Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 11, November 2024

Hybrid Attribute Based Encryption to Secure Data in Wireless Sensor Networks

Manisha Kumari
Department of Computer Science and Engineering, HPTU, India

Avni Sharma
Department of Computer Science and Engineering, HPTU, India

Abstract
Wireless Sensor network provides easy-to-use, on-request admittance to shared pools of information, applications and hardware tools. Wireless Sensor network facilitates clients and businesses with different capacities so that they can store and handle their data in the data centers of third party. It depends on exchange of assets to obtain intelligibility and substantial savings, just like a utility (like the power grid) across an organization. The fully Homomorphic encryption (FHE) is adaptable to perform all kinds of calculation on the data that the cloud has contained. The FHE facilitates the execution of all kinds of operations on encrypted data without performing decryption. The application of FHE is essential to keep the CC infrastructure secure. This work suggests an innovative attribute-based framework for enhancing the security of cloud. The proposed model is implemented in MATLAB and results are analyzed in terms attack probability, time analysis, and space utilization Analysis.

Keywords: **WSN, Security, Encryption, Attribute Based Encryption, Diffie-Hellman**

1. INTRODUCTION

Wireless sensor networks are key components of the Internet of Things (IoT), supporting a wide range of applications including habitat monitoring, disaster prevention, automation control, and infrastructure security. These networks consist of nodes equipped with sensors that gather data from their environment. Due to the limited communication range and processing power of these nodes, ad hoc routing protocols are commonly employed in wireless sensor networks. Traditional networking protocols, as well as their security features, are not suitable for these settings and cannot be used to mitigate threats in wireless sensor networks [1]. To address this, various routing protocols and algorithms have been developed to ensure efficient data transmission within these networks. However, they remain vulnerable to security threats such as flooding attacks and eavesdropping [2]. These threats are generally categorized into two types: internal and external attacks. While external attacks can be mitigated through encryption and authentication, which restrict unauthorized access, these methods are ineffective against internal attacks. Internal attacks occur when nodes within the network are compromised and engage in malicious activities.

Trust management emerges as a critical solution for defending against internal attacks, as it relies on monitoring and evaluating the behavior of nodes to detect malicious activity [3]. Choosing the right cryptographic method is essential in wireless sensor networks (WSNs) because cryptography underpins all security functions. Cryptographic techniques for WSNs must be designed to accommodate the limitations of sensor nodes, taking into account code size, data size, processing time, and power consumption. Cryptography is key to WSN security, helping to prevent attacks and protect data. Cryptography in WSNs generally involves encryption, turning standard data packets into secured packets with coded data words. This encryption process adds extra bits to the original data to protect it from unauthorized access during transmission, ensuring security while being compatible with existing network protocols in a layered structure [4]. Cryptographic schemes aim to meet basic security requirements, like confidentiality and integrity. There are two main types of cryptographic algorithms: symmetric cryptography, which uses a shared secret key for encryption and decryption, and asymmetric cryptography, which involves a public-private key pair. Symmetric key encryption involves encrypting plaintext by applying a mathematical algorithm with a secret key. The resulting encrypted data, known as ciphertext, is transmitted to the recipient, who then decrypts it back to plaintext using the same secret key [5]. If an unauthorized person gains access to the key, they could decrypt the ciphertext and reveal the original data.

Symmetric key encryption is commonly used in IoT security to secure data transmissions within a network, and it is often integrated with other cryptographic techniques to provide additional layers of security, such as electronic signatures or hash functions. This approach helps ensure the confidentiality, integrity, and authenticity of data in transit. Examples of symmetric key encryption algorithms include AES (Advanced Encryption Standard), DES (Data Encryption Standard), and TDEA (Triple Data Encryption Algorithm). Asymmetric key encryption, also known as public-key encryption, relies on a pair of keys: a public key and a private key. A user generates this key pair, with the public key used for encrypting data and the private key used for decrypting it. The public key can be shared freely, allowing anyone to send encrypted data to the key owner, while the private key is kept secret and allows the owner to access the encrypted information. The key advantage of asymmetric encryption is that it eliminates the need for secure key distribution, a common challenge in symmetric key encryption [6]. However, asymmetric key encryption is generally slower and more computationally demanding compared to symmetric key encryption. It is also more complex, requiring higher computational power to implement effectively. Asymmetric key

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 11, November 2024

encryption is often used alongside other security techniques, like symmetric key encryption, hash functions, and digital signatures, to create a layered security approach that protects the confidentiality, integrity, and authenticity of transmitted data. Examples of asymmetric key encryption algorithms include Rivest-Shamir-Adleman (RSA), elliptic curve cryptography, and Diffie-Hellman key exchange. These algorithms use distinct mathematical operations and key lengths to perform encryption and decryption. RSA is a popular algorithm for encryption and digital signatures, known for its security, which is based on the difficulty of factoring large numbers.

2. LITERATURE REVIEW

S. Anitha, et.al (2023) suggested a LEACH Protocol based on Novel Trust Management with Cryptographic RSA algorithm (NTM-LEACH-RSA) for prolonging the duration of network and consuming least energy [7]. Two stages were employed to enhance security in WSN in which cluster was formed and cluster head (CH) was selected initially. Moreover, the threshold function value, the distance and density among neighboring nodes, and the trust value were considered for selecting CH. The energy and the distance domain were employed for estimating the threshold function value. Subsequently, RSA cryptography method was implemented for protecting the way to transmit data and ensuring data integrity. The experiments depicted that the suggested protocol had generated superior results.

B. Valluri, et.al (2024) proposed a method to protect sensor data during transmission and when the nodes received the data [8]. The Exceptional Key based Node Validation for Secure Data Transmission using Asymmetric Cryptography (EKbNV-SDT-AC) method was suggested. This method was focused on validating node, encrypting and decrypting the data in WSN so that the data was transmitted securely amid source and destination. This data was not required to be sent to all nodes. The more vigorous and creative kind of key related to basic public key cryptography (PKC) systems was contained in key administration, which offered efficacy and reliability to PKC for several applications. The results indicated that the suggested method offered an accuracy of 98% to validate node, and 98.6% to encrypt and decrypt data.

S. Tabbassum, et.al (2024) presented a low-energy adaptive clustering hierarchy (LEACH) algorithm for transmitting data [9]. The Fuzzy Logic (FL) and Artificial Neural Network (ANN) methods were put forward. The primary goal was to locate the nodes at random within the network and initialize them for collecting information. This algorithm was utilized for randomly selecting cluster heads (CHs) and allocating this role to diverse nodes using a round-robin management (RRM) system. The intrusion-detection process was assisted in determining the presence of intruders. A Fuzzy interference rule (FIR) was adopted for differentiating malicious nodes from authentic ones. Finally, the harmful nodes were differentiated from suspected ones via ANN. The presented algorithm yielded an accuracy of 97%, specificity of 97%, and sensitivity of 95%.

C. S. Reddy, et.al (2022) projected a secure routing method with deep learning methods [10]. At first, long short-term memory (LSTM) was implemented to verify trust for selecting the non-malicious node and eliminating them. At second, an elliptic curve cryptography (ECC) algorithm was deployed to encrypt the data for further transmitting it to the secured shortest paths. For this, dragonfly algorithm (DA) was applied to choose these paths. Diverse metrics, such as distance, energy, delay, throughput, and trust were deployed to tackle multi-objective function (MOF). In the end, the simulation results indicated that the projected method was robust in WSN to transmit data securely.

C. Li, et.al (2023) analyzed that the restricted energy of nodes and selfish nodes led to mitigate the packet delivery rate (PDR) [11]. An energy-harvesting Q-learning secure routing (EQLSR) algorithm was introduced with authenticated-encryption. The physical unclonable functions and optimized QL were adopted for ensuring the reliability of transmission path. The issue of restricted energy in nodes was resolved using solar panels that helped in charging the nodes. In the meantime, the LSTM-based predictive framework was incorporated for predicting the energy value which was refilled via nodes. The introduced algorithm was simulated against existing technique. The experiments demonstrated that the introduced algorithm was led to enhance packet delivery rate (PDR), filter selfish nodes, and mitigate node energy utilization.

S. S. Priya, et.al (2023) established an energy-efficient secure data transmission (EESDT) system for WSNs in which trust concept was deployed for detecting and preventing data compromise and performed well [12]. Firstly, a novel data security method was adopted in which data was kept confidential and reliable. Secondly, the trust concept was utilized to analyze the quality of data links so that the data was transmitted securely, and nodes and edges were isolated on the basis of trust value. Diverse variables, such as energy usage and secure data delivery were considered to provide reliability and dependability in WSN broadcasting. The countermode encryption (CE) method was led to enhance the data security due to its lightweight, simplicity, and unpredictability. The established system was proved effective concerning duration of network and energy usage.

3. RESEARCH METHODOLOGY

Following are the various stages of proposed model: -

3.1 ORIGINAL IDENTITY TRANSMISSION AND SECURE CHANNEL GENERATION

At initial stage, the user sends the original identity to the Key Identity Provider and creates a secure channel. For this, Diffie-Hellman (DH) algorithm is implemented. DH is considered as a mathematical algorithm which assists two systems in generating an identical secret whose transmission is done on both systems. However, these systems have not any communication among one another. The transmitted secret is employed for broadcasting a cryptographic encryption key in a secure manner. This work aims to encrypt the traffic amid 2 systems. This algorithm is effective for encrypting the data on web on the basis of Secure Socket Layer (SSL) or Transport Layer Security (TLS). Moreover, this algorithm makes the deployment of Secure Shell (SSH) protocol. This protocol is employed for exchanging the key securely for encrypting the data. A shared secret which is also known as Key Encryption Key (KEK) is considered for exchanging this secure transmission. Thereafter, the transmitted secret helps to encrypt the symmetric key to achieve safe transmittal. This process is

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 11, November 2024

initialized by generating a private key on every side of the correspondence. Every end focuses on generating a public key that is obtained as the derivation of the private key. The next task is to exchange the public keys amid both systems. Hence, it provides own private key and the other public key of systems to each side of the correspondence. After completing the key sharing, the process is executed further. Consequently, this algorithm leads to generate a shared key as identical cryptographic key whose transmission is done via each side. Afterward, the mathematical operation is deployed against the private key and other side's public key for acquiring a value. In the end, cryptographic key assists in encrypting the traffic. The Diffie-Hellman algorithm often utilizes a shared secret for encrypting a symmetric key for one of the symmetric algorithms and transmitting it in secure manner. The inaccessible end is exploited in this algorithm for decrypting it with the shared secret. At the completion of transmitting a symmetric key securely, the data is encrypted and a communication is established securely.

3.2 VIRTUAL IDENTITY GENERATION AND TRANSMISSION

The key identity provider provides an identity provider and private key to the user. Moreover, it sends a public key and identity to the WSN. The fourth stage employs the HE technique so that the data is encrypted. The HE is a property of an encryption methodology which is robust to be executed in the encrypted information (ciphertexts) and to preserve the actual operation outcomes on the underlying clear text operands. This approach is consisted of a number of applications and it is deployed for carrying out computations on encrypted data on the basis of data which is concealed from it. Assume a scenario in which a client is there along with a relatively weak computing device and a server which is comprised of robust computing resources. Moreover, considers that a client focuses on outsourcing its data to the remote server so that computing results are obtained and performing computations over the data. The HE approach is provide suitable for this process. It helps a client in generating a ciphertext of its secret data and transmitting it to a server. Afterward, a ciphertext of the computation result is provided to the server. For this, the homomorphic evaluations are carried out on the ciphertext of client and this ciphertext is returned to the client. At last, the client is able to decrypt the evaluated ciphertext, and attains the computation result. There is not any association amid the computation cost for a client and the size of a delegated function. HE is capable of handing the ciphertext for users without key, and in this process, no information related to plaintext is revealed. This attribute is effective for protecting the security of information and enhancing the efficacy to process the information. More specifically, in case an encryption function f results in satisfying

$$f(a) + f(b) = f(a + b) \quad (1)$$

It is considered that it has additive homomorphism, and in case it satisfies

$$f(a) * f(b) = f(a * b) \quad (2)$$

This implies that this function contains multiplicative homomorphism. The Homomorphic encryption (HE) is executed for managing ciphertext and to retrieve, calculate and compute the ciphertext within the WSN directly. Hence, the output is provided to customers as ciphertext. There is not any necessity of regular encryption and decryption amid the WSN and customers in this approach. It results in mitigating the message and computational overhead. There are some properties of this approach. This procedure is executed in seven stages: original identity transmission, secure channel generation, Identity provider and private key transmission, public key and identity transmission, data encryption, data transmission and data storage in WSN. The key sizes for fully homomorphic encryption (FHE) schemes commonly used in practical applications can vary, but they are generally larger than those of traditional encryption schemes due to the additional requirements for supporting computations on encrypted data. Key sizes are influenced by factors such as the specific FHE algorithm, the desired security level. In this research work we have used 150-bit long key for the encryption and decryption. The Fully homomorphic encryption keys are bit long than traditional algorithms due to which it has less chances of attacks and also less execution time.

3.3 DATA SECURITY

In the next stage, the encrypted data is transmitted to the WSN. In the last stage, the WSN attains the public key and identity from the key identity provider and private key from user. Then it focuses on decrypting both the keys and storing the data. Homomorphic encryption (HE) is an effective method to perform data encryption and decryption in diverse phases which are described as:

3.3.1 Data Encryption

The data owner focuses on encrypting their sensitive data. For this, a homomorphic encryption method is employed. This method further has diverse kinds namely partially homomorphic encryption or fully homomorphic encryption. The next task is to transmit and store the encrypted data in a secure way for which there is not any necessity of decrypting the data.

3.3.2 Data Processing

A third party, like a service provider or an application, is capable of executing calculations on the encrypted data. HE method is composed of particular mathematical operations such as addition and multiplication, which can be executed on the encrypted data.

3.4 DATA DECRYPTION

After completing the selected computations on the encrypted data, the results are generated in encrypted form. The data owner, who is responsible for possessing the decryption key, becomes able to decrypt the result for attaining the final output. Homomorphic encryption is consisted of diverse levels for determining the kinds of operations which are suitable to preserve the encryption. Moreover, partially homomorphic encryption methods namely Paillier encryption etc. are also available. But, these method comprises only restricted number of operations such as addition and multiplication, and fully homomorphic encryption methods, namely TFHE, BFV, CKKS can be deployed to carry out complicated computations.

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 11, November 2024

4. RESULT AND DISCUSSION

	BF-IBE	Out-FS	Improved Out-FS
120	100	220	32

This research work is implemented in MATLAB using the mathematical tool box. It is an interactive program which provides numerical computation and visualization of data. With the help of its programming capabilities, it provides tool which is very useful for all areas of science and engineering.

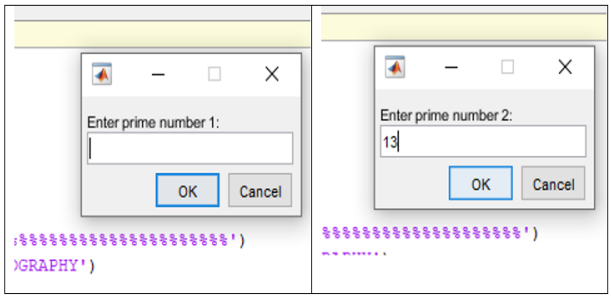

Fig.1. Enter prime Numbers

As shown in figure 1, the Diffie-Hellman algorithm is applied for the secure channel establishment. The prime number of entered for secure key generation

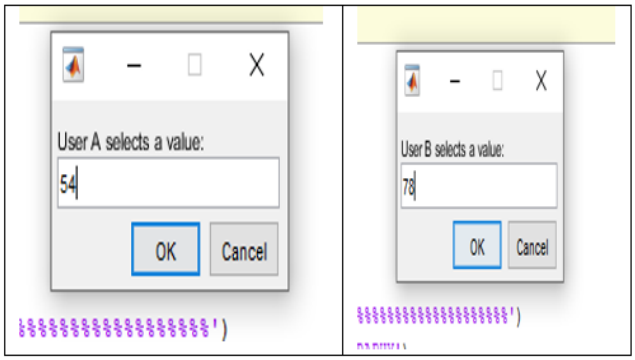

Fig.2. Enter Secrete Keys

As shown in figure 2, the user A and B enter their secrete keys for the secure key calculation.

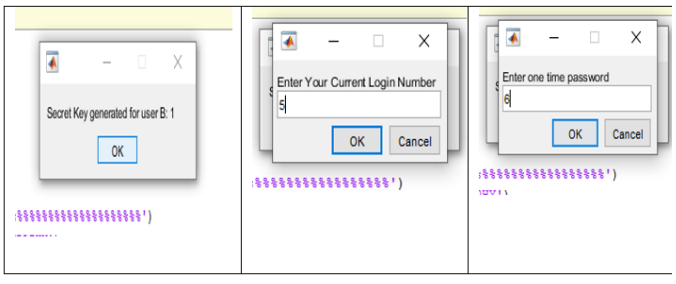

Fig.3. Generation of Keys

As shown in figure 3, the OTP is generated in this phase which is the combination of secrete key and number of login times.

Table.1. Probability of Attacks

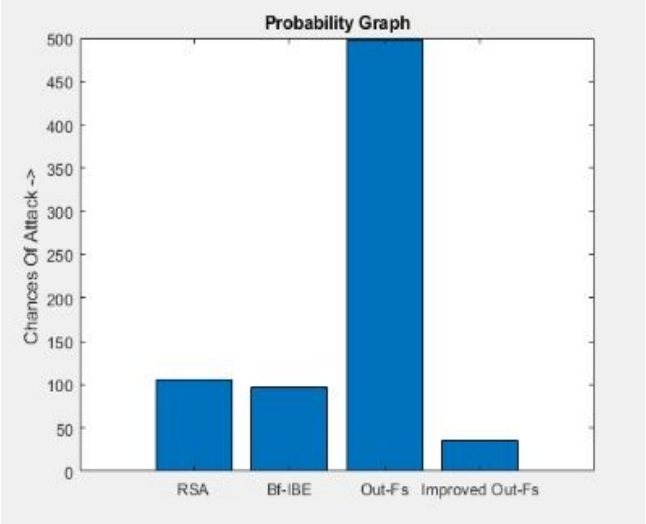

Fig.4. Attack Probability Analysis

As shown in figure 4, the attack probability of proposed technique is compared with Out-Fs, Bf-IBE and RSA. The Proposed technique has least chances of attack as compared to other techniques.

Table. 2. Time Comparison

RSA	BF-IBE	Out-FS	Improved Out-FS
70	67	140	35

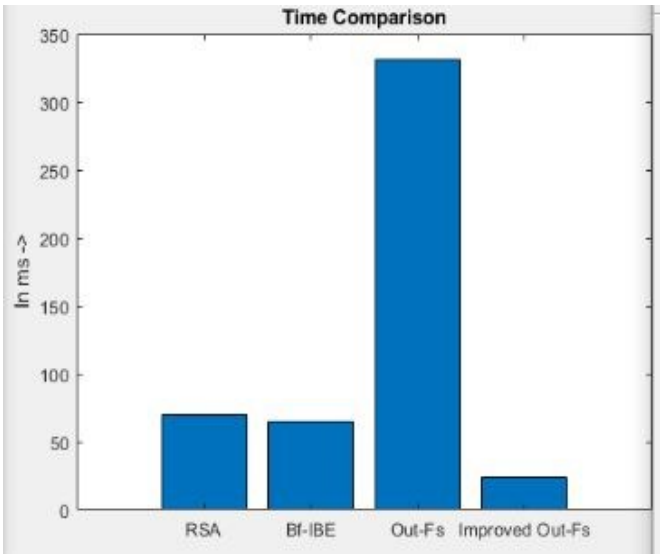

Fig.5. Time Analysis

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 11, November 2024

As shown in figure 5, the Execution time of proposed technique is compared with Out-Fs, Bf-IBE and RSA. The Proposed technique has least execution time as compared to other techniques.

Table.3. Space Utilizations

RSA	BF-IBE	Out-FS	Improved Out-FS
3000	2800	2600	2500

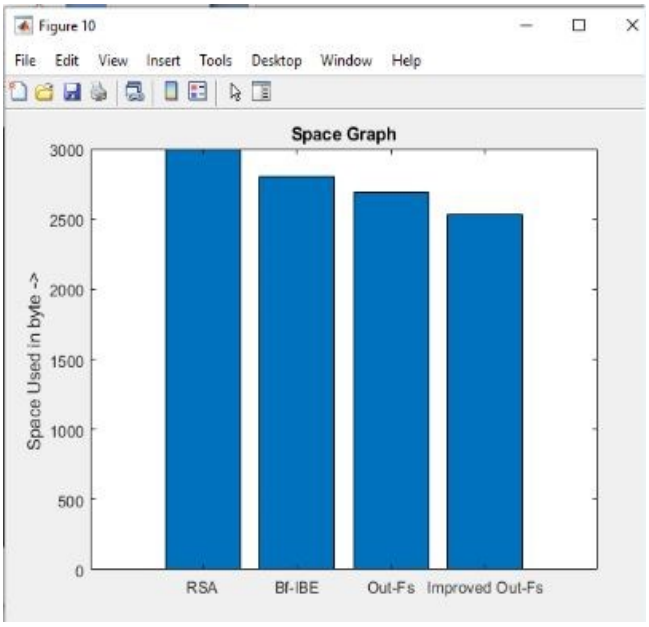

Fig.6. Space Utilization Analysis

As shown in figure 6, the space utilization of proposed technique is compared with Out-Fs, Bf-IBE and RSA. The Proposed technique has minimal space utilization as compared to other techniques.

5. CONCLUSION

The performance of wireless sensor networks is affected due to data breaches and security issues. Therefore, to provide security measures and privacy, the service providers focus on deploying cryptography methods, authentication approaches and virtualization. Detecting and analyzing the security risks, perform implementation scope and auditing in network scenarios is very difficult. An important step that secures wireless sensor networks is the removal of security risks and maintenance of privacy. The control will no longer persist in the hand of user's id the service provider hosts the data and web applications. The encryption schemes are suggested for the secure authentication and certification in wireless sensor networks. This work suggests a novel attribute-based scheme will be proposed which will be less complex and more secure for the certificate distribution. The proposed method is the based on the Diffie-Hellman algorithm or the identity exchange. The homomorphic encryption (HE) approach is applied to encrypt the data. The proposed model is implemented on MATLAB and an analysis is conducted on results concerning energy, time and chances of attacks. It is analyzed that proposed model performs well as compared to existing Identity-Based Encryption model for wireless sensor networks data security.

REFERENCES

[1] J. Li, L. Zhang, and D. S. Wong, "Identity-Based Encryption for Cloud Computing," in Proceedings of the IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 2013, pp. 387-394.
[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute-Based Encryption with Privacy Preserving in Cloud Computing," in Proceedings of the IEEE INFOCOM, 2010, pp. 1-9.
[3] C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Cloud Storage," in IEEE Transactions on Dependable and Secure Computing, 2015 vol. 12, no. 4, pp. 435-448.
[4] Y. Zhu, H. Wang, Z. Hu, and G.-J. Ahn, "Ciphertext-Policy Attribute-Based Encryption with Efficient Revocation in Cloud Computing," in IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 7, pp. 1442-1453.
[5] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Data in Cloud Computing," in Proceedings of the IEEE International Conference on Distributed Computing Systems (ICDCS), 2010, pp. 383-392.
[6] X. Li, M. Li, and S. Chen, "Identity-Based Encryption with Outsourced Revocation in Cloud Computing," in Proceedings of the IEEE International Conference on Cloud Computing (CLOUD), 2012, pp. 730-737.
[7] O. A. Khashan, "Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System," in IEEE Access, 2020, vol. 8, pp. 210855-210867.
[8] Z. -Y. Liu, Y. -F. Tseng, R. Tso, Y. -C. Chen and M. Mambo, "Identity-Certifying Authority-Aided Identity-Based Searchable Encryption Framework in Cloud Systems," in IEEE Systems Journal, Sept. 2022, vol. 16, no. 3, pp. 4629-4640.
[9] Kwangsu Lee, "Revocable hierarchical identity-based encryption with adaptive security", Theoretical Computer Science, 3 June 2021, vol. 880, no. 12, pp. 37-68.
[10] H. Deng et al., "Identity-Based Encryption Transformation for Flexible Sharing of Encrypted Data in Public Cloud," in IEEE Transactions on Information Forensics and Security, 2020, vol. 15, pp. 3168-3180.
[11] D. Jeyakumar, K. Chidambarathanu, S. Pradeepkumar and T. P. Anish, "OUTFS+. An Efficient User-Side Encrypted File System Using IBE With Parallel Encryption," 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2022, pp. 760-766
[12] L. Liu, Y. Zhang and X. Li, "KeyD: Secure Key-Deduplication with Identity-Based Broadcast Encryption," in IEEE Transactions on Cloud Computing, 1 April-June 2021, vol. 9, no. 2, pp. 670-681.