2021 4th International Conference on Recent Trends in Computer Science and Technology (ICRTCST) | 978-1-6654-6633-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICRTCST54752.2022.9781993

Privacy Preserving Data Sharing in Cloud Using EAE Technique

N Jagadish Kumar
Department of Information Technology, Velammal Institute of Technology
Chennai, India
n.jagadishiva@gmail.com

K V Vinisha
Department of Information Technology, Velammal Institute of Technology
Chennai, India
vinisha0909vini@gmail.com

C Balasubramanian
Department of Computer Science and Engineering, P.S.R. Engineering CollegeSivakasi, India
balasubramanian@psr.edu.in

Dasam Sowmya
Department of Information Technology, Velammal Institute of Technology
Chennai, India
dasamsowmyait0131@gmail.com

K S Prathibapriya
Department of Information Technology, Velammal Institute of Technology
Chennai, India
prathibapriya.saravanan.prathiv@gmail.com

***Abstract*—Accessing and controlling data on the cloud is a low-cost method of ensuring data security. However, in cloud storage systems with untrusted cloud servers, data storage and retrieval management become a challenge. Because this new computing technology encourages users to leave their sensitive data to cloud providers, security and privacy issues over outsourced data are growing. To protect data privacy, attribute-based encryption (ABE) systems and variations are frequently used. ABE scheme are resistant to a variety of assaults. Which includes data access, interruption, interception alteration, illegal authentication, and fabrication? Existing encryption approaches, on the other hand, necessitate greater processing time and secure communications of sensitive information transport, both of which remain unsolved. The proposed scheme uses enhanced elliptic curve Attribute-based Encryption (EAE) to address this problem. EAE encrypts user data during transmission to ensure privacy. EAE generates the hash value for the encrypted data and stores it in the cloud server after completing the encryption process. To strengthen data transfer security, this produced hash value is sent to the associated users in the cloud. We deployed our scheme and demonstrated that this is both effective and versatile for outsourcing data in the cloud.**

Keywords—Cloud storage systems, Security, privacy, Attribute-based encryption and Elliptic curve Attribute-based Encryption.

I. INTRODUCTION

Grid computing facilitated the growth of cloud computing, and maintaining security for cloud data is a big challenge for the information technology community. Because of its inability to sustain storage devices, businesses are increasingly turning to cloud computing, where cloud storage is managed by third parties [1]. To manage data and remote services, cloud computing creates a link between central remote servers and the network. Managing data on the cloud offers more benefits in terms of hardware maintenance.

Providing cloud storage with security is a critical issue. For data encryption, before it has been transferred to the cloud, various encryption algorithms have been developed. The primary purpose of encryption systems should be to provide cloud data with strong security, access control, and data secrecy. It provides scalable resources across the internet on a dynamic basis. The following are the main benefits of cloud computing: flexibility, cost savings, and great scalability. The existing ABE approaches are complicated since they call for a significant number of security parameters to be implemented in order to provide 2^{128} security [2-5]. Aside from that, the ABE methods take into account a certificate authority (CA) who participates actively in the application procedure. Secret keys are generated and distributed by the CA to data users. The distribution of personal information with the certificate authority, however, may jeopardize client and data privacy, as the certificate authority can decipher communications and access data, based on application cases. Furthermore, if CA is compromised, the sender and receiver's communication anonymity is jeopardized. General View of Secure Cloud is shown in Fig. 1.

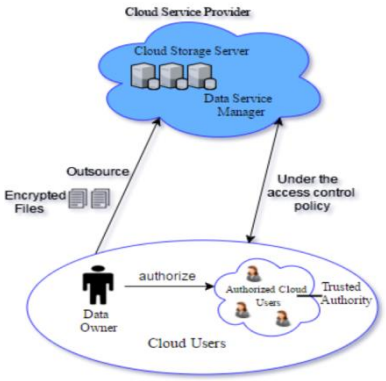


Fig.1. General View of Secure Cloud

We will discuss how, without the usage of a certifying authority, using elliptic curve cryptography (ECC) approaches; we can create effective ABE methods [3-7]. Since most previous research has focused on either secure

transmission or the PPDM technique, the goal of this paper is to present a unique framework that provides both secure transmission and information secrecy. For privacy-preserving data exchange in the cloud, we propose an Enhanced elliptic curve Attribute-based encryption. For at least 2^{128} computational security, our EAE approach uses fewer security parameters, which makes it efficient in resource-constrained computing machines.

The primary goal of our approach is to establish high security for confidential data transfer in a virtualized environment. The following is the research goal of the EAE technique: 1) In a cloud context, using Elliptic Curve Attribute Encryption and Decryption to improve data transfer secrecy while requiring little processing effort. 2) In the EAE approach, the Hashing Function is employed to increase data transfer security and reduce complexity in a cloud context. In section 2, we give a related work. Section 3 contains information on how to put the plan into action. Section 4 contains the details of the experiment. Section 5 concludes with a conclusion and recommendations for future work.

II. Literature Survey

One-to-many data encryption is attribute-based encryption. The encryption text can decrypt only by a user whose attributes comply with the encryptor's access policy. Identity-based encryption inspired this approach.

S. Arun et al. [4] concentrated on elliptical curve cryptography for data security. Using Elliptical Curve Cryptography, which is a powerful and secure methodology for integrating and developing secure cloud applications. Nikos Komninos et al. [5] Focuses on how to create efficient ABE schemes without the usage of a certifying authority using elliptic curve cryptography (ECC) techniques. They perform cryptography functions like addition and multiplication together in a subgroup by jeopardizing the security of the ABE system. Sadia Syed et al. [6] propose Hierarchical Attribute-Set-Based Encryption (HASBE) for the cloud environment. This is a multilevel user architecture featuring complex parameters which enhance the cipher message Attribute-Set-Based Encryption (ASBE). Establish scalable, flexible, and powerful data access policies with the aid of HASBE compound attributes. For increasing the security of cloud data, Athena et al. [7] implemented efficient approaches such as cryptography Diffie–Hellman for private key creation and identifying attribute-based cryptography. PHR allows the authenticated user to view the patient's data.

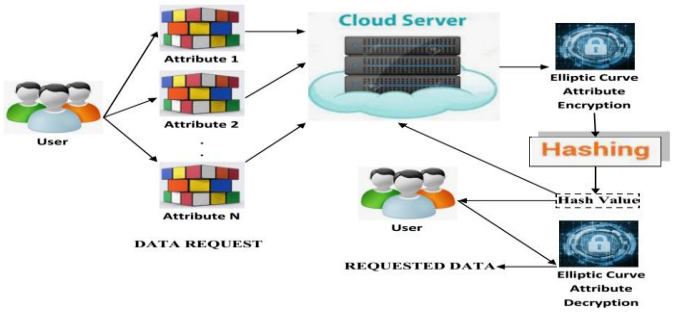
Pradeep et al. [8] proposed a novel key generation and cryptosystem that combines the GCD and LCM between in principal key-value pair and first arithmetic quasi attributes. Which is moderately vulnerable information in the cloud to provide secure storage via effective ABE. Furthermore, a new sophisticated technique Elliptic Curve Cryptography with the Base100 Table technique to execute cryptographic processes above one of the confidential data for users. Sandhya et al. [9] propose that Elliptic Curve Encryption using Multi-Authority Ciphertext - Policy attribute Attribute-Based Encryption (ECC-MA-CPABE) is best for cloud security as it has a lower key length, more privacy, and takes less time to compute. The information is encrypted based on attributes that the owner selects at the time of submission. Only at the moment of data uploading has ECC-MA-CPABE fixed the attribute selection.

Yujiao Song et al. [10] devised a new ABE technique that safeguards user privacy when providing keys. They segregate the functions of key generation and attributes audit to make sure that neither the KGC nor the attribute audit centre can see the client attributes or access the client private key. This is suitable for several privacy situations, including those involving commercial large datasets. Rui Cheng et al. [11] developed a novel CP-ABE system based on ECC, which substitutes the bilinear pairing process and decryption work is outsourced to edge devices. Furthermore, the suggested approach combines time and location features, allowing users to request data within the period and geographical parameters set by the involved parties, resulting in a finer-grained accessibility control process. For fine-grained access control, Tran Viet et al. [12] used ABE. The secret keys can be punctured to disable decryption for certain messages, recipients, or periods, ensuring that essential messages remain protected even if the existing key has been exposed. They devise a novel method for combining punctured keys and attribute-based in such a way that key size is alike to that of the original ABE.

III. System Model

The EAE technology was created to provide extremely secure confidential data transport in the cloud. In the EAE approach, elliptic curve attribute cryptography is utilised to improve the secrecy of transmission in a cloud. The elliptic curve attribute cryptograph is a public-key cryptography technique that relies on the algebraic creation of elliptic curves over constrained fields. To ensure security in cloud service provisioning, the Elliptic curve attribute cryptograph requires fewer keys. Encryption, digital signatures, pseudo-random generators, and other applications use elliptic curves.

The attribute cryptography of the elliptic curve is a asymmetric encryption that uses attributes to determine a cipher texts and cloud user's secret key [13-16]. Only if the user key's set of attributes matches the properties of cipher text can a cipher text be decrypted. Collusion-resistance is an elliptic curve attribute encryption. As a result, the EAE technique prevents unauthorized data access, resulting in a higher level of data confidentiality in the cloud [17]. In addition, the EAE technique uses the Hashing function to improve the protection of data communication in the cloud environment.



ISBN: 978-1-6654-6633-2 PART: CFP22P42-ART

Fig. 2. Structure of EAE technique

The EAE technique's architecture diagram for presenting the secured answer from the server to the client is in Fig. 2. The client request is initially the number of attributes sent to the cloud server. The ECA encryption is to achieve improved data confidentiality. Using the hash function to calculate the hash value for the encrypted data, ensuring security throughout transmission. As a result, the EAE approach increases data security and confidentiality in cloud service delivery.

A. Simple Hashing

The EAE approach uses simple hashing to ensure the security of cloud service provisioning. For storing cloud data, it is a space-efficient probabilistic data structure. To save the input data, the simple hash function generates a hash value. It takes any input string as input and produces a fixed-length output string known as a hash value. The data properties are initially fed into the simple hash function, as shown in Fig. 3. A one-way function is the simple hash function. Collision resistance is a characteristic of hashing functions that prevent intruders from accessing cloud data. As a result, hashing is also known as collision-free hashing. The hashing produces a fixed-size result.

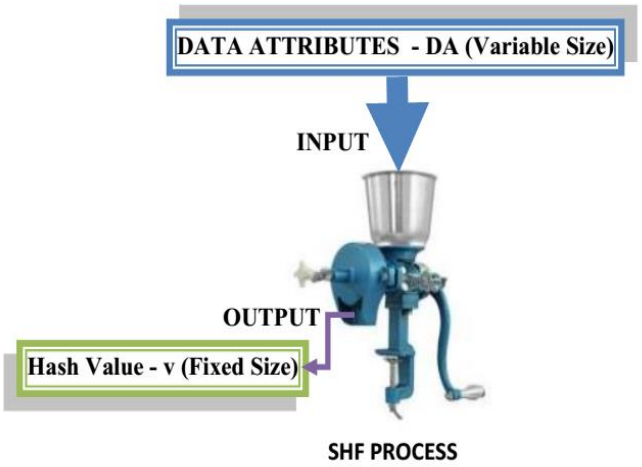


Fig. 3. Simple Hash Function

B. Elliptic Curve Attribute Encryption / Decryption Technique

Elliptic Curve Attribute Encryption is used in the EAE approach to improving data confidentiality while transmitting over the internet. The data attributes to be encrypted are considered plaintext in the EAE approach. The original data characteristics are turned into encrypted text during the elliptic curve attribute encryption procedure [18]. The encrypted ciphertext is then decoded using the elliptic curve attribute decryption to obtain the plaintext. The encryption and decryption are carried out using the Elliptic Curve Attribute Encryption/Decryption method and a simple hash function. In order to improve data security in the cloud environment, the EAE approach is used in the basic hash function to provide the hash value for encrypted data. The term "security" refers to the confidentiality and availability of data stored in clouds, as well as the major challenges that must be addressed in order to improve the performance of cloud service provisioning. Fig. 4 depicts the Elliptic Curve Attribute Encryption procedure.

Initially, the cloud sender provides the encrypted data attributes that the user has requested. The ciphertext is then encrypted using elliptic curve attribute encryption. using the simple hash function to generate a hash value for encrypted ciphertext. Finally, the cloud service provider receives the created hash value. The value of encrypted data's hash is obtained by the cloud service provider and communicated to relevant cloud users in the cloud environment.

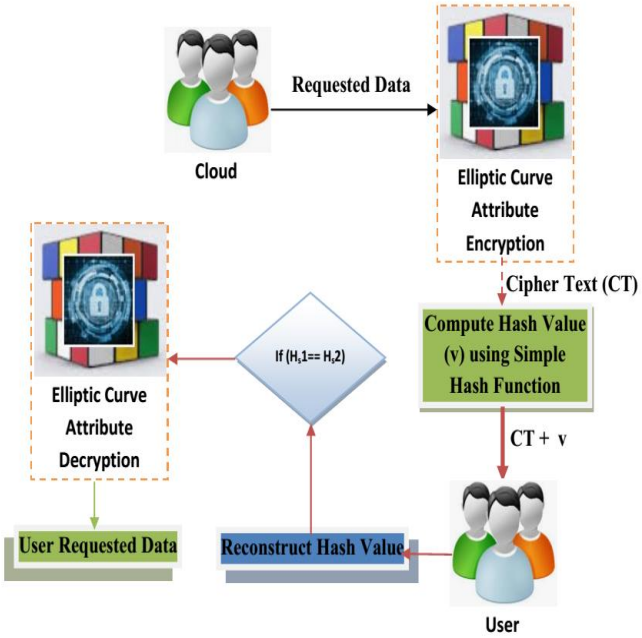


Fig. 4. Elliptic Curve Attribute Encryption and Decryption using Simple Hash Function

Using EAE approach for attribute encryption and decryption. The elliptic curve attribute cryptography algorithm is a method of encrypting and decrypting data as well as exchanging cryptographic keys that relies on the algebraic construction of elliptic curves over constrained fields. The equation produced from the mathematical group acquired from the spots where the line meets the axis in elliptic curve attribute cryptography. The equations based on elliptic curves have a unique property using cryptography. A plane curve over a finite field is called an elliptic curve that consists of points meeting the equation, which is technically expressed as,

$$z^3 = y^3 + by + c \quad (1)$$

Elliptic curve attribute cryptography chooses a number 'p' from the range of 'r' for key creation. The following equation was used to generate the key in elliptic curve attribute cryptography:

$$K = p * o \quad (2)$$

p is the random number picked from the range of (1 to r - 1) in equation (2). The point on the curve is denoted by o, while the public key is denoted by K, and the private key is denoted by p. Assume that 'a' is the set of characteristics to be encrypted, with the point 'A' on the curve 'E', and choose 'rk' at random from [1 to (r -1)]. The elliptic curve attribute encryption

ISBN: 978-1-6654-6633-2

PART: CFP22P42-ART

method produces two cipher messages, C_i1 and C_i2, which are mathematically expressed as follows,

$C_i1 = rk * o$; $C_i2 = a + rk * K$ (3)

Two cipher messages, C_i1 and C_i2, are obtained from equation (3). After encryption, the hash value is computed using a basic hash function and stored on a cloud server, from which it is transferred through the internet to the appropriate cloud users in a cloud environment. Consider the two cipher texts C_i1 and C_i2, both of which are represented by the letters C_i.

$C_i = (C_i1, C_i2)$ (4)

Because the simple hash function (SHF) gives a variable-length block of input cipher text (C_i), the output hash value can be fixed in size.

$H_s1 = SHF(C_i)$ (5)

H_s1 computes the hash code of data encrypted using equation (6). After determining the hash value of the data encrypted, it is placed in a cloud service provider. When a user accesses data saved in the cloud, the hash value is regenerated using the same simple hash algorithm to ensure that the data received is valid. As a result, the recomputed hash value is expressed mathematically as,

$H_s2 = SHF(C_i')$ (6)

Two hash values are compared on the receiver side to guarantee that the data is valid. Decryption is used to recover the original data if the two hash values are equivalent. As a result, only lawful users that utilise elliptic curve attribute decryption can see the data's cipher text (C_i). To get the original message, which is mathematically defined as, the elliptic curve attribute decryption techniques are used

$a = C_i2 - p * C_i1$ (7)

IV. Experimental Results

The EAE technique's outcome analysis is assessed in this section. The EAE methodology is compared to two current methods: the Multi-Authority Ciphertext Policy Attribute-Based Encryption (MA-CPABE) scheme [9] and the Elliptic Curve Cryptography Secure Transmission (EC-SET) scheme [8]. The effectiveness of the EAE approach is assessed using measures such as execution time and memory use.

Table 1: Experimental settings

CPU	Intel(R) Core i5- 2.30 GHz
Software	Windows 7 64-bit and Jira
Memory	16.00 GB
Cloud Service	Microsoft Azure
Data bit length	< 128 bits

A. Execution Time

The execution time in the EAE technique refers to the time it takes to encrypt data in order to achieve secure data transfer in cloud service provisioning. The execution time is stated mathematically as, and is measured in milliseconds (ms).

Execution Time = Time taken for Elliptic Curve Attribute (ECA) Encryption – start time of ECA (8)

Fig. 5 shows the influence of encryption time vs different file sizes in the range of 100-500 KB using three different approaches. Compared to the two existing approaches, MA-CPABE and EC-SET, the suggested EAE technique provides a faster execution time for encrypting data, resulting in enhanced cloud data security. Furthermore, with all three approaches, increasing the file size of the data for encryption increases the execution time. However, the EAE technique takes less time to execute.

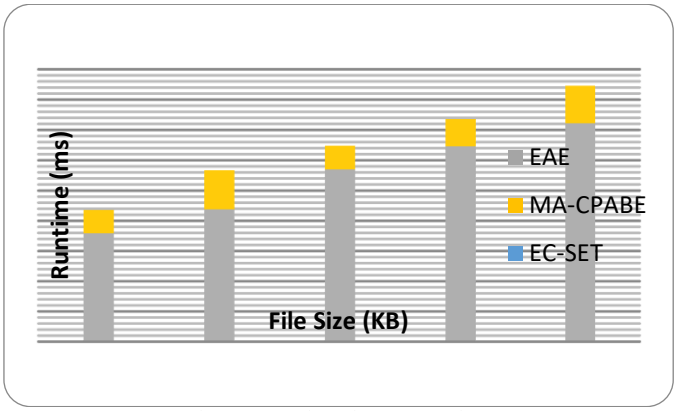


Fig. 5. Execution Time Comparison

B. Memory Utilization

Memory utilization in the EAE approach refers to the amount of memory used to store the hash value of data encrypted on the cloud server. The memory usage is expressed in KiloBytes (KB) and is mathematically described as follows,

Memory Utilization = Total memory − memory unused (9)

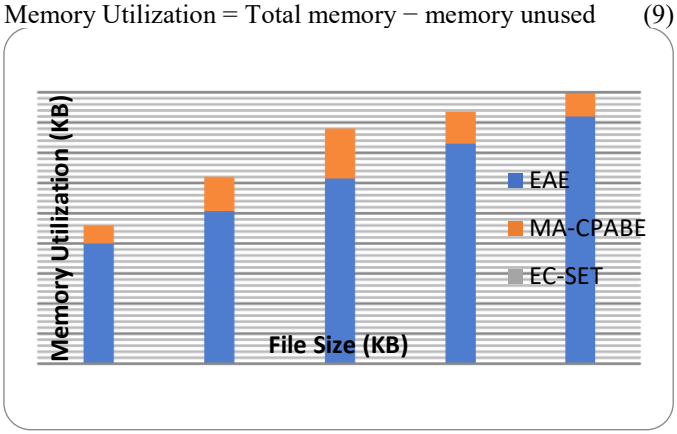


Fig. 6. Memory Utilization Comparison

Fig. 6 shows the impact of memory use on secure cloud service provisioning for file sizes ranging from 100 to 500 KB utilizing three different ways. Compared to the two current approaches, MA-CPABE and EC-SET, the suggested EAE technique provides superior memory use, as shown in the figure. Furthermore, increasing the file size of the data for encryption increases the space complexity when using any of the three ways. However, memory use employing the EAE technique is found to be lower. The hash function is to obtain the hash value for storing cloud data efficiently.

ISBN: 978-1-6654-6633-2

PART: CFP22P42-ART

V. CONCLUSION

EAE was proposed as a new encryption method for offering safe data access. The primary goal is to improve the protection of cloud data transactions. An elliptic curve attribute encryption is to encrypt the user-requested data. The hash function is worn to calculate the hash-code for the data encrypted and store it in the cloud. Transmit the hash value subsequently to users in the cloud to strengthen the data transfer security in the cloud. The suggested encryption technique has the following key advantages over other techniques. The performance of existing and suggested strategies is investigated and assessed in experiments. When comparing the results of the suggested EAE approaches to the results of the other techniques, it is clear that the proposed EAE techniques produce better outcomes. Improving our work in the future by including the techniques for access restriction based on anonymity to reduce the key generation complexity. This will be strengthened in the future with supplementary safe validation, such as one-time passwords for clients who log in multiple times.

REFERENCES

[1] 1) Kavin B., Ganapathy S., Kanimozhi U., and Kannan A., "An Enhanced Security Framework for Secured Data Storage and Communications in Cloud Using ECC, Access Control and LDSA," Wireless Personal Communications, vol. 115, pp. 1107-1135, 2020.

[2] Lian H., Wang Q., and Wang G., "Large Universe Ciphertext-Policy Attribute-Based Encryption with Attribute Level User Revocation in Cloud Storage," The International Arab Journal of Information Technology, vol. 17, no. 1, pp. 107-117, 2019.

[3] Liu H., Ning H., Yue Y., Wan Y., and Yang L., "Selective Disclosure and Yoking-Proof based Privacy-Preserving Authentication Scheme for Cloud Assisted Wearable Devices," Future Generation Computer Systems, vol. 78, no. 3, pp. 976-986, 2018.

[4] S. Arun and N. R. Shanker, "Data security in cloud storage using elliptical curve cryptography," International Journal of Pure and Applied Mathematics, Vol. 120, No. 6, pp. 27-38. 2018.

[5] Nikos Komninos, "Preserving Privacy of Data with Efficient Attribute-based Encryption Schemes," UMAP '21 Adjunct, June 21–25, pp. 366-367, 2021.

[6] Sadia Syed and M. Ussenaiah, "Dynamic hierarchical attribute set-based ECC encryption for secure cloud storage," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, no. 9, 2016.

[7] Athena J, Sumathy V and Kumar K, "An identity attribute–based encryption using elliptic curve digital signature for patient health record maintenance," Int J Commun Syst., pp. 1-22, 2017.

[8] Pradeep Suthanthiramani, Muthurajkumar Sannasy, Ganapathy Sannasi and Kannan Arputharaj, "Secured Data Storage and Retrieval using Elliptic Curve Cryptography in Cloud," The International Arab Journal of Information Technology, Vol. 18, No. 1, 2021.

[9] Jeevan Kumar, Rajesh Kumar Tiwari and Vijay Pandey, (2021), "Blood Sugar Detection Using Different Machine Learning Techniques" Int. J. of Electronics Engineering and Applications, Vol. 9, No. 3, pp. 23-33, DOI 10.30696/IJEEA.IX.III.2021.23-33.

[10] Yujiao Song, Hao Wang, Xiaochao Wei and Lei Wu, "Efficient Attribute-Based Encryption with Privacy-Preserving Key Generation and Its Application in Industrial Cloud," Security and Communication Networks, vol. 2019, pp. 1-9, 2019.

[11] Xiong LIU and Haiqing LIU, (2021), "Data Publication Based On Differential Privacy In V2G Network" Int. J. of Electronics Engineering and Applications, Vol. 9, No. 2, pp. 34-44, DOI 10.30696/IJEEA.IX.I.2021.45-53.

[12] Tran Viet Xuan Phuong, Rui Ning, Chunsheng Xin and Hongyi Wu, "Puncturable Attribute-Based Encryption for Secure Data Delivery in Internet of Things," IEEE INFOCOM 2018 - IEEE Conference on Computer Communications,Honolulu, HI, USA, 2018.

[13] H. Deng, Z. Qin, L. Sha and H. Yin, "A Flexible Privacy-Preserving Data Sharing Scheme in Cloud-Assisted IoT," in IEEE Internet of Things Journal, vol. 7, no. 12, pp. 11601-11611, Dec. 2020, doi: 10.1109/JIOT.2020.2999350.

[14] J. Aruna Jasmine, V. Nisha Jenipher, J. S. Richard Jimreeves, K. Ravindran and D. Dhinakaran, "A traceability set up using Digitalization of Data and Accessibility," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), 2020, pp. 907-910, doi: 10.1109/ICISS49785.2020.9315938.

[15] Dolly Daga, Haribrat Saikia, Sandipan Bhattacharjee and Bhaskar Saha, (2021), "A Conceptual Design Approach For Women Safety Through Better Communication Design" Int. J. of Electronics Engineering and Applications, Vol. 9, No. 3, pp. 01-11, DOI 10.30696/IJEEA.IX.III.2021.01-11.

[16] Xiong LIU and Haiqing LIU, (2021), "Data Publication Based On Differential Privacy In V2G Network" Int. J. of Electronics Engineering and Applications, Vol. 9, No. 2, pp. 34-44, DOI 10.30696/IJEEA.IX.I.2021.45-53..

[17] XIAOYU YANG, (2021), "Power Grid Fault Prediction Method Based On Feature Selection And Classification Algorithm" Int. J. of Electronics Engineering and Applications, Vol. 9, No. 2, pp. 34-44, DOI 10.30696/IJEEA.IX.I.2021.34-44.

[18] H. Xiong, H. Zhang and J. Sun, "Attribute-Based Privacy-Preserving Data Sharing for Dynamic Groups in Cloud Computing," in IEEE Systems Journal, vol. 13, no. 3, pp. 2739-2750, Sept. 2019, doi: 10.1109/JSYST.2018.2865221.