Computers, Materials & Continua
DOI:10.32604/cmc.2022.019802
Article

Tech Science Press

Building a Trust Model for Secure Data Sharing (TM-SDS) in Edge Computing Using HMAC Techniques

K. Karthikeyan* and P. Madhavan

School of Computing, SRM Institute of Technology, Kattankulathur, Chennai, 603203, India
*Corresponding Author: K. Karthikeyan. Email: kk9569@srmist.edu.in
Received: 26 April 2021; Accepted: 22 June 2021

Abstract: With the rapid growth of Internet of Things (IoT) based models, and the lack amount of data makes cloud computing resources insufficient. Hence, edge computing-based techniques are becoming more popular in present research domains that makes data storage, and processing effective at the network edges. There are several advanced features like parallel processing and data perception are available in edge computing. Still, there are some challenges in providing privacy and data security over networks. To solve the security issues in Edge Computing, Hash-based Message Authentication Code (HMAC) algorithm is used to provide solutions for preserving data from various attacks that happens with the distributed network nature. This paper proposed a Trust Model for Secure Data Sharing (TM-SDS) with HMAC algorithm. Here, data security is ensured with local and global trust levels with the centralized processing of cloud and by conserving resources effectively. Further, the proposed model achieved 84.25% of packet delivery ratio which is better compared to existing models in the resulting phase. The data packets are securely transmitted between entities in the proposed model and results showed that proposed TM-SDS model outperforms the existing models in an efficient manner.

Keywords: Secure data sharing; edge computing; global trust levels; parallel processing

1 Introduction

Internet of Things (IoT) is the recent advancement in communication, in which data is the valuable resource, providing several intelligent services to the people [1]. However, the IoT data contain private data and can disclose the user identities, if it is not efficiently secured [2]. For instance, the malicious user can utilize the user's private data like date of birth, bank details and so on. The authorized person identification is considered that influences the adverse effects, when there are responsible for user actions. So, an effective privacy preserving models and protocols are necessary in edge computing. In recent times, edge computing is a distributed computation model with many trust models in which the coexistence of multiple operational entities, authentication models require the attribute validation for every unit in single trust model [3,4]. Hence, the entities are mutually authenticated each other

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

with varied secure models. For some resource-limited entities, it is unfeasible to store or process big data or to run a highly complex trust model. Edge computing model comprises big data processing, parallel computation aspects, distributed data transmission processing, location-aware, mobility and dynamicity, and so on. The conventional privacy and security models in edge computing are ineffective for securing the massive data processing [5]. Specifically, secure data processing and privacy preserving problems are effectively important. Major concerns that are faced in edge computing related to data security and privacy-preserving issues are lightweight and fine-grained, distributed access control, limited resources and efficient privacy preservation.

The above-stated data security and privacy preserving issues of edge computing model are stimulated to develop a security model in edge computing. The edge computing model can solve the problems that are related with the centralized system by approaching data pipeline operations over the edge of models with resource accessibility and application needs [6,7]. Moreover, the framework deployment is more advanced in developing model with content providers, network entity, and third party element. Thereby, it is essential to enhance the end-user experience, because of the energy computing strategies [8–10]. Nevertheless, edge computing cannot secure the user data privacy, since new set of attacks with multiple attack models are associated with the heterogeneity of element resources, network measurement and user accessibility [11,12]. So, a Trust Model for Secure Data Sharing (TM-SDS) with HMAC algorithm is proposed in this research paper. The technology utilizes data blocks that are connected with one another with a cryptographic hash key [13,14]. However, the Homomorphic Encryption incorporating in edge computing is a challenging process, because of the resource constraints and the scalability problems. The contributions of the proposed model are listed below,

- Developing enhanced privacy with efficient HMAC Algorithm.
- Local and global trust levels are developed with the centralized processing of cloud and conserving resources effectively.
- For data and communication security, HMAC algorithm is used with hashing concept.
- Providing compatibility with the efficient trust chain process that makes effective decision making without depending on the central admin of each node.
- Interoperability between the trust blocks for efficient data security over communication.
- Evaluation of results based on factors such as processing delay, rate of security, packet delivery ratio, communication overhead and packet drop.

The structure of this paper is organized as follows: Section 2 provides the concepts of security management in edge computing that are applied for data security so far. Section 3 presents the preliminaries that support the proposed idea. Section 4 discussed the working procedure of the proposed Trust Model. The results and evaluations are presented in Section 5 for evidencing the model efficiency. Finally, Section 6 concludes the paper with some motivations for enhancement.

2 Related Works

Each merchant in IoT based communications are used for developing smart entities based on requirements that acts effectively in dynamic platforms [15]. In addition, the framed data are to be secured in such a way that no one can access or misuse data. A valuable review work that described the security issues in several computation platforms. Tao et al. [16] developed a new multi-layered cloud architectural framework in which the services are given with the IoT based smart devices. Additionally, an ontology-based knowledge representation model has been presented in this literature. Lee et al. [17] used semantic web rule language for an effective interoperability of heterogeneous devices.

An Intrusion Detection model (IDM) is developed based on SDN framework by Nobakht et al. [18]. The developed model is used to solve the issues of host-based attack. In addition, the communicational, and computational overhead is significantly reduced by designing the traffic flow based on the target nodes. In this literature, IoT-IDM involved in monitoring the attack-based network activities, and tried to derive the attributes based on data flow of networks. The machine learning techniques are used for the classification of malicious traffics accurately. Gheisari et al. [19] and Madhavan et al. [20] implemented Support Vector Machine (SVM) technique with homomorphic encryption and friendly algorithm to detect the normal and abnormal node activities. The classification operations are performed based on the selected features of the attacks. Mohammadi et al. [21] and Mamolar et al. [22] has tried to resolve the attacks with defined traffic protocols with proper switching and hubs.

Yu et al. [23] has presented a four image encryption algorithm based on chaos and computer generated hologram and quaternion Fresnel transform technique. The developed algorithm improved the security and weaken the correlation, where the extensive experiment showed the effectiveness of four image encryption algorithm. Esposito et al. [24] developed a novel model to authorize and find the policies by leveraging on the block-chain technology for holding a global view of the security policies with-in the system. Further, Li et al. [25] implemented a new algorithm based on synergetic neural networks. Firstly, the developed algorithm embeds the gray watermark signals into discrete cosine transform components. Additionally, the companion algorithm along with co-operative neural network is used for the extraction of watermark. Lastly, the suspected watermark signal is considered as the input, and the output image is considered as the outcome of recognition mechanism.

Stergiou et al. [26] developed an innovative architecture that operates in a wireless mobile 6G network to manage big data on smart buildings. Al-Qerem et al. [27] developed a new variant optimistic con-currency control protocol that decreases the computation, and communication at the cloud. Hence, the developed protocol supports transactional and scalability of the services. The author analyzed the validation process under three con-currency protocols based on the numerical studies. The validation results represent that the developed protocol is more beneficial for the IoT users. Tewari et al. [28] developed a new ultra-light weighted mutual authentication protocol that utilizes bit-wise operations. This protocol is effective by means of communication cost, and storage. Zheng, et al. [29] implemented a light-weighted authenticated encryption approach on the basis of discrete chaotic s box coupled map lattice that superiorly improves the security in IoT environment. Further, Yu et al. [30] developed a new single bit public key encryption approach on the basis of learning parity with noise for an effective encryption. The extensive experiment showed that the developed approach achieved better plaintext attack security.

Gupta et al. [31] developed an attribute based searchable encryption algorithm that provides better flexibility and usability by means of effective search. The developed attribute based searchable encryption algorithm delivers better performance in medical field by preserving privacy of the health data by keeping the data in an encryption form. Tewari et al. [32] performed a mutual authentication process between server and the IoT devices on the basis of elliptic curve cryptography that provides better solution by means of attack resistance and communication over-head. Further, Alsmirat et al. [33] determines the optimal ratio of the finger-print image compression to improve the recognition accuracy of finger-print identification system. In this study, the experiment was performed on large in house dataset and the obtained results showed that the developed approach accurately determines the compression ratio.

The major drawback noticed in the existing works is that the feature selection has been carried out with the static mode. Then, the malicious activities that are not detected in dynamic process, and also the existing models can secure only the target host and not the complete network. To address these issues, a new model is proposed in this research paper.

3 Preliminaries

This section describes the background research about the trust model. In this paper, the concepts of Homomorphic Encryption technique are incorporated to resolve the security issues and efficient resource utilization in Edge Computing. The basic edge computing model is depicted in Fig. 1.

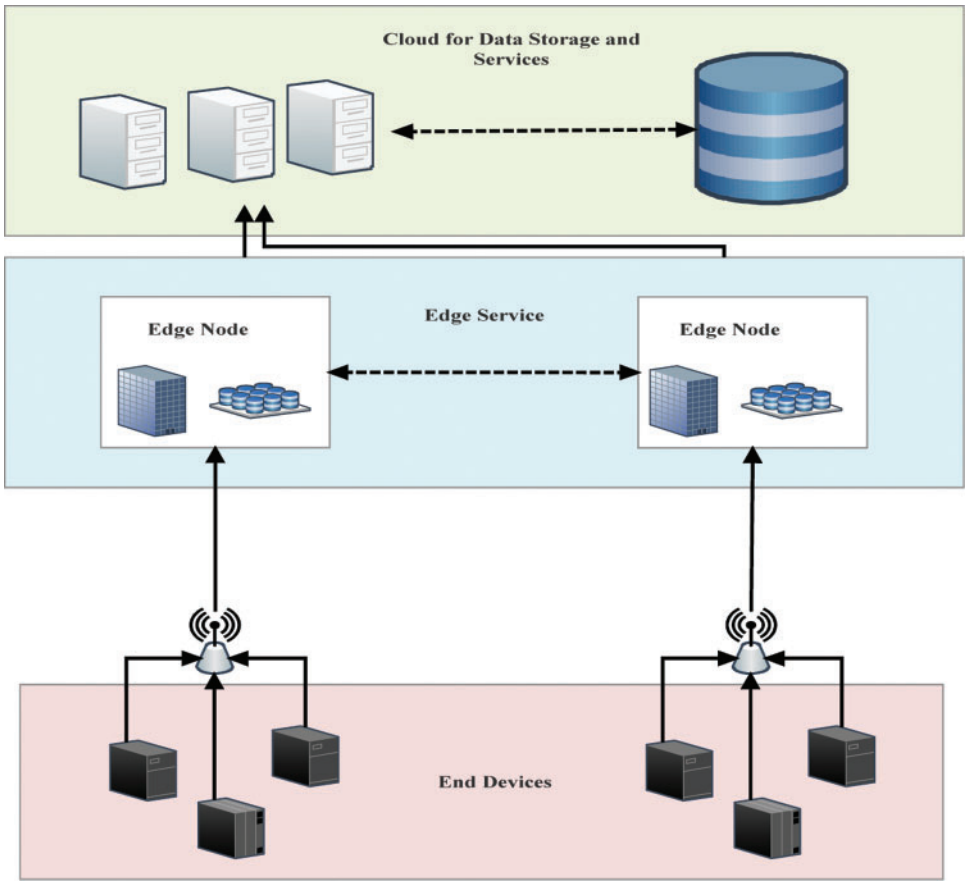

Figure 1: General edge computing framework

The Trust model estimates the security strength and computes the trust esteem value. A trust esteem value comprises of various parameters along with the security of edge computing. The sub parameters and functions also be evaluated in the Trust model [34,35]. Fig. 2 measure the conceptual view of the trust model with their parameter, sub parameter and functions [36].

In Fig. 2, 'A' addresses the Identity Management (IDM), which is the vital components of security frameworks in the cloud, where the cycle analyzed the sign strength with in it. The authentication process represented as 'B' that increase the end user security access at the time of the login and verification process. The verified end user is determined by the strength of the authentication, and

it is processed by the segments of trust models. The authorization process represented as 'C', which is measured by authorization strength. The cloud computing provides the authorization services by the various model using Access Control Strength (ACL) and all the activities need authorization permission in this stage.

The data protection, confidentiality, communication, isolation and virtualization security process are represented from 'D' to 'I', where the trust model security covers all aspects of parameters [37]. The above boundaries are estimated independently and it is joined to calculate the distributed computing strength and application.

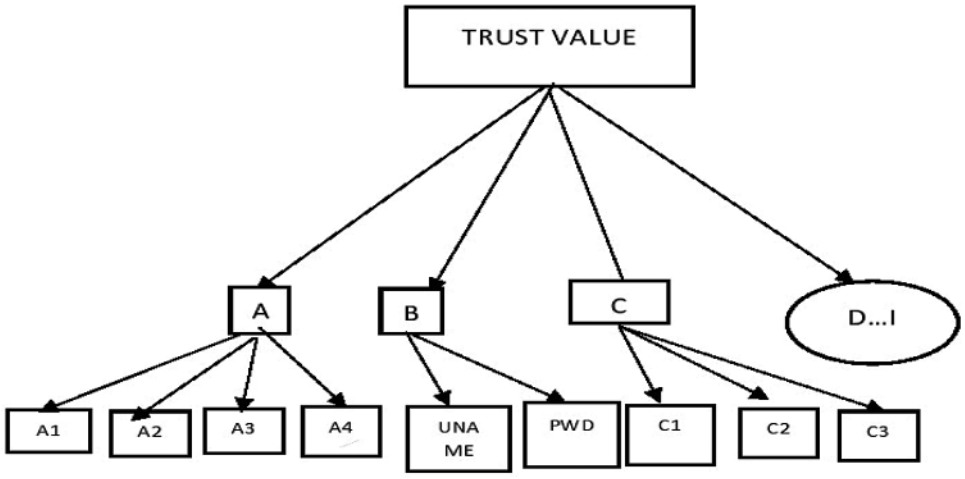

Figure 2: Conceptual view of trust model

4 Proposed Model

In this section, the novel techniques for privacy preserving and utilization of effective computational resources are presented with the proposed model named Trust Model for Secure Data Sharing (TM-SDS) that includes HMAC algorithm for security in edge computing. The proposed model provides enhanced scalability with the secure and distributed storage mechanism, where the high security is achieved with the homomorphic encryption and HMAC algorithm with the trusted model. This process makes the distributed decision making effective without relying on the central admin, who has the control over each node in the network. Furthermore, the interoperability among the multiple blocks is effectively managed. Additionally, the local and the global trust levels are designed for efficient resource usage, which is graphically presented in Fig. 3.

In this research paper, the proposed trust model is implemented with the trust service levels called global and local trust levels. The home or the industrial routers are defined as the trust agent. Based on the demands of security platform, trust services are employed in both the local trust levels. Moreover, in this framework, the homomorphic encryption based trust model technology is enabled for communicating with each other without the requirement of central admin in the pattern of peer-to-peer model. Additionally, the distributive characteristic of edge computing makes both parallel and serial levels based on the application requirements. For computing the authority, there are several trust ranges are defined based on entities, data trust, and user privacy related trust.

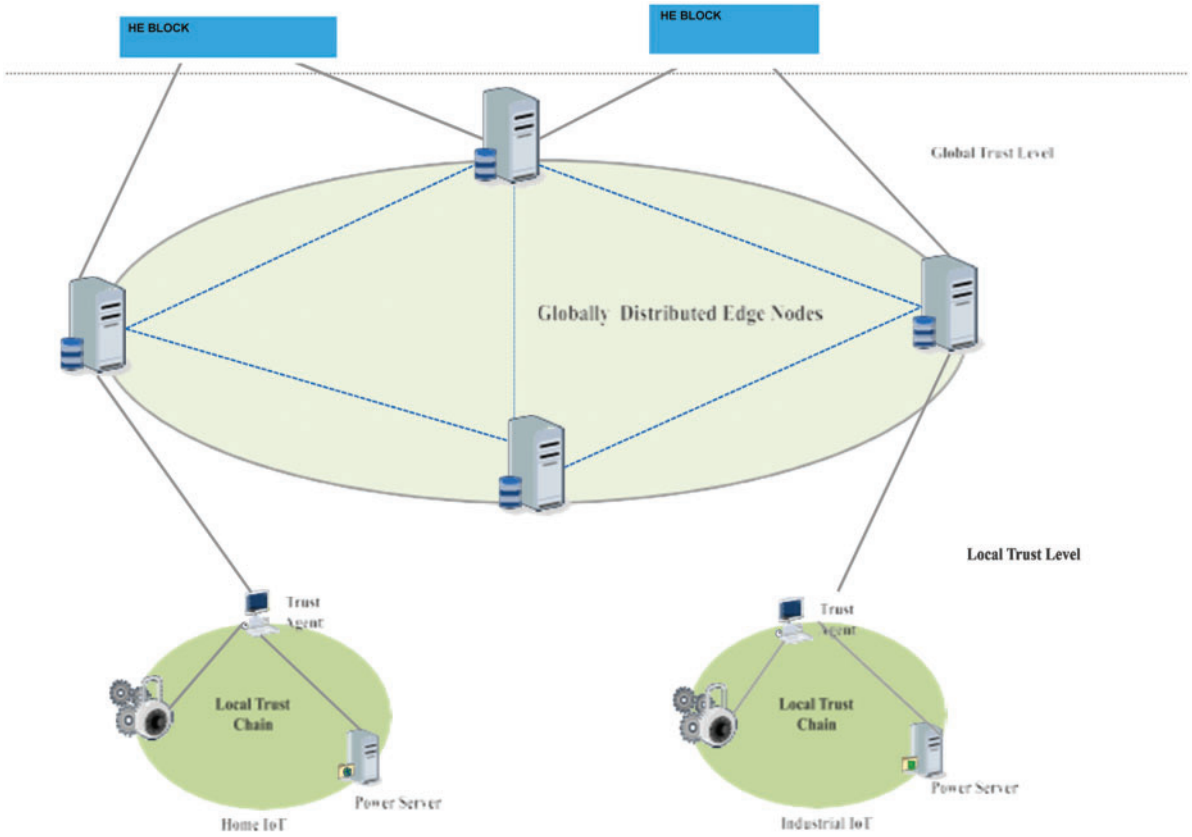

Figure 3: Overall design of the proposed TM-SDS model

Further, the proposed work comprises of three phases such as, (i) initialization phase, (ii) data encryption with homomorphic encryption, and (iii) secure data processing with HMAC. The functions performed in each phase are clearly depicted in Fig. 4, which is executed in bottom-up manner, comprises lower, middle and upper layers.

4.1 Initialization Phase

In this phase, initial setups are processed by preparing the networks based on security demands. The system comprises of edge devices and aggregation point (Ap) for receiving the collected data from edge devices. The data are secured before sending to A_p for data aggregation. Steps involved in the initialization phase are given as,

- Each host of end device (D) in the edge computing network is provided with an identity as $D_i \in \{1, \ldots, n\}$.
- Aggregation points are also provided for some device set, which are also given with identities.
- The base station broadcasts a distinctive key-pair for all devices with similar A_p to produce HMAC for data security.

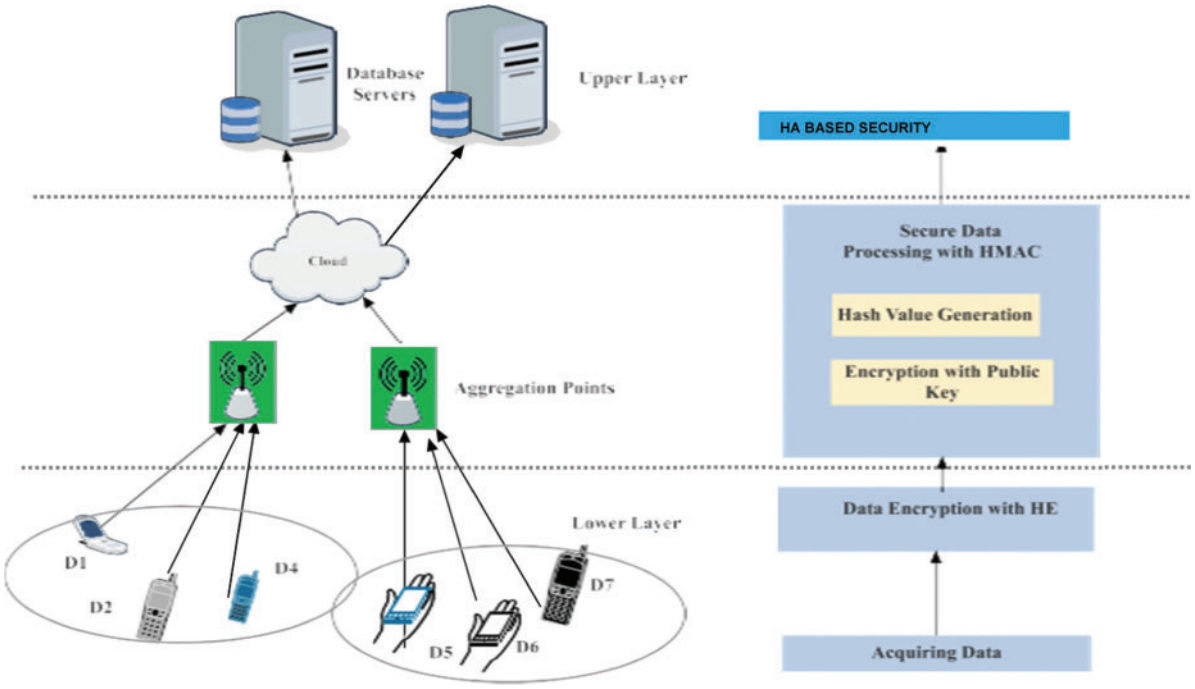

Figure 4: Layers and function in proposed TM-SDS model

4.2 Data Encryption with HE

4.2.1 Process of Data Split

For enhancing the security process, the data split method is used here and the divided data are switched in pair-wise process. Here, it is taken that the A_p is connected with multiple devices, which are termed as, $D_i = \{1, \ldots, n\}$. For specific timestamp, the end devices in edge computing receive data $M = \{m_1, m_2, \ldots, m_n\}$, respectively. The initial phase, each device 'D', 'M' splits the acquired data into 'n' number of sections as, $S_{ij}(i \in 1, 2, \ldots, n), (j \in 1, 2, \ldots, n)$ considerably, in which 'n' points the number of devices presented in the network. The equation for data split is given as Eq. (1),

$$\begin{cases} m_1 = \sum_{j=1}^{n} S_{1j}, \\ m_2 = \sum_{j=2}^{n} S_{2j}, \\ m_n = \sum_{j=n}^{n} S_{nj} \end{cases} \tag{1}$$

Following the data split operation, the sections are interchanged with themselves. The section, 'S_{11}' is protected by the device 'D_1', where the other devices are in effective distribution. Based on the device, D_1 is transmitting $(n-1)$ sections of data, where $S_{ij}(j \neq i)$ to others. Next to the process of swapping, the encryption process is performed, where the model HE derives fast encryption and decryption. The algorithm works on the basis of probabilistic asymmetric method for securing the scalar parameter of shared data. The process of key generation is demonstrated below.

i. **Key Generation Process**

1. Two random numbers 'a' and 'b' are selected, which are mutually independent and provides that is mathematically indicated in Eq. (2).

$$\gcd(ab, (a-1)(b-1)) = 1 \tag{2}$$

It is assumed that the numbers are with equal length.
2. Compute $n - ab$ and $\beta = 1$, which is the parameter constant, for $(x-1, y-1)$.
3. Random integer 'L' is selected, where $L \in \mathbb{Z}^*_{n^2}$.
4. The number of devices 'n' divides the 'L' random number's order with respect to the modular inverse product (ϑ), which is stated in Eq. (3).

$$\vartheta = (F(L^{\gamma} \bmod^{n^2}))^{-1} \bmod n \tag{3}$$

In which, function F is given as, $F(A) = (a-1)/n$
5. Here, the public key is derived as, (n, L)
6. And, private key is stated as, (β, ϑ)

ii. **Process of Encryption**
The obtained data D_i, in which $0 \leq D_i \leq n$, a random number 'v' is selected, that relies in between $(0, n)$. The encrypted text (ET) is derived as Eq. (4),

$$ET = L^m.v^n \bmod n^2 \tag{4}$$

iii. **Process of Decryption**
The 'ET' is decrypted using Eq. (5).

$$D = F(ET^{\beta} \bmod n^2).\vartheta \bmod n \tag{5}$$

4.2.2 HMAC Operations in the Proposed Model

In this model, HMAC is produced for the 'ET', which effectively controls the impacts of node capture attacks and compromised node attacks in edge computing. Here, the HMAC for ET is generated with the identical keys that are used in the $A_p s$. The pseudocode for HMAC generation is given below;

Algorithm 1: Process of HMAC Generation for ET

1. Begin
2. Network Setup Initialization
//Key Generation:
Select p_1 *and* $p_2 \in \mathbb{Z}^*_{n^2}$, then $P = p_1, p_2$
//HMAC Generation,
Do
Derive
$U \leftarrow F(p_1) \in \mathbb{Z}^*_{n^2}$
$V \leftarrow G(p_2(ID, i))) \in \mathbb{Z}^*_{n^2}$
$HMAC_{ET} \leftarrow (U.V) + S) \in \mathbb{Z}^*_{n^2}$
Call Data-Aggregation ( )
Call homomorphic security ( )
End

4.2.3 Operations in Aggregation Point

The data aggregation process is performed in secure manner and the process is explained below, which is run when the pseudocode calls Data-Aggregation ( ). Moreover, the additive operations are performed as given as follows,

$$\begin{cases} d_1{}^0 = S_{11} + \sum_{j=1}^{n} S_{1j},\ (i \neq 1) \\ d_2{}^0 = S_{22} + \sum_{j=2}^{n} S_{2j},\ (i \neq 2) \\ \qquad\quad + \\ \qquad \cdots \quad \cdots \\ \qquad\quad + \\ d_n{}^0 = S_{nn} + \sum_{j=n}^{n} S_{nj},\ (i \neq n) \end{cases} \tag{6}$$

The final results (FD) are derived using Eq. (7),

$$FD = \{d_1{}^0 + d_2{}^0 + \ldots + d_n{}^0\} \tag{7}$$

The private keys are used for device-to-device communications that are to be updated frequently. In addition, the hashing operations are performed for one instant pad with the assumption that the initial private-key is taken as, 'q_1' and the set ends with 'q_n' for 'n' number of devices.

$$\begin{cases} q_2 = HS(ET \parallel q_1) \\ q_3 = HS(ET \parallel q_2) \\ \qquad \cdots \\ q_4 = HS(ET \parallel q_{n-1}) \end{cases} \tag{8}$$

The resultant data obtained for each device is portrayed in Tab. 1 where, $d_i (i \in (1, 2, \ldots, n))$ are the shared data to the edge devices $D_i (i \in (1, 2, \ldots, n))$. The respective encrypted data is $d_i{}^0 (i \in (1, 2, \ldots, n))$. In this way, the real time data are acquired by end devices from the edge computing, which are by secured data storage and transmission between the servers. The data aggregation converts the $\sum_{i=1}^{n} d_i = \sum_{i=1}^{n} d_i{}^0$. Hence, the data cannot be disclosed or accessed at A_p and the real shared data are more secure.

Table 1: Results of secure data aggregation process

	D_1	D_2	...	D_i	...	D_n	Real data
D_1	S_{11}	S_{12}	...	S_{1i}	...	S_{1n}	d_1
D_2	S_{21}	S_{22}	...	S_{2i}	...	S_{2n}	d_2
...	...	...	...	...	...	...	...
D_i	S_{i1}	S_{i2}	...	S_{ii}	...	S_{in}	d_i
...	...	...	...	...	...	...	...
Dn	S_{n1}	S_{n2}	...	S_{ni}	...	S_{nn}	d_n
Encrypted data	$d_1{}^0$	$d_2{}^0$	...	$d_i{}^0$	...	$d_n{}^0$	

When the edge devices share the obtained data, the real data is encrypted with the above operations and the Homomorphic_ security ( ) is executed at the upper layer for securing the keys from unknown access. The encrypted data $d_i^0 (i \in (1, 2, \ldots, n))$ is concealed with the public key of the cloud server before it is shared, which is given as Eq. (9),

$$ET_i = K_{pk}(d_i^0)\ (i \in (1, 2, \ldots, n)) \tag{9}$$

The hash rate is produced by each device with their unique identities (ID), time-stamp and ET. Here, the hash rate is given as, $HS(ID \parallel t_p \parallel ET_i)$, and it helps A_p to verify that the shared private data of the users are confidential and not accessed by anywhere between the transmission process.

5 Results and Discussions

The proposed model is simulated utilizing Network Simulator NS2 device. The results and discussions are presented in this section. Furthermore, the proposed model is accessed the evaluation metrics such as rate of model security, packet delivery rate, transmission delay, packet drop, communication overhead. For evidencing the model efficiency, the results are compared with Support Vector Machine for attack detection and IoT-Intrusion Detection Model (IDM). The initial parameter setting for the simulation tool is provided in the Tab. 2.

Table 2: Initial simulation settings

Parameters	Values
Simulator	NS-2.34
Sensing area	1000 m×m
Simulation time	800 s
Packet length-data	100 bytes
Packet length-total observed data	100 k bytes
No. of devices	Varies from 100–1000
Simulation end time	50 s
Mobility model	Random waypoint
MAC layer protocol	Pure ALOHA
MAC type	IEEE 802.11
MAC layer-back off time	30 s
Traffic type	CBR
Mobility speed	5 m/s
Modulation method	BPSK
Avg. hop distance between devices	10 m
Payload size	512 bytes
Transmission range of each MD	500 m

The significant factor for determining the performance of the proposed model is the communication complexity. During the process of data accumulation, there are some possibilities for attackers

to access the data, and the communication complexity is measured as $O(d * y)$, where, d represents devices and y indicates number of third-party attackers possibly to attack the communication, which is to be less in an efficient model for communication. The evaluation results based on the factor called communication complexity is given in Fig. 5. It is obvious from the results that the proposed model produces minimal complexity than other, since the risks of attacks are minimal in the model with the effectively defined trust model.

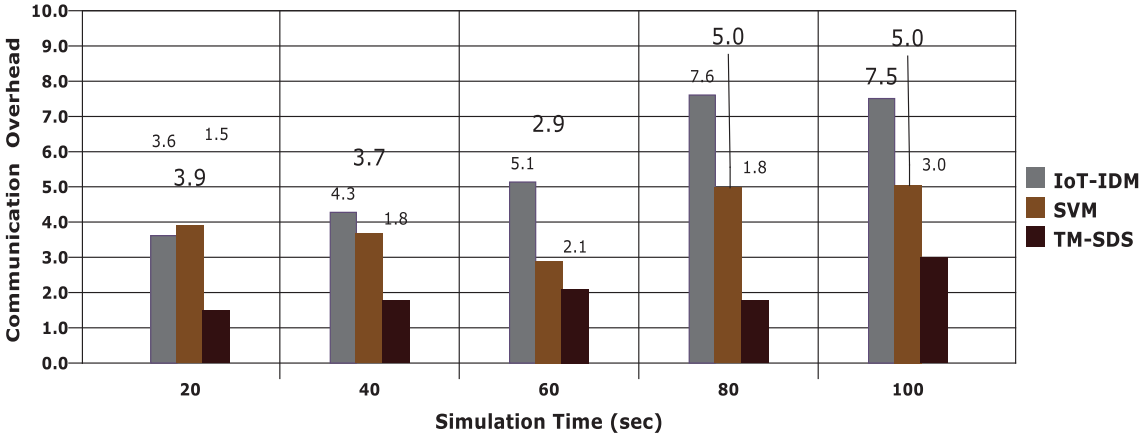

Figure 5: Communication overhead-comparisons

The Packet Delivery Ratio (PDR) is derived with respect to the simulation time and the results are portrayed in Fig. 6. The proposed model achieves 84.25% of PDR in average, which is higher compared to other models such as SVM and IoT-IDM. The data packets are securely transmitted between entities in the proposed model.

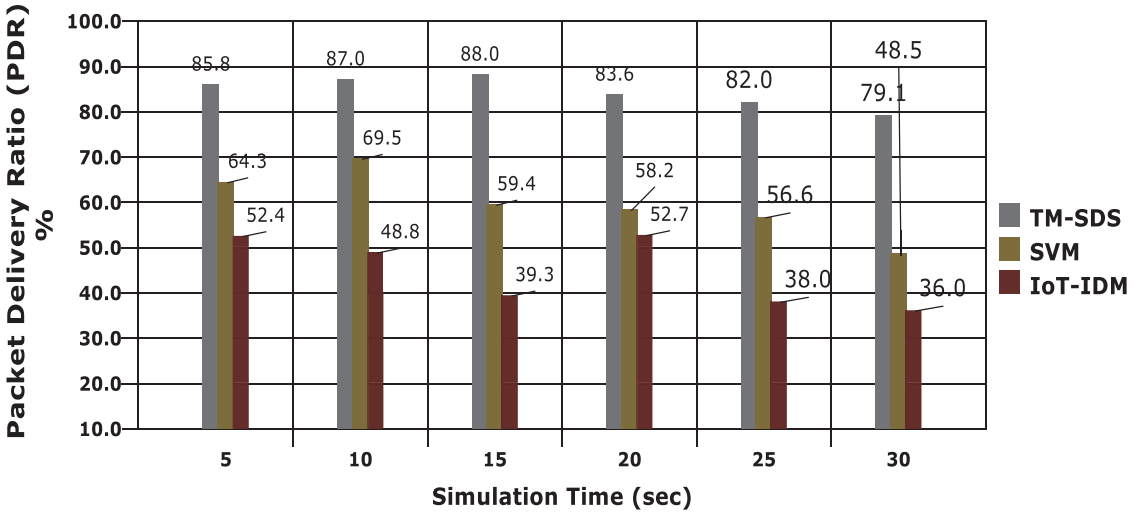

Figure 6: Packet delivery ratio *vs.* simulation time

The transmission delay occurs in a communication model for various reasons and the major issue is the troubles caused by the attackers. In the proposed model, the security of data is effectively handled with the trust model and the homomorphic encryption based security implementations, the overall

transmission delay is effectively reduced in the proposed model and the evidences are provided in the graph in Fig. 7. Another factor, packer drop also should be minimal in efficient edge computing model. The evaluations are carried out against the simulation time and the results are depicted in Fig. 8. It is shown that the proposed model achieves minimal packet drop than the comparative models.

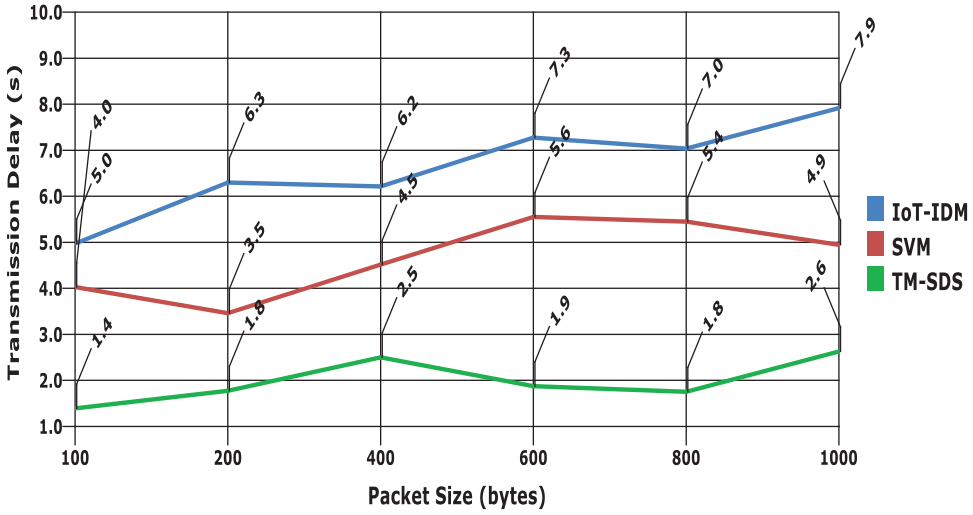

Figure 7: Transmission delay *vs.* packet size

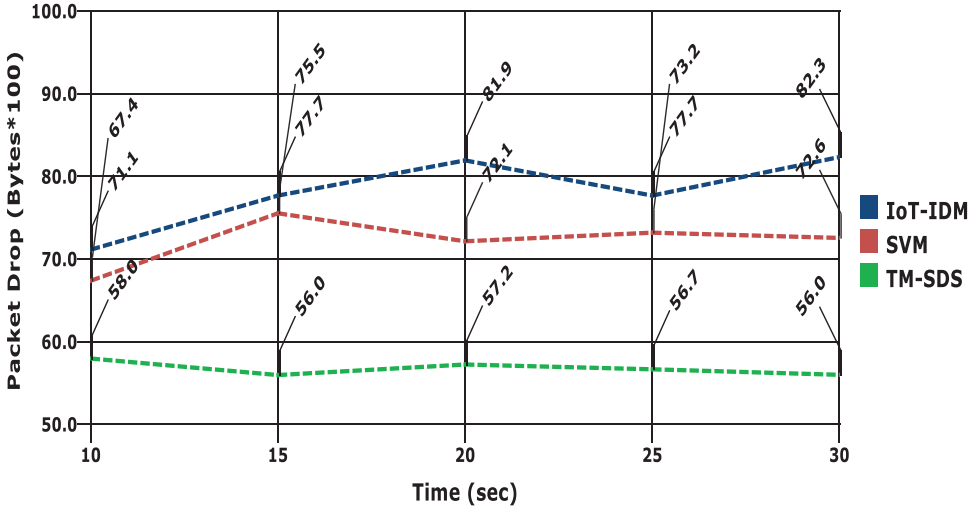

Figure 8: Packet drop *vs.* simulation time

As mentioned earlier, the main motivation of the proposed model is to be derived an efficient data security mechanism for shared data between entities in edge computing. Hence, the security rate of the proposed model is evaluated against a particular attack called compromised node attack and the results are given in Fig. 9. When the compromised attacks are happened in the proposed work, the model effectively detects the attack and showed that there is the attack possibility with minimal rate of security than others. The evaluations are performed against the simulation time.

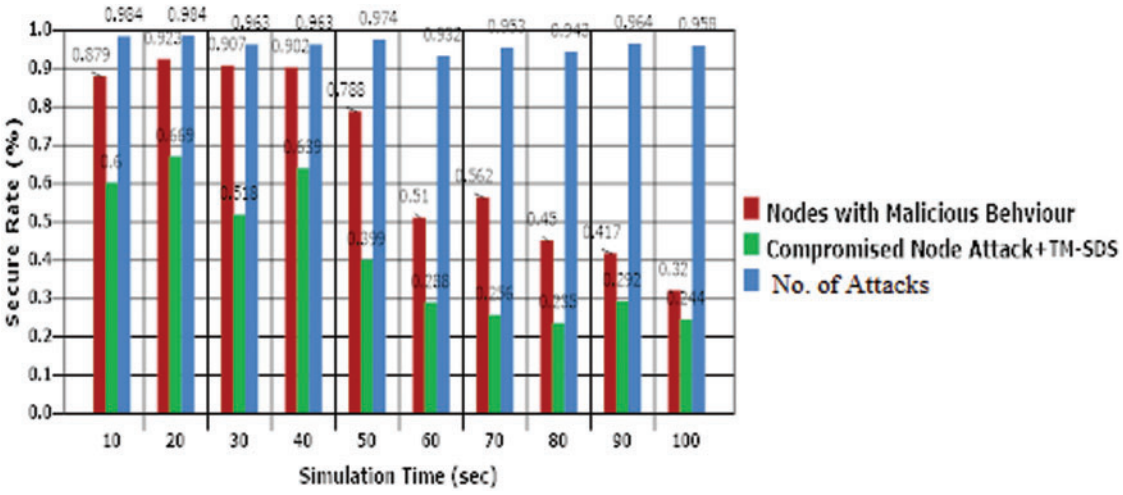

Figure 9: Security rate analysis

6 Conclusion and Future Work

This paper presented a secure communication model in edge computing called Trust Model for Secure Data Sharing (TM-SDS) with homomorphic encryption based Techniques. The model used Homomorphic Encryption and the cross verification is implemented with trust model. Moreover, the security of the shared data is provided with local and global trust levels to be considered with the centralized processing of cloud and conserving resources in efficient manner. HMAC is also utilized for enhancing the rate of data security at the aggregator point in the process of data transmission. The outcomes are assessed based on significant factors such as packet drop, model efficiency and PDR. The comparative analysis showed that the proposed model obtained better results and outperforms the results of the existing works with the effective integration of cryptography and trust model. In future, the proposed work is enhanced by deriving novel mechanisms for integrity verification and seamless communication between entities. In addition, the proposed work is also improved by implementing and evaluating in a real-time environment.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[2] C. Stergiou, K. E. Psannis, B. G. Kim and B. Gupta, "Secure integration of IoT and cloud computing," *Future Generation Computer Systems*, vol. 78, pp. 964–975, 2018.

[3] K. Seyhan, T. N. Nguyen, S. Akleylek, K. Cengiz and S. H. Islam, "Bi-gISIS KE: Modified key exchange protocol with reusable keys for IoT security," *Journal of Information Security and Applications*, vol. 58, pp. 102788, 2021.

[4] M. A. Naeem, T. N. Nguyen, R. Ali, K. Cengiz, Y. Meng and T. Khurshaid, "Hybrid cache management in IoT-based named data networking," *IEEE Internet of Things Journal*, vol. 1, pp. 1–1, 2021. https://doi.org/10.1109/JIOT.2021.3075317.
[5] T. Song, R. Li, B. Mei, J. Yu, X. Xing *et al.*, "A privacy preserving communication protocol for IoT applications in smart homes," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1844–1852, 2017.
[6] T. Snyder and G. Byrd, "The internet of everything," *Computer*, vol. 50, no. 5, pp. 8–19, 2017.
[7] H. Sundmaeker, P. Guillemin, P. Friess and S. Woelfé, "Vision and challenges for realising the internet of things," *Cluster of European Research Projects on the Internet of Things, European Commision*, vol. 3, no. 3, pp. 34–36, 2010.
[8] R. Lu, K. Heung, A. H. Lashkari and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.
[9] M. T. Beck, M. Werner, S. Feld and S. Schimper, "Mobile edge computing: A taxonomy," in *Proc. Sixth Int. Conf. on Advances in Future Internet*, Hangzhou, China, pp. 48–55, 2014.
[10] S. Yi, C. Li and Q. Li, "A survey of fog computing: Concepts, applications and issues," in *Proc. Workshop on Mobile Big Data*, Osaka, Japan, pp. 37–42, 2018.
[11] W. Shi and S. Dustdar, "The promise of edge computing," *Computer*, vol. 49, no. 5, pp. 78–81, 2016.
[12] P. Madhavan, "Framework for QOS optimization in MANET using GA-aCO techniques," in *Proc. Int. Conf. on Advanced Computing and Communication Systems*, Coimbatore, Tamilnadu, India, pp. 529–532, 2019.
[13] T. T. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi *et al.*, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366–1385, 2018.
[14] N. Rifi, N. Agoulmine, N. Chendeb Taher and E. Rachkidi, "Blockchain technology: Is it a good candidate for securing IoT sensitive medical data," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–11, 2018.
[15] S. Sengupta, J. Garcia and X. Masip-Bruin, "A literature survey on ontology of different computing platforms in smart environments," *ArXiv:1803.00087*, 2018.
[16] M. Tao, J. Zuo, Z. Liu, A. Castiglione and F. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes," *Future Generation Computer Systems*, vol. 78, pp. 1040–1051, 2018.
[17] K. C. Lee and J. H. Lee, "Integration of OWL and SWRL Inference using Jess," *Journal of Fuzzy Logic and Intelligent Systems*, vol. 15, pp. 875–880, 2005. https://doi.org/10.5391/JKIIS.2005.15.7.875.
[18] M. Nobakht, V. Sivaraman and R. Boreli, "A host-based intrusion detection and mitigation framework for smart home IoT using open flow," in *Proc. 11th Int. Conf. on Availability, Reliability and Security (ARES)*, Salzburg, Austria, pp. 147–156, 2016.
[19] M. Gheisari, D. Panwar, P. Tomar, H. Harsh, X. Zhang *et al.*, "An optimization model for software quality prediction with case study analysis using MATLAB," *IEEE Access*, vol. 7, pp. 85123–85138, 2019.
[20] P. Madhavan and P. Malathi, "Intelligent framework for QoS optimization in MANET using soft computing models," *International Journal of Advanced Engineering Technology*, vol. 7, no. 2, pp. 890–3, 2016.
[21] M. Mohammadi, T. A. Rashid, S. H. Karim, A. H. Aldalwie, Q. T. Tho *et al.*, "A comprehensive survey and taxonomy of the SVM-based intrusion detection systems," *Journal of Network and Computer Applications*, vol. 178, pp. 102983, 2021.
[22] A. S. Mamolar, P. Salva-Garcia, E. Chirivella-Perez, Z. Pervez, J. M. Calero *et al.*, "Autonomic protection of multi-tenant 5G mobile networks against UDP flooding DDoS attacks," *Journal of Network and Computer Applications*, vol. 145, pp. 102416, 2019.
[23] C. Yu, J. Li, X. Li, X. Ren and B. B. Gupta, "Four-image encryption scheme based on quaternion fresnel transform, chaos and computer generated hologram," *Multimedia Tools and Applications*, vol. 77, no. 4, pp. 4585–4608, 2018.

[24] C. Esposito, M. Ficco and B. B. Gupta, "Blockchain-based authentication and authorization for smart city applications," *Information Processing & Management*, vol. 58, no. 2, pp. 102468, 2021.
[25] D. Li, L. Deng, B. B. Gupta, H. Wang and C. Choi, "A novel CNN based security guaranteed image watermarking generation scenario for smart city applications," *Information Sciences*, vol. 479, pp. 432–447, 2019.
[26] C. L. Stergiou, K. E. Psannis and B. B. Gupta, "Iot-based big data secure management in the fog over a 6G wireless network," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5164–5171, 2020.
[27] A. Al-Qerem, M. Alauthman, A. Almomani and B. B. Gupta, "Iot transaction processing through cooperative concurrency control on fog-cloud computing environment," *Soft Computing*, vol. 24, no. 8, pp. 5695–5711, 2020.
[28] A. Tewari and B. B. Gupta, "Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags," *The Journal of Supercomputing*, vol. 73, no. 3, pp. 1085–1102, 2017.
[29] Q. Zheng, X. Wang, M. K. Khan, W. Zhang, B. B. Gupta *et al.*, "A lightweight authenticated encryption scheme based on chaotic scml for railway cloud service," *IEEE Access*, vol. 6, pp. 711–722, 2017.
[30] Z. Yu, C. Z. Gao, Z. Jing, B. B. Gupta and Q. Cai, "A practical public key encryption scheme based on learning parity with noise," *IEEE Access*, vol. 6, pp. 31918–31923, 2018.
[31] B. B. G. Mamta, K. C. Li, V. C. M. Leung, K. E. Psannis and S. Yamaguchi, "Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 12, pp. 1877–1890, 2021. https://doi.org/10.1109/JAS.2021.1004003.
[32] A. Tewari and B. B. Gupta, "A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices," *International Journal of Advanced Intelligence Paradigms*, vol. 9, no. 2–3, pp. 111–121, 2017.
[33] M. A. Alsmirat, F. Al-Alem, M. Al-Ayyoub, Y. Jararweh and B. Gupta, "Impact of digital fingerprint image quality on the fingerprint recognition accuracy," *Multimedia Tools and Applications*, vol. 78, no. 3, pp. 3649–3688, 2019.
[34] S. Park, J. Byun, J. Lee, J. H. Cheon and J. Lee, "HE-Friendly algorithm for privacy-preserving SVM training," *IEEE Access*, vol. 8, pp. 57414–57425, 2020.
[35] R. Shaikha and M. Sasikumarb, "Trust model for measuring security strength of cloud computing service," *International Conference on Advanced Computing Technologies and Applications*, vol. 45, pp. 380–389, 2015.
[36] P. Madhavan and P. Malathi, "Effective path discovery among clusters for secure transmission of data in MANET," *Artificial Intelligence and Evolutionary Algorithm in Engineering System*, vol. 1, pp. 499–509, 2015.
[37] G. Peralta, R. G. Cid-Fuentes, J. Bilbao and P. M. Crespo, "Homomorphic encryption and network coding in IoT architectures: Advantages and future challenges," *MDPI Electronics*, vol. 8, no. 8, pp. 827, 2019.