is adopted to constructing keys on the basis of secret key installation, which executes encryption operation using the concept of a low-complex hashing mechanism. After the security key is installed with the gateway node and with all its member nodes, then a reliable grouping is established to assign the valid node to the gateway node. The proposed system is also built to take into account the movement of sensor nodes to evaluate dynamic scenarios and has the potential for supporting rapid secret key updates.

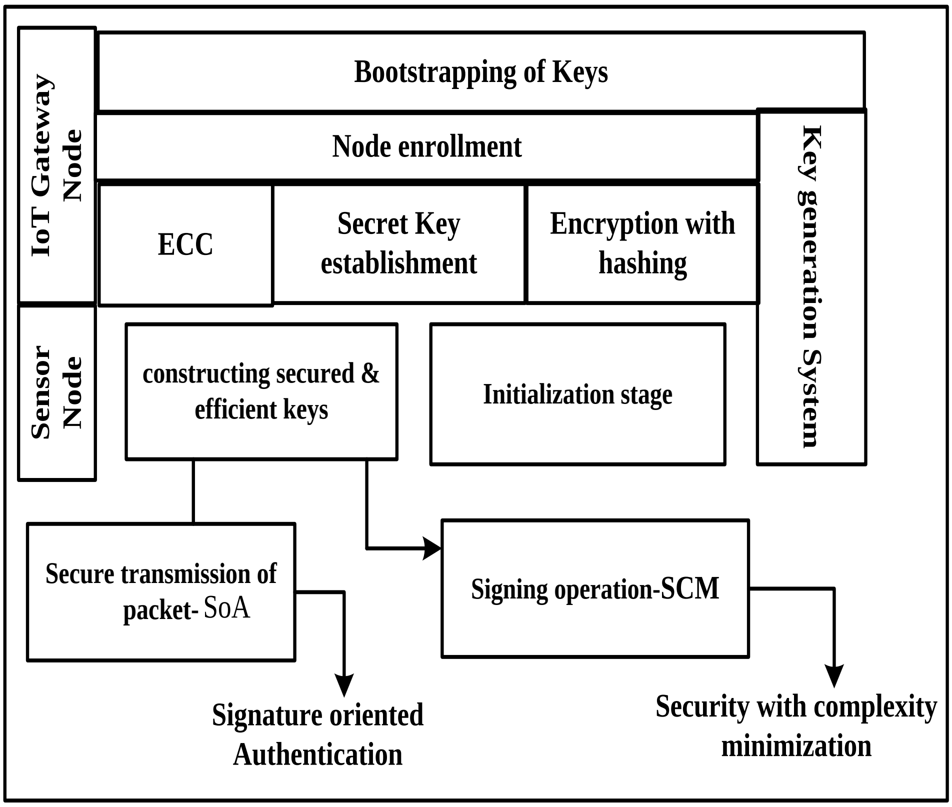


**Fig.1 Proposed system**

The second layer of the implementation module is responsible for enabling a secure authentication system, with a novel energy-efficient mechanism for communication operation from IoT nodes. The proposed system uses Signature oriented Authentication-(SoA) and Security with Complexity minimization-(SCM). In SoA, a digital signature is generated, where an initialization process is subject to homomorphic encryption over the packet to be transmitted. Further, the secret key constructor is built using a stochastical method, where the master secret key is chosen in a random manner to generate the private key. The next operation is responsible for creating secure and efficient keys based on the private key acquired from the master matrix. The proposed system then performs an authentication process based on the timestamp to validate the integrity of the acquired message. Once the correct time is found, the IoT node will perform a calculation to estimate if the acquired message is originated from a valid user or not.

The SCM is responsible for performing authentication over the generated messages, primarily to minimize the complexity that may be caused by the addition of digital signatures. The initial operation of SCM is nearly the similar as SoA, but the key management process in SCM is little different. In this system, a secure and efficient key is constructed by acquiring a private key before a digital signature is applied, and the IoT node calculates the dynamic signature based on the encrypted data and signature obtained in previous operations. Also, the authentication operation is performed over the received messages based on the timestamp, after which the destination IoT node performs a calculation to estimate if the received data is valid or not. The packet is then forwarded to the next IoT node and continues till it uploaded to the cloud through the access point. The next section presents the algorithm description for the proposed security implementation.

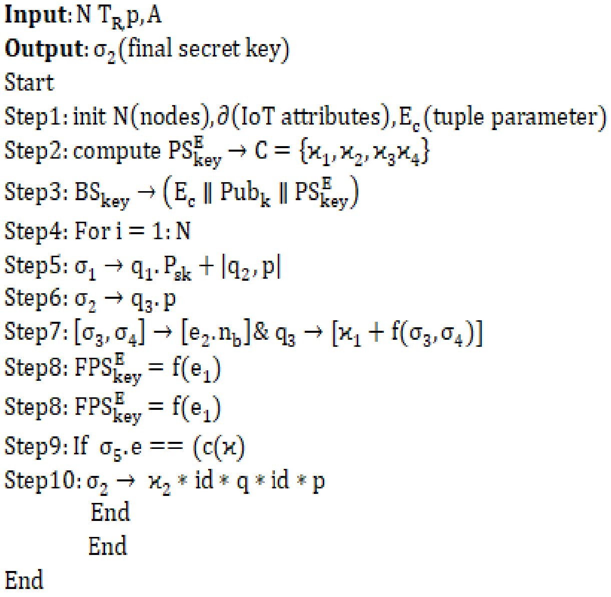
## V. Algorithm Description

The proposed system recognizes the strengths of using a digital signature, that offers rapid security validations and cost-aware implementation where the framework is primarily comprised of multi-level stages that constructs unique keys in an efficient way that even if any key is tempered by malicious user, then the malicious user can never be able to decrypt.

Another peculiarity of the proposed system is that it provides energy saving mechanism using concept that dynamically selects local gateway nodes, which is different form the existing systems where IoT devices send messages directly to the IoT gateway.

### i) Algorithm for secret key generation

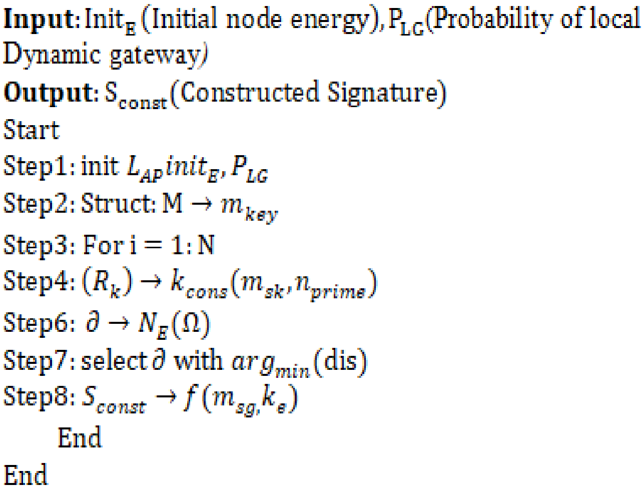
This algorithm is executed within the gateway node which is responsible for generating secret key. The steps involved in the proposed algorithm are as follows:



```
Input: N T_R, p, A
Output: $\sigma_2$(final secret key)
Start
Step1: init N(nodes), $\partial$(IoT attributes), $E_c$(tuple parameter)
Step2: compute $PS_{key}^{E} \rightarrow C = \{\varkappa_1, \varkappa_2, \varkappa_3 \varkappa_4\}$
Step3: $BS_{key} \rightarrow (E_c \parallel Pub_k \parallel PS_{key}^{E})$
Step4: For i = 1: N
Step5: $\sigma_1 \rightarrow q_1 . P_{sk} + |q_2, p|$
Step6: $\sigma_2 \rightarrow q_3 . p$
Step7: $[\sigma_3, \sigma_4] \rightarrow [e_2 . n_b] \& q_3 \rightarrow [\varkappa_1 + f(\sigma_3, \sigma_4)]$
Step8: $FPS_{key}^{E} = f(e_1)$
Step8: $FPS_{key}^{E} = f(e_1)$
Step9: If $\sigma_5 . e == (c(\varkappa)$
Step10: $\sigma_2 \rightarrow \varkappa_2 * id * q * id * p$
            End
            End
End
```

This algorithm is executed within the gateway node, which is responsible for producing a new form of initial secret key. The algorithm takes input as N-(number of nodes), A( Deployment area) $T_R$-(Transmission range), and P-(prime number). The algorithm considers an IoT attribute of variable $\partial$ as a set of various protocols accomplished by the gateway node (Step-1). Since the proposed system adopts concept of ECC, therefore, it calculates a set of prime numbers-(p) that begin from $2^{\partial}$ to 0. The system also makes use of ECC tuple parameter $E_c$ which is a component of multiple unit finite field attribute on the ECC curve. The proposed system uses the private key $P_k$ to calculate the public key $Pub_k$. In the next step, $\varkappa_1$, $\varkappa_2$, $\varkappa_3$, and $\varkappa_4$ are treated as elements of the matrix C (Step 2), forming an encrypted pass key $PS_{key}{}^{E}$. Finally, the algorithm generates the bootstrap key $BS_{key}$ based on $E_c$, $Pub_k$, and $PS_{key}{}^{E}$ (Step 3). The next step is subjected to perform secret key generation, where the algorithm considers all nodes N (step 4) and obtains node location information. Then it calculates the temporary variable id by multiplying the unique identifier $u_i$ by $e_4$. Then after $\sigma_1$ is generated as first security token (step5), where variable $q_1$ is subjected to scalar product of the unique node identifier, $\varkappa_1$, $e_4$ and $P_{sk}$-(public secret key), while variable $q_2$ is subjected to scalar product of the unique node identifier with low processing capability p. Another security token is produced by the scalar product of $q_3$ and node with less computing capacity (step5). The system also calculates the other three security tokens $\sigma_3$, $\sigma_4$ and $\sigma_5$ (step7)). The final encrypted pass key $FPS_{key}{}^{E}$ is constructed using function f(x) which is subjected to $\varkappa_3$ * id * $k_2$ * $\boldsymbol{\sigma_1}$ * $k_3$ * $k_4$ * p (step8) where k is a random variables. A condition is established(step9) to construct final secret key, if there is event of matching two dissimilar keys generated by the gateway node and the sensor node (line 10). The algorithm efficiently sustains good layers of protection and therefore provides global privacy.

### ii) Algorithm for Authentication



```
Input: $Init_E$ (Initial node energy), $P_{LG}$(Probability of local
Dynamic gateway)
Output: $S_{const}$(Constructed Signature)
Start
Step1: init $L_{AP} init_E, P_{LG}$
Step2: Struct: $M \rightarrow m_{key}$
Step3: For i = 1: N
Step4: $(R_k) \rightarrow k_{cons}(m_{sk}, n_{prime})$
Step6: $\partial \rightarrow N_E(\Omega)$
Step7: select $\partial$ with $arg_{min}$(dis)
Step8: $S_{const} \rightarrow f(m_{sg,} k_e)$
      End
End
```

This algorithm takes input as $L_{AP}$ (location of the access point), $Init_E$ (initial node energy), and $p_{LG}$ (probability of the local dynamic gateway). After executing all steps it will generate signature which is mainly subjected to the authentication mechanism. The first stage of the algorithm is subject to the initialization of parameters (step-1). In the next step a memory structure is created to recall the master key (step2). The proposed algorithm takes into account all IoT nodes-(N) (step3) and performs its initial step of parameter initialization to generate a random key-( $R_k$) (line 4). The constructor $k_{cons}$ accepts the input of the master key ($m_{key}$) and the prime number P to generate the private key (line 4). The proposed system then adopts the concept of SoA, which implements the selection of dynamic local IoT gateway nodes, where the nodes with sufficient energy are considered $n_E$ (step 5). This operation also considers a parameter $\Omega$ to confirm that the qualified IoT gateway node is dynamically included. Finally, the optimal IoT gateway node is chosen locally according to the minimum distance (Step 6). The next step considers the input parameters of the message $m_{sg}$ and the encryption key $k_e$ (line 7), to produce the signature sig using the encryption function f(x). For the SCM method, similar steps are repeated, considering active and passive operation. The SCM mechanism executes at compile time and automatically selects the dynamic local IoT gateway node without performing transmission of unnecessary data packets to get the information. In addition to the active mode that includes signature generation, a similar process to the digital signature used in SoA is used in the SCM. The final step transmits the data through access node, by which the end user can access it through the cloud service. The next section presents outcome of the proposed system to validate its effectiveness and scope for proving efficient security in IoT ecosystem.

## VI. RESULT

This section presents the result of the proposed methodology, followed by the comparative analysis.

The implementation and strategy of the proposed integrated system is carried on a numerical computing tool installed on windows 10, 64 bit. The proposed study brings a unified framework to secure IoT communication system based on a novel mechanism of secret key generation based on ECC and authentication where encryption mechanism using signature generation (SoA) and signature verification (SCM) is applied. In order to validate the effectiveness and scope of the proposed integrated framework for IoT protection, a comparative analysis is performed with energy-efficient systems of the existing work by Shen et al. [33]. In order to conduct a comparative analysis, only the main approach of Shen et al. [33] has been used on the same implantation environment as the proposed system. The analysis is performed on 50–500 IoT nodes in the simulation.

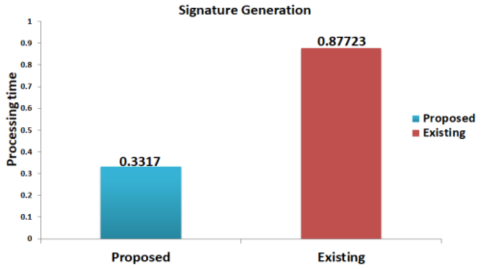


**Fig.2 Comparative analysis of processing time in signature generation**

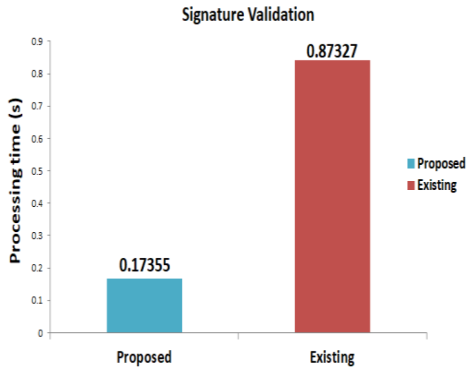


**Fig.3 Comparative analysis of processing time in signature validation**

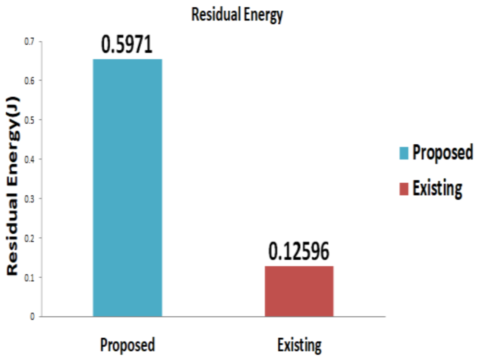


**Fig.4 Comparative analysis for residual energy**

**A. Security Performance Analysis:** The proposed system is introduced to withstand different types of security attacks. Despite any attacks, no valid IoT node can decrypt an encrypted message due to relying on authentication using digital signatures. Another significant factor is that the computation of digital signature has to be performed on every usage without depending on prior information, so the generated signature is extremely secure, and its authentication policy (SCM) offers proof of verification. Therefore, the attacker cannot obtain encrypted data because the next authentication module will cause the opponent to fail because it has no option to calculate verification model dependencies. In addition, the proposed system has not implemented any complex nature of the encryption mechanism. Compared with the existing systems in Fig. 2 and Fig. 3, it is analyzed that the processing time is significantly shortened. It has also been observed that the proposed system reduces delay factor i.e. time required in signature verification and also protects the system from man-in-the-middle attacks due to faster response times.

**B. Energy Performance Analysis:** Energy is a critical parameter for assessing the performance of any security technique in the context of energy constraints nodes. If a security mechanism found to be effective in terms of energy efficiency, it can be considered that it prolongs network service duration and also contribute to the performance enhancement for data delivery operation. The proposed system provides an energy savings mechanism as it does not depend on the location of the IoT gateway and access nodes. The proposed system does not require consuming large energy to perform data processing operations because the proposed algorithm does not include complex encryption operations. This means that the proposed algorithm involves a very less number of iterative steps while performing security operations. Therefore, the introduced framework is found to be highly power-efficient, as seen from the comparative analysis of residual energy (Fig. 3).

## VII CONCLUSION

The proposed study has offered a novel integrated framework to provide efficient security mechanisms in the IoT ecosystem based on a secret key generation using encryption and digital signature mechanisms using ECC and authentication mechanisms. Overall contributions of proposed system are: i) a novel bootstrapping technique is implemented to produce a public key to be used the IoT gateway node for its assigned member node, ii) a different secret key generation scheme has been designed based on light-weight hashing approach, iii) Although the accumulated data is forwarded from the IoT node to the static gateway node, the proposed system allows selection of IoT node dynamically to act as a gateway node and Iv) the proposed system gives novel authentication scheme using digital signatures, where the proposed algorithm generates it based on analysis of the traffic pattern of the IoT node. The simulation outcome exhibits that the proposed security method is efficient to offers reliable security solutions, with quick processing time and energy-saving mechanism compared to existing algorithms in IoT.

## REFERENCES

1. Dudhe, P. V., N. V. Kadam, R. M. Hushangabade, and M. S. Deshmukh. "Internet of Things (IOT): An overview and its applications." In 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), pp. 2650-2653. IEEE, 2017.

2. Dorsemaine, Bruno, Jean-Philippe Gaulier, Jean-Philippe Wary, Nizar Kheir, and Pascal Urien. "Internet of Things: a definition & taxonomy." In 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, pp. 72-77. IEEE, 2015.
3. Yelamarthi, Kumar, Md Sayedul Aman, and Ahmed Abdelgawad. "An application-driven modular IoT architecture." Wireless Communications and Mobile Computing 2017 (2017).
4. Pilloni, Virginia, Luigi Atzori, and Matteo Mallus. "Dynamic involvement of real world objects in the IoT: A consensus-based cooperation approach." Sensors 17, no. 3 (2017): 484.
5. Boyes, Hugh, Bil Hallaq, Joe Cunningham, and Tim Watson. "The industrial internet of things (IIoT): An analysis framework." Computers in Industry 101 (2018): 1-12.
6. Cvitić, Ivan & Vujić, Miroslav & Husnjak, Sinisa. (2015). Classification of Security Risks in the IoT Environment. 10.2507/26th.daaam.proceedings.102.
7. Aydos, Murat, Yılmaz Vural, and Adem Tekerek. "Assessing risks and threats with layered approach to Internet of Things security." Measurement and Control (2019): 0020294019837991.
8. Deogirikar, Jyoti, and Amarsinh Vidhate. "Security attacks in IoT: A survey." In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pp. 32-37. IEEE, 2017.
9. Punia, Aanchal, Daya Gupta, and Shruti Jaiswal. "A perspective on available security techniques in IoT." In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), pp. 1553-1559. IEEE, 2017.
10. Mustafa, Ghulam & Ashraf, Rehan & Mirza, Muhammad & Jamil, Abid & Muhammad,. (2018). A review of data security and cryptographic techniques in IoT based devices. 1-9. 10.1145/3231053.3231100.
11. Y. Shi, “An Obfuscatable Aggregatable Signcryption Scheme for Unattended Devices in IoT Systems”, IEEE Internet of Things Journal, 2017
12. N. N. Dao, Y. Kim, S. Jeong, M. Park and S. Cho, "Achievable Multi-Security Levels for Lightweight IoT-Enabled Devices in Infrastructureless Peer-Aware Communications," in IEEE Access, vol. 5, pp. 26743-26753, 2017.
13. 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.
14. 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.
15. R. Arshad, “Green IoT: An Investigation on Energy Saving Practices for 2020 and Beyond”, IEEE Access, 2017
16. 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.
17. Santos, João, Joel JPC Rodrigues, JoãoCasal, KashifSaleem, and Victor Denisov. "Intelligent personal assistants based on internet of things approaches." IEEE Systems Journal 12, no. 2 (2018): 1793-1802.
18. S-M. Cheng, “Traffic-aware Patching for Cyber Security in Mobile IoT”, arXiv preprint arXiv: 1703.05400, 2017
19. I. Yaqoob et al., ‘‘The rise of ransomware and emerging security challenges in the Internet of Things,’’ Comput. Netw., vol. 129, pp. 444–458, Dec. 2017.
20. W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, ‘‘The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved,’’ IEEE Internet Things J., vol. 6, no. 2, pp. 1606–1616, Apr. 2019.
21. X.liu, Z. Sheng, C.Yin, F.Ali and D.Roggers of Routing Protocol for Low Power and Lossy Networks (RPL) in Large Scale Networks,” IEEE Internet of Things Journal, vol. 4, no. 6, pp. 2172–2185, December 2017
22. Fu, Kevin, et al. (2017). Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things.Technical Report. Computing Community Consortium.[Online]. Available: http://cra.org/ccc/wp-content/uploads/sites/2/2017/02/Safety-Security-an d-Privacy-Threats-in-IoT.pdf.
23. R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed Internet of Things,” Comput. Netw., vol. 57, no. 10, pp. 2266–2279, 2013.
24. L. Wallgren, S. Raza, and T. Voigt, “Routing Attacks and Countermeasures in the RPL-based Internet of Things,” International Journal of Distributed Sensor Networks, vol. 2013, pp. 1–11, 2013.
25. Hassija, Vikas, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, and Biplab Sikdar. "A survey on iot security: Application areas, security threats, and solution architectures." IEEE Access 7 (2019): 82721-82743.
26. P. Pongle and G. Chavan, “A survey: Attacks on RPL and 6LoWPAN in IoT,” in International Conference on Pervasive Computing (ICPC 2015), January 2015, pp. 1–6.
27. A.H.Ngu, M.Gutierrez, V.Metsis, S.Nepal, andQ.Z.Sheng, ‘‘IoTMiddleware: A survey on issues and enabling technologies,’’ IEEE Internet Things J., vol. 4, no. 1, pp. 1–20, Feb. 2017.
28. Shamshekhar S. Patil, Arun Biradar, "Novel Authentication Framework for Securing Communication in Internet-of-Things", ternational Journal of Electrical and Computer Engineering (IJECE), Vol.10, No.1, pp. 1092-1100, 2020
29. Patil, Shamshekhar S., and N. R. Sunitha. "A Novel, Lightweight, and Cost-Effective Mechanism to Secure the Sensor-Gateway Communication in IoT." In Computer Science On-line Conference, pp. 403-412. Springer, Cham, 2018.
30. D. Airehrour, J. Gutierrez, and S. K. Ray, “Secure Routing for Internet of Things: A Survey,” Journal of Network and Computer Applications, vol. 66, pp. 198–213, 2016.
31. F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, “Internet of Things security: A survey,” Journal of Network and Computer Applications, vol. 88, no. December 2016, pp. 10–28, 2017.
32. Yang, Yuchen, et al. "A Survey on Security and Privacy Issues in Internet-of-Things." IEEE Internet of Things Journal 4.5(2017):1250-1258.
33. Shen, John Paul, and Stephen P. Tomas. "A roving monitoring processor for detection of control flow errors in multiple processor systems." *Microprocessing and Microprogramming* 20, no. 4-5 (1987): 249-269.

## AUTHORS FROFILE

**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 DrAIT 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.