International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Data Transmission Framework for the Internet of Things: Safe and Power-Proficient

K. Pradeepa[1*], Dr. M. Parveen[2]

Submitted: 01/10/2023 **Revised**: 20/11/2023 **Accepted**: 01/12/2023

Abstract: Researchers and corporations have been paying close attention to the Internet of Things (IoT) concept lately. Building different smart systems, such the smart grid, smart city, and smart healthcare, requires a base station in the Internet of Things to handle data that is collected from millions of sensor devices. To guarantee the accuracy of the data collected, a secure link needs to be established between the base station and the sensor units. If the information is tainted, the results of the data analysis will be inaccurate and result in more serious harm. In addition, many IoT gadgets have relatively little interaction because of their incredibly low-power computational CPUs. A critical performance measure to take into account while developing a routing algorithm with low-power IoT devices is power efficiency. Thus, a secure and energy-efficient data transmission framework (SE-DTF) for the Internet of Things was introduced in this research. The results of the experiment show how safely a public and a secret key may be shared with a token via the IoT-PSKTS algorithm. It also proves that the throughput, power consumption, and packet delivery ratio of the MPCR using the HFLC algorithm are better than those of other methods. It also shows that compared to other cryptography systems, the two-tier cryptography methodology consumes less energy and requires less processing time for encryption and decoding.

Keywords: *IoT gadgets, Clustering, Cryptography, Signature, Ciphertext shifting, PSKTS algoritham.*

1. Introduction

The Internet of Things is used in many different industries, such as smart cities and homes, medical services, industrial automation, disaster relief, agriculture, etc. Wirelessly linked devices are frequently used by the Internet of Things network to perform certain intelligent tasks [1]. The Internet of Things (IoT) network is not the same as a traditional wireless sensor network (WSN) since its devices work together with other similar devices to accomplish tasks and dynamically connect to the internet [2]. Just like in a conventional WSN network, IoT devices send sensed data to the base station (BS) on a regular basis. The base station transmits the detected data, which is then received by the administrator. Furthermore, transceivers, batteries, and microprocessors are commonly used by Internet of Things utility devices to perform necessary functions [3].

This feature makes it possible to use the Internet of Things network for a variety of tasks, including automation, remote access, and tracking. Almost every technical field has come to recognize the increasing use of the Internet of Things (IoT) network. Important uses include, for example, traffic monitoring in smart cities, healthcare, and industrial operations [4]. The appliance integrates the Smart Grid, Smart Hospital, Smart Home, and more. It is automated and utilized for remote access.

[1]*Assistant Professor, Department of Computer Science, Cauvery College for Women (Autonomous), Trichy.*
[2]*Professor and Head, Department of Information Technology, Cauvery College for Women (Autonomous), Trichy.*
Affiliated to Bharathidasan University

Smart agriculture to increase yield, smart traffic, smart health, disaster detection, water control, surveillance, and leak prevention systems are just a few of the industries that employ IoT technologies. Data collection and transfer are essential for all applications to be completed. The restricted communication range of any IoT device could only allow data transfer over a specific distance. To transfer data from the IoT device to the base station, the other intermediate devices must work together. The Internet of Things gadget acts as a source and a relay. Data transmission to the base station should be done with minimal latency, low power consumption, and high security [5]. Consequently, a framework for Secure and Energy-Efficient Data Transmission (SE-DTF) was described in this research. There are three stages to this structure.

Key leakage is prevented in the first place via IoT-PSKTS, a technique that combines token sharing with public and secret keys. Three components make up an IoT network: an administrator, an IoT base station, and IoT devices. Field monitoring is the administrator's responsibility, and he may do it from anywhere at any time with the aid of IoT. IoT gadgets observe their surroundings and generate perceived data. It then sends detected data to the administrator via an IoT base station. An IoT base station is an IoT network controller. It transmits the detected data to the administrator after obtaining it. IoT devices have limited energy and coverage regions, among other resources.

Every IoT device is positioned differently around the field to monitor pressure, temperature, sound, vibration, and

other factors. To securely transmit this detected data with the admin, encryption is required. This observed data has to be encrypted using both public and private keys. Ensuring that IoT devices have proper network access may also be accomplished through access control. As a result, the administrator uses these keys to generate the access control token for every IoT device. In order to securely distribute these keys with a token to every IoT device, the IoT-PSKTS method was created.

In order to lower energy usage, the second phase employs the Minimum Power usage Routing (MPCR) method and the Hierarchical Fuzzy Logic Clustering (HFLC) algorithm. By employing the MPCR method to aggregate the data in the cluster head, we can minimize communication costs and save battery life while reducing the amount of data transmitted to the base station. Furthermore, the MPCR algorithm significantly reduces the network overheads required to keep the best route.

Cluster creation is implemented via hierarchical clustering, which creates a cluster hierarchy by often dividing a large cluster into smaller ones or merging many tiny clusters into one. Fuzzy logic-based cluster head formation implementations are machine learning algorithms suitable for uncertain applications. For instance, because the IoT competence depends on overlapping criteria like power, the number of devices, the distance between devices and base stations, etc., constructing clusters in the context of predetermined rules may not be acceptable. Fuzzy logic is thus a suitable approach to handle the ambiguity in selecting the cluster head.

Token-based access control, HMAC-SHA1 signature, and two-tier cryptography with ciphertext shifting are used in the third phase, which is dedicated to secure data transmission. Using a secret key and a ciphertext shifting-based encryption approach, Tier-1 data detected by an IoT device is encrypted. Tier 2 involves the public key-based ciphertext shifting encryption approach being used to encrypt the ciphertext that the IoT base station receives from each IoT device. To allow only the administrator with the token of the sending IoT device to read the received ciphertext, a token-based access control mechanism is also used. To further confirm that the received ciphertext is safe, the HMAC-SHA1 signature is employed.

2. Secure and Energy-efficient Data Transmission Framework (SE-DTF):

This section describes the proposed Secure and Energy-efficient Data Transmission Framework (SE-DTF). Since this framework focused on reducing energy consumption while routing and securing data transmission in IoT. Figure 1 demonstrates the architecture of the SE-DTF framework.

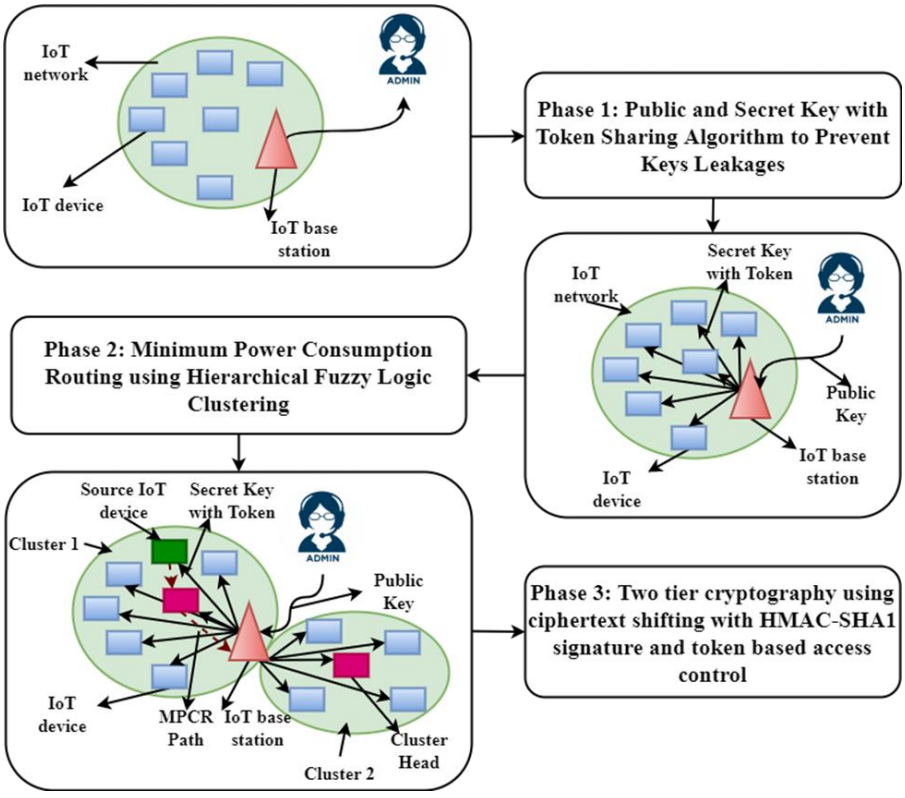

Fig 1: Architecture of SE-DTF framework

This framework has 3 phases. The first phase is public and secret keys with a token sharing (IoT-PSKTS) algorithm, which is used to prevent key leakage. This algorithm enables secure communication over an untrusted IoT network by setting up shared keys between two or more parties. The second phase focuses on low power consumption using the Hierarchical Fuzzy Logic Clustering (HFLC) algorithm and Minimum Power Consumption Routing (MPCR) algorithm. Finally, the third phase focuses on safe data transfer, employing two-tier cryptography with ciphertext shifting, token-based access control, and HMAC-SHA1 signature. The following sections discuss each phase.

3. Results and Discussions

This section presents the results of the experiments conducted on the secure and energy-efficient data transmission framework (SE-DTF) in the Internet of Things. Randomly generated networks are used in experimental research. As seen in Figure 2, the uniform and random deployment of 100 IoT devices throughout a 900 m 600 m unit area serves as the initial point of this simulation. Every Internet of Things device has an initial energy of 100 J and a radio propagation range of 100 meters. A 512-byte data payload capacity has been assigned. To evaluate the SE-DTF framework, MATLAB is utilized.

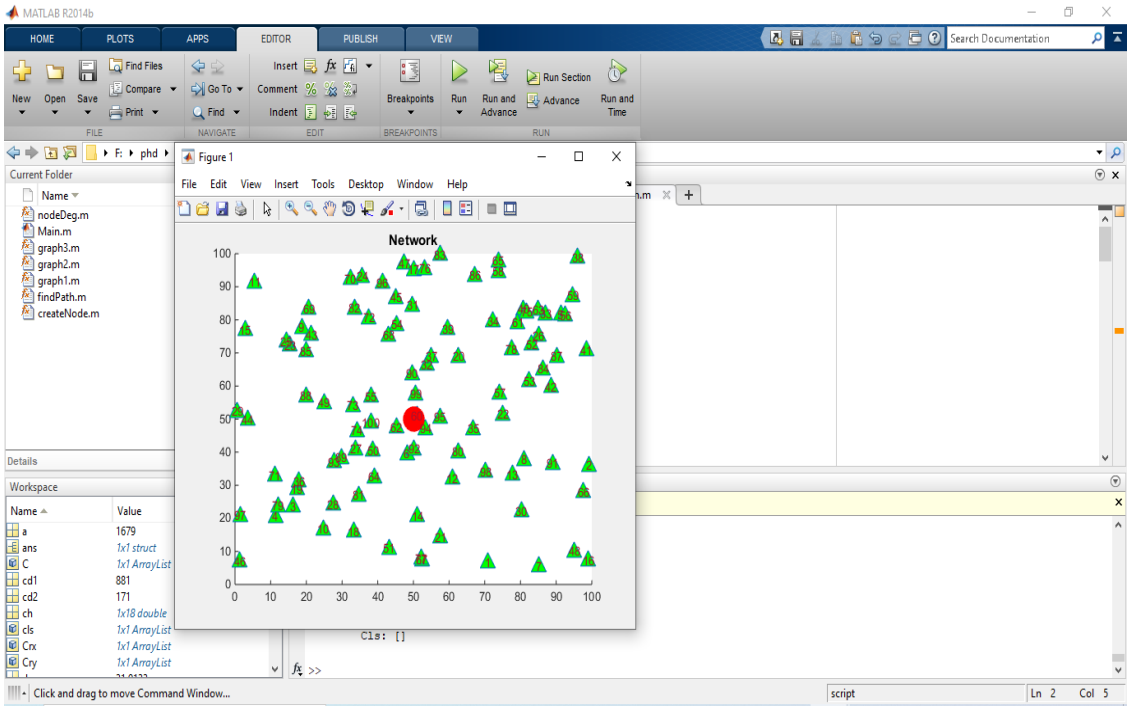

Fig 2: IoT network formation

Phase 1: IoT-PSKTS algorithm

The performance of the suggested IoT-PSKTS algorithm is assessed by contrasting it with alternative secret-sharing methods. In particular, the IoT-PSKTS algorithm's share creation and recreation timings are compared with those of AdiShamir's Perfect Secret Sharing Scheme (PSS), Hugo Krawczyk's Computational Secret Sharing scheme (CSS), and Rabin's Information Dispersal Algorithm (IDA) [16]. In order to evaluate the share creation time, Table 1 shows the milliseconds needed to generate shares, with n and k set to 5 and 3, respectively.

Table 1: The time (in milliseconds) required for generating shares (where n equals 5, and k equals 3).

Algorithm	Data size (in KB)		
	16	32	64
CSS	19.45	25.03	31.80
IDA	12.82	19.59	21.19
PSS	28.78	40.01	42.89
IoT-PSKTS	10.97	17.19	19.68

Figure 3 depicts a time-versus-data-sizes graph for creating shares when n = 5 and k = 3.

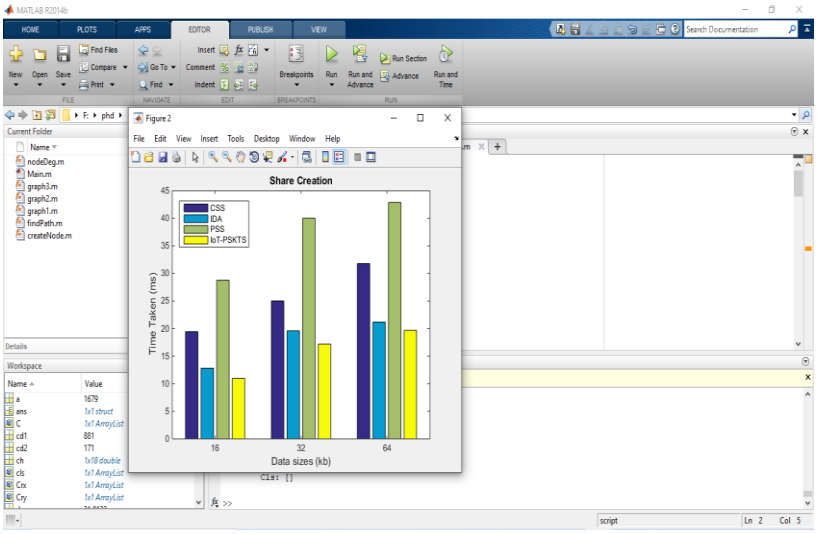

Fig 3: Visual representation indicating the relationship between the share creation time and data size is presented in the graph, where n is set to 5 and k is set to 3

Table 1 and Figure 3 illustrate that the IoT-PSKTS algorithm boasts the fastest performance among all algorithms, regardless of the size of the data being processed. Regarding how long it takes to create shares, IDA comes in second, CSS in third, and PSS last. One important finding from the results is that, compared to the other three algorithms, PSS exhibits more scalability problems as the size of the data increases. The duration required (in milliseconds; ms) for recreating shares (where n equals 5 and k equals 3) is exhibited in Table 2.

Table 2: The time duration (measured in milliseconds) for recreating shares with n set at 5 and k set at 3

Algorithm	**Data size (in KB)**		
	16	**32**	**64**
CSS	19.27	21.63	26.11
IDA	17.82	19.51	22.57
PSS	30.01	20.00	23.89
IoT-PSKTS	15.76	17.04	20.49

Figure 4 presents a graph illustrating the relationship between data size and time consumption for share recreation, with n and k assigned values of 5 and 3, respectively.

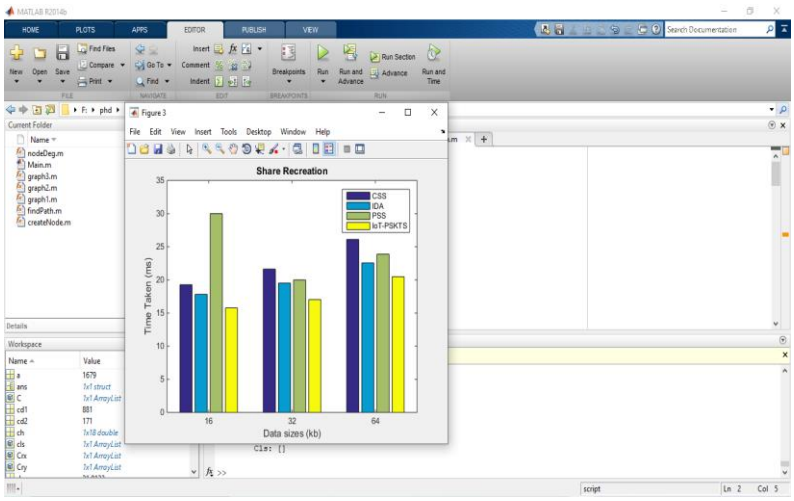

Fig 4: The relationship between data size and time consumption for share recreation, with n and k assigned values of 5 and 3

IoT-PSKTS is the quickest algorithm regardless of data size, as shown in Table 2 and Figure 4. However, regarding the time spent on share recreation, IDA comes in second, followed by CSS and PSS. Some noteworthy findings from the results include that, compared to the other three algorithms, PSS exhibits more scalability problems as the size of the data increases.

4.2 Phase 2: MPCR with the HFLC algorithm:

Furthermore, compare the MPCR with the HFLC algorithm with other routing approaches, such as InFRA [17], DRINA [17], and CBPR [17], in terms of throughput, packet delivery ratio, and energy utilization to assess the effectiveness of the MPCR with the HFLC algorithm. Throughput is the total number of data packets an algorithm might effectively send to the base station in a certain period. The throughput difference for MPCR using the HFLC algorithm, CBPR, DRINA, and InFRA at varying network device densities is demonstrated in Table 3 for each algorithm.

Table 3: Throughput Comparison

Number of IoT devices	InFRA	DRINA	CBPR	MPCR with HFLC
50	72	81	93	104
100	74	86	108	113
150	79	96	115	121
200	88	112	132	139

Figure 5 shows that the MPCR with the HFLC algorithm outperforms the InFRA, DRINA, and CBPR in terms of throughput for all network densities of device situations. Since the MPCR with the HFLC algorithm frequently uses just the optimal pathways while routing packets toward the base station. The MPCR employing the HFLC algorithm chose the path with the highest residual power, the lowest power consumption rate, and the closest proximity to the base station. As a result, it demonstrates connection solidity and lowers packet drop rates when transmitting data. The proposed MPCR with the HFLC algorithm also uses the Fuzzy Logic cluster head selection technique to dynamically identify the best cluster head for use in transmitting aggregated packets. When MPCR with the HFLC algorithm considers everything above, it outperforms its rivals regarding throughput effectiveness.

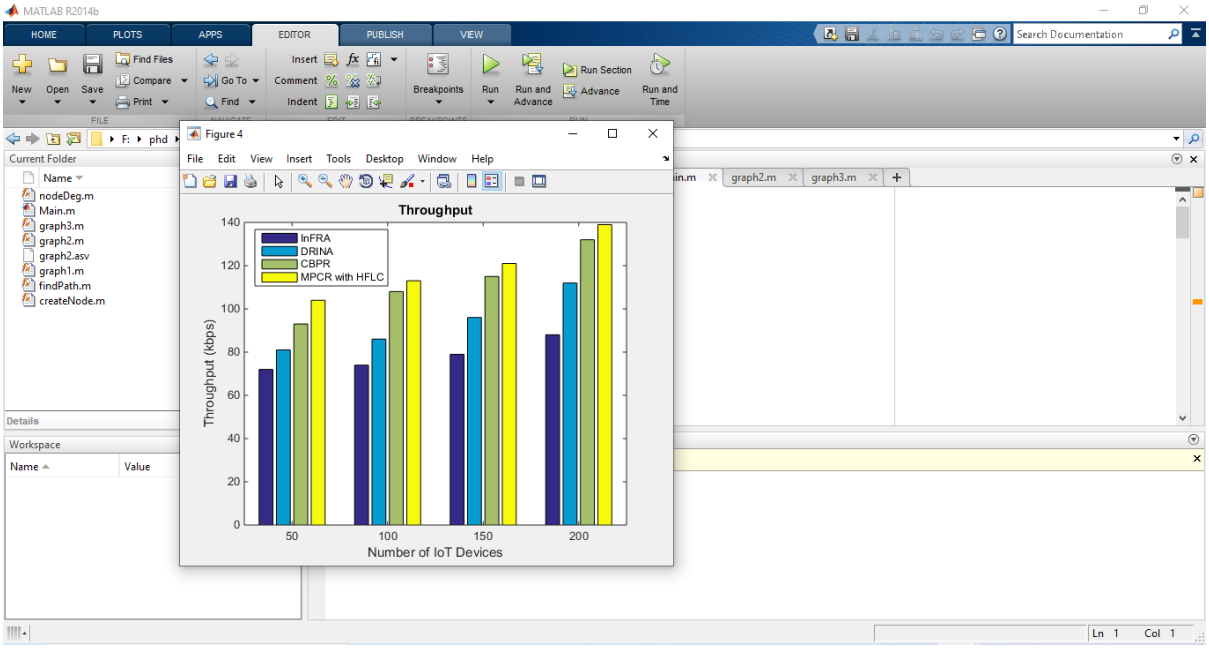

Fig 5: Throughput comparison

The ratio of packets received at the base station throughout the simulation time to the total number of packets emitted from the IoT device of origin is known as the packet delivery ratio. High PDR indicates optimal routing and optimal integration. In addition to the number of network devices and intermediary devices in the route, there are many route possibilities between the source and destination devices.

The MPCR with HFLC algorithm makes use of this multi-path factor to boost efficiency, guiding to competent transfer and a higher packet delivery ratio by selecting intermediate cluster heads with more energy remaining to create the ideal forwarding routes with fewer chances of a link breakdown in the system. In addition, the MPCR with the HFLC algorithm prioritizes the packets based on the IoT device queue size condition, giving precedence to the devices with a shorter queue size, in an effort to lessen network congestion and minimize wait times. It raises the PDR score as a result. Furthermore, MPCR using the HFLC algorithm efficiently makes use of data aggregation, which eliminates superfluous data by combining all related event data into a single data unit, in contrast to InFRA, DRINA, and CBPR routings. Rates of packet delivery are compared in Table 4.

Table 4: Comparison of Packet Delivery Ratios

Number of IoT devices	InFRA	DRINA	CBPR	MPCR with HFLC
50	38	46	64	76
100	39	49	66	79
150	40	60	72	81
200	44	63	76	84

Figure 6 demonstrates the PDR performances of the assessed systems, showing that each scheme's value increases as the number of devices increases.

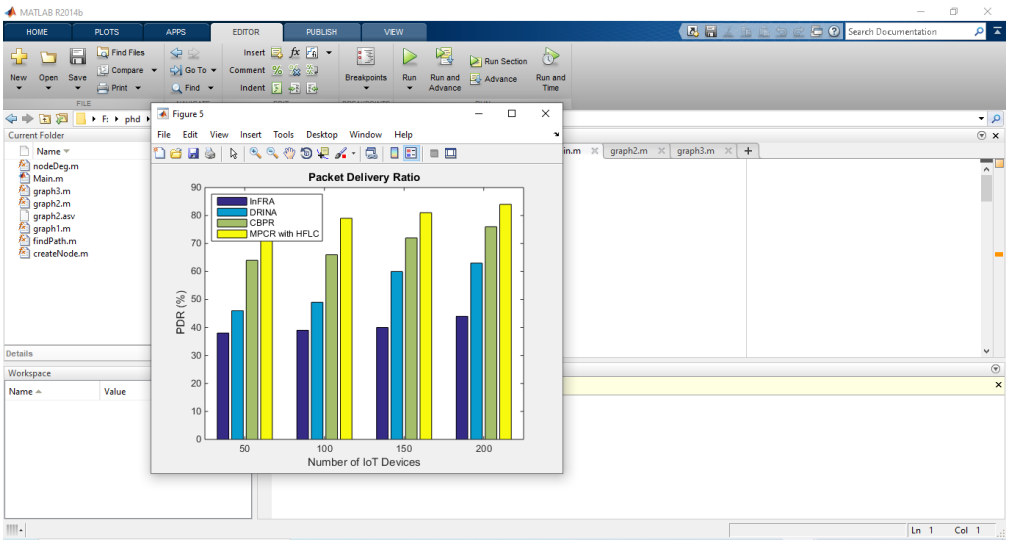

Fig 6: Packet delivery ratio comparison

Energy expenditure in an IoT system denotes the amount of power used to send a unit of information from a source IoT device to a base station. The efficiency of the MPCR with the HFLC algorithm's power utilization has been evaluated utilizing different network device densities and compared to the InFRA, DRINA, and CBPR routing systems, as demonstrated in Table 5 and Figure 7.

Table 5: Energy Consumption Comparison

Number of IoT devices	InFRA	DRINA	CBPR	MPCR with HFLC
50	0.59	0.38	0.23	0.19
100	0.46	0.34	0.17	0.15
150	0.43	0.31	0.14	0.12
200	0.37	0.29	0.13	0.1

MPCR, with the HFLC algorithm, always selects the shortest path to minimize energy consumption. Also, the better cluster head with higher residual energy is chosen closer to the base station and closer to all cluster members.

Hence, it leads to a reduction in energy consumption. Subsequently, it used the packet aggregation technique. Hence, it leads to a reduction in unnecessary energy consumption.

Additionally, this algorithm also has a backup path. In case of connection failure, this algorithm automatically selects another shortest route. A lot of energy is saved this way. Therefore, compared to other proposed algorithms, MPCR with the HFLC algorithm effectively reduces energy consumption.

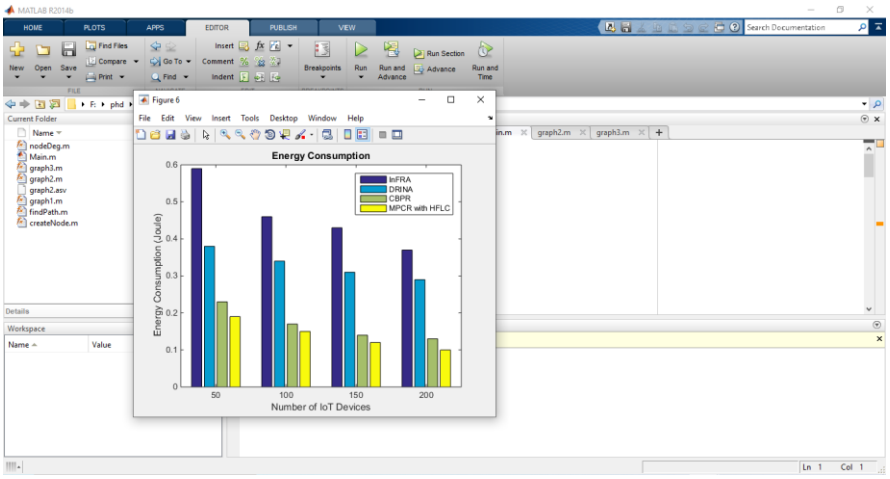

Fig 7: Energy expenditure comparison

4.3 Phase 3: Two-Tier Cryptography Technique:

To evaluate two-tier cryptography techniques, compare the proposed two-tier cryptography technique with existing cryptography techniques such as Blowfish [18] and AKCSS [18] regarding energy consumption and cryptography time. Table 6 depicts the energy expenditure comparison of the proposed two-tier cryptography technique with the existing cryptographic techniques.

Table 6: Energy Consumption Comparison

Technique	Energy Consumption (in microjoule/byes)
Blowfish	0.81
AKCSS	0.02692
Two Tier Cryptography	0.01571

Also, Figure 8 shows the comparison of energy consumption in graph form.

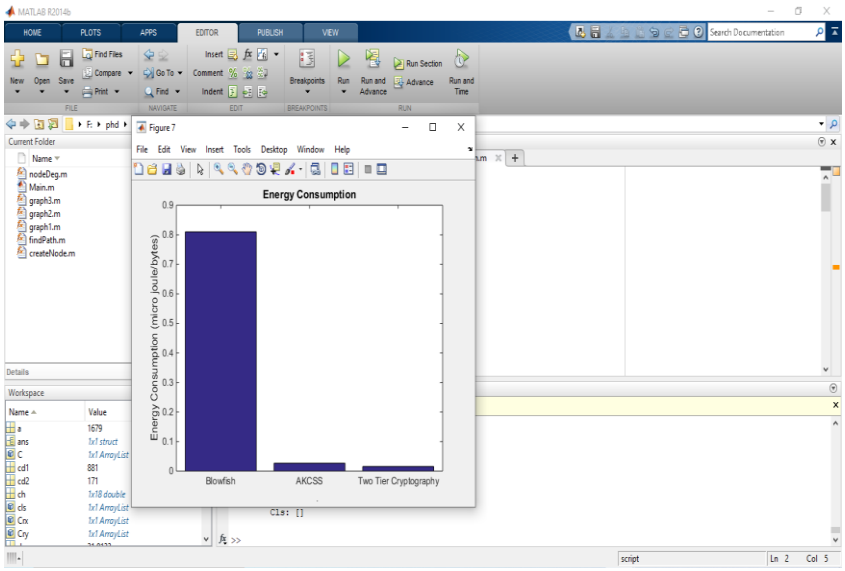

Fig 8: Energy Consumption Comparison

Figure 8 shows that the AKCSS technique consumes less energy compared to Blowfish. But compared to AKCSS, the proposed two-tier cryptography technique consumes much less energy for encryption. Since it uses lightweight cryptography (Tier-1 cryptography) in IoT devices. Also, Table 7 shows the encryption time comparison of the proposed two-tier cryptography technique with the existing cryptography techniques.

Table 7: Encryption Time comparison (in microseconds)

Message Size (in bits)	Blowfish	AKCSS	Two Tier Cryptography
100	9	2	1
500	23	12	9
1000	42	33	28
2000	88	82	76

Also, Figure 9 demonstrates the encryption time comparison in graph form.

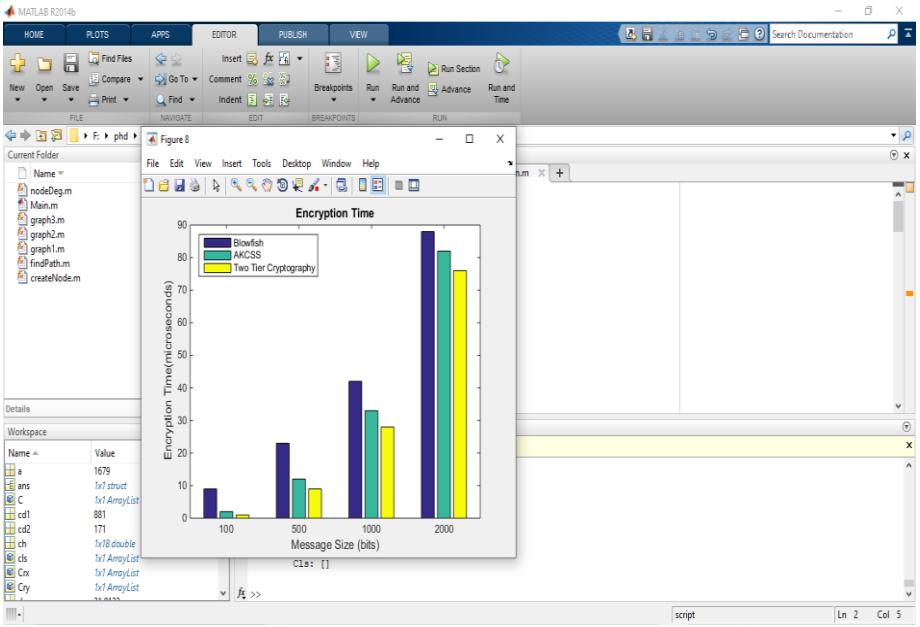

Fig 9: Comparison of encryption time

Figure 9 shows that compared to Blowfish, the AKCSS technique takes less time for encryption. But compared to AKCSS, the proposed two-tier cryptography technique takes less time for encryption. Because it splits the entire encryption process into two tiers and two devices to avoid the computational burden. The first tier is implemented at the sender IoT device and another at the IoT base station. Hence, it takes much less time than other encryption techniques. Also, Table 8 shows the decryption time comparison of the proposed two-tier and existing cryptography techniques.

Table 8: Decryption Time Comparison of Different Cryptography Techniques (in microseconds)

Message Size (in bits)	Blowfish	AKCSS	Two Tier Cryptography
100	4	2	1
500	20	16	12
1000	38	23	20
2000	82	53	48

Also, Figure 10 shows the decryption time comparison in graph form.

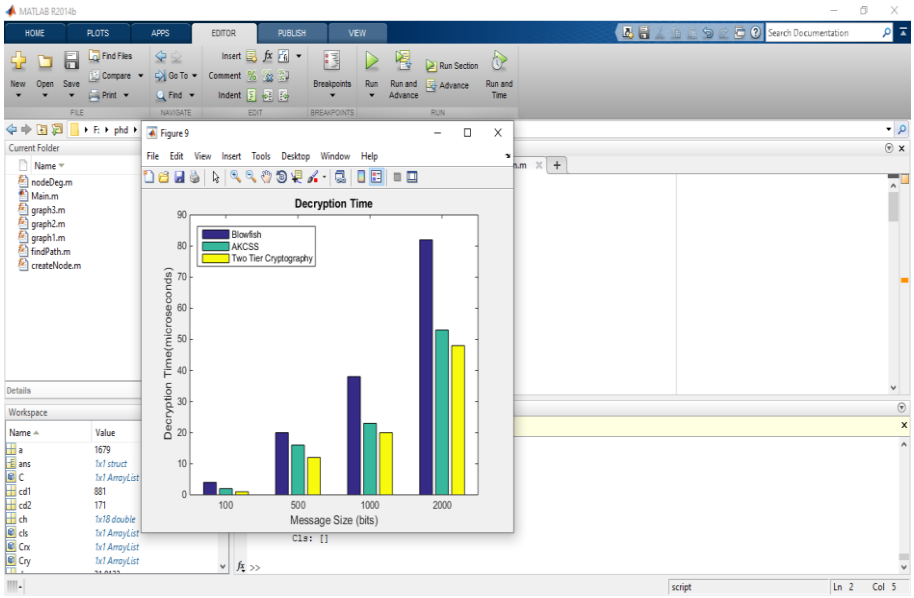

Fig 10: Decryption Time Comparison

Figure 10 shows that compared to Blowfish, the AKCSS technique takes less time for decryption. But compared to AKCSS, the proposed two-tier cryptography technique takes much less time for decryption.

4. Conclusion

By enabling the exchange of cryptographic keys between two entities, key exchange is a technique in cryptography that permits the use of a cryptographic approach. If encrypted communications are to be exchanged, both the admin and the IoT devices need to be able to decode and encrypt messages. The type of encryption method they should choose determines what kind of equipment they need. If they use a similar key, both will need a replica. To stop others from obtaining a copy, the key switch problem describes how to exchange any keys or other data needed to establish a secure communication channel. Sensing data is intercepted, encrypted, and sent to the base station, where it is combined and then sent to the administrator. When using low-power IoT devices to develop a routing algorithm, energy efficiency should also is considered a critical performance metric. Consequently, this paper presented a secure and energy-efficient data transmission framework (SE-DTF) for the IoT. The outcomes of the experiment demonstrated how securely a token with a public key and a secret key could be shared using the IoT-PSKTS algorithm. It was also demonstrated that the MPCR utilizing the HFLC algorithm outperformed other existing algorithms in terms of throughput, packet delivery ratio, and energy consumption. It also shown that the two-tier cryptography approach used less energy and needed less processing time for encryption and decryption when compared to other cryptography systems already in use.

References:

[1] Sankar, S., & Srinivasan, P. (2018). Multi-layer cluster-based energy-aware routing protocol for the IoT. Cybern. Inf. Technol, 18(3), 75-92.

[2] Sujanthi, S., & Kalyani, S. N. (2020). SecDL: QoS-aware secure deep learning approach for dynamic cluster-based routing in WSN-assisted IoT. Wireless Personal Communications, 114(3), 2135-2169.

[3] Aranzazu-Suescun, C., & Cardei, M. (2019). Anchor-based routing protocol with dynamic clustering for IoT WSNs. EURASIP Journal on Wireless Communications and Networking, 2019(1), 1-12.

[4] Maheswar, R., Jayarajan, P., Sampathkumar, A., Kanagachidambaresan, G. R., Hindia, M. N., Tilwari, V., ... & Amiri, I. S. (2021). CBPR: A cluster-based backpressure routing for the IoT. Wireless Personal Communications, 1-19.

[5] Li, J., Silva, B. N., Diyan, M., Cao, Z., & Han, K. (2018). A clustering-based routing algorithm in IoT-aware Wireless Mesh Networks. Sustainable cities and society, 40, 657-666.

[6] J. Tang, H. Song, A. Xu, Y. Jiang, H. Wen, Y. Zhang, K. Qin, "Secret Sharing Simultaneously on the Internet of Things," 2020 IEEE International Conference on Power, Intelligent Computing and Systems, ISBN: 978-1-7281-9874-3, Jul 2020.

[7] M. Farhadi, H. Bypour, R. Mortazavi, "An efficient secret sharing-based storage system for cloud-based IoT," 2019 IEEE 16th International ISC Conference on Information Security and Cryptology, ISBN: 978-1-7281-4374-3, Aug 2019.

[8] Maheswar, R., Jayarajan, P., Sampathkumar, A., Kanagachidambaresan, G. R., Hindia, M. N., Tilwari, V., ... & Amiri, I. S. (2021). CBPR: A

cluster-based backpressure routing for the IoT. Wireless Personal Communications, 1-19.

[9] Kumar, N. P. R., & Gnanadhas, J. B. (2020). Cluster Centroid-Based Energy Efficient Routing Protocol for WSN-Assisted IoT. Advances in Science, Technology, and Engineering Systems Journal, 5(4), 296-313.

[10] Sankar, S., & Srinivasan, P. (2018). Multi-layer cluster-based energy-aware routing protocol for the IoT. Cybern. Inf. Technol, 18(3), 75-92.

[11] Zhang, K., Long, J., Wang, X., Dai, H. N., Liang, K., & Imran, M. (2020). Lightweight searchable encryption protocol for the industrial IoT. IEEE Transactions on Industrial Informatics, 17(6), 4248-4259.

[12] Yousefi, S. M. Jameii, "Improving the security of IoT using encryption algorithm," 2017 IEEE International Conference on IoT and Application, ISBN: 978-1-5386-1698-7, May 2017.

[13] Choudhary, K., Gaba, G. S., Butun, I., & Kumar, P. (2020). Make-it—a lightweight mutual authentication and key exchange protocol for the industrial IoT. Sensors, 20(18), 5166.

[14] Schuster, R., Shmatikov, V., & Tromer, E. (2018, October). Situational access control in the IoT. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 1056-1073).

[15] Terkawi, N. Innab, S. A. Amri, A. A. Amri, "IoT Increasing the Necessity to Adopt Specific Type of Access Control Technique," 2018 IEEE 21st Saudi Computer Society National Computer Conference, ISBN: 978-1-5386-4110-1, Apr 2018.

[16] W. J. Buchanan, D. Lanc, E. Ukwandu, L. Fan, G. Russell, and O. Lo, "The Future Internet: A World of Secret Share," Future Internet 2015, 7, 445-464, DOI:10.3390/fi7040445.

[17] Maheswar, R., Jayarajan, P., Sampathkumar, A., Kanagachidambaresan, G. R., Hindia, M. N., Tilwari, V., ... & Amiri, I. S. (2021). CBPR: A cluster-based backpressure routing for the IoT. Wireless Personal Communications, 1-19.

[18] Preethi, R., & Sughasiny, M. (2018, December). AKCSS: An Asymmetric Key Cryptography Based on Secret Sharing in Mobile Ad Hoc Network. In International Conference on Intelligent Systems Design and Applications (pp. 73-86). Springer, Cham.

[19] Venu, S., Kotti, J., Pankajam, A., Dhabliya, D., Rao, G.N., Bansal, R., Gupta, A., Sammy, F. Secure Big Data Processing in Multihoming Networks with AI-Enabled IoT (2022) Wireless Communications and Mobile Computing, 2022, art. no. 3893875,

[20] Vadivu, N.S., Gupta, G., Naveed, Q.N., Rasheed, T., Singh, S.K., Dhabliya, D. Correlation-Based Mutual Information Model for Analysis of Lung Cancer CT Image (2022) BioMed research international, 2022, p. 6451770.