International Journal of Engineering, Science and Mathematics
Vol. 12 Issue 6, June 2023,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

STUDY THE EFFECTIVE ATTRIBUTE-BASED BROADCAST ENCRYPTION FOR DYNAMIC GROUPS

Kumud Gupta, (21RCHPHDCA010) and Dr.Shweta Mishra
Department of Computer Science and Applications
Desh Bhagat University, Mandi Gobindgarh

ABSTRACT

The ease of sharing data with other users is a major benefit given by cloud providers. As compared to older approaches, an efficient ABBE may be utilized for both optimum secure conference calls and large-scale systems in which the encryptor is not necessary to explicitly provide the list of decryptors. The total number of stored public keys increases at most by O(logN) even when the number of users is quite huge (N). Compared to ABE and other key management systems used by the Broadcast Group, E-ABBE was shown to be more effective in tests measuring performance. In this work, the author presents a new method for implementing safe cloud-based data sharing, one that makes use of the efficient attribute-based broadcasting encryption algorithm.

Keywords: E-ABBE, algorithm, cloud, dynamic groupings.

1. INTRODUCTION

As cloud computing matures as a marketable technology, a growing number of service providers have emerged to meet consumer demand. For this reason, most large businesses are shifting towards more cost-effective methods of using resources like data storage, maintenance, and computing.[1]

Information Exchange among Evolving Communities

With the benefits offered by cloud providers, data storage has emerged as one of the most crucial technologies. Several Owners may add to, delete from, or otherwise interact with Cloud-stored data. This means that providing access depending on the person, group, or position seeking it would be fraught with security risks.[2]

The majority of businesses now facilitate cloud-based file sharing between coworkers with shared goals and responsibilities. Data storage facility maintenance and problem solving are rendered unnecessary by this method. The only thing to worry about while storing data on the cloud is the potential lack of privacy and security. [3]

While it has been suggested to prevent unwanted and uncontrolled access by encrypting data before uploading the files, the actual practicality and the amount of safety offered by this strategy are unclear. In the sections that follow, we'll present the difficulties associated with dynamic groups and the fundamental group key management technique, highlighting both the data sharing and key management aspects.[4]

Case of Information Exchange

Users with similar interests or personalities may be gathered into groups for simple security administration. When defining a group, the primary emphasis is on the identities of the people in the group, who are the owners of the data. The practice of sharing information inside a group has gained popularity in many fields, including business, government, academia, etc. The following demonstrates the data exchange among the numerous dynamic groupings. In this, the root node indicates a group which is later separated into several sub-divisions. Each subgroup consists of numerous consumers consuming the data. Several people from different organizations may claim ownership of the same material in a cloud storage service like Google Drive or Dropbox. For instance, if all data owners share ownership of data generated at time X, then all data created at that moment belongs to all data owners.[5]

Users are denoted by U, whereas groups are denoted by G,

$$\text{where } G \in \{g_1, g_2, g_3 \ldots . g_i\}, \qquad 1 \leq i \leq n$$

with n being the total size of the collections.

$$g_i \in \{u_1, u_2, \ldots . u_j\}, \text{where } 1 \leq j \leq k$$

X represents data generated by users belonging to distinct groups, and k represents the size of group i.

X={U51,U23,U34,...Uij}

where I is the group identifier and j is a User or group member.

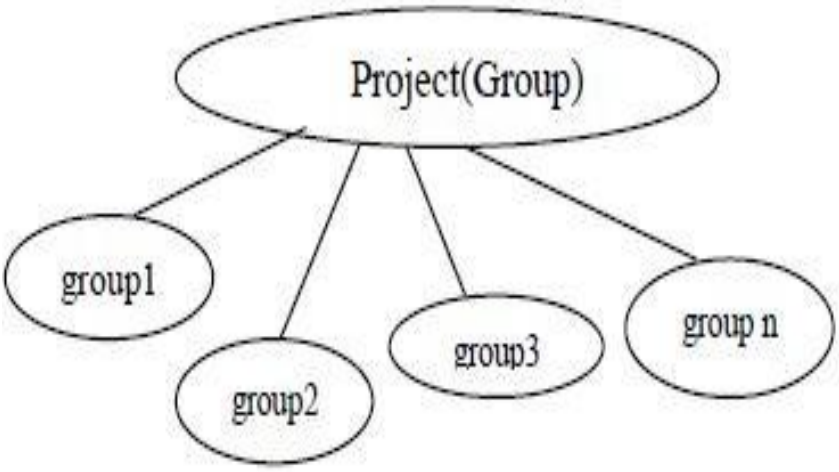

Figure1.1:Mutual information sharing

In the context of data use, for instance. A company's "cloud" is a place where employees from the same division, branch, or team may go to store and exchange data. That's how long the company's employees won't be able to work on repairs and other storage-related problems. Yet, online storage raises privacy concerns for documents.

Group Key Administration

Particularly difficult is the management and coordination of data assimilation and distribution in group communications, when all the organizations involved have equal access to the data stored in the cloud. Data may now be accessed on an as-needed basis, with various members of a group granted varying degrees of access and responsibility in accordance with established protocols, greatly reducing the severity of this issue.[6]

With a single broadcast, broadcast GKM (BGKM) methods produce a new system key that does not compromise the secret key shared with current members. Currently available BGKM methods need the dissemination of O(n) public information during rekeying. Subset-cover techniques add complexity to the process. It is on the basis of such augmented BGKM schemes that AB-GKM may be implemented, allowing for efficient handling of fluctuations in dynamic groups. They are unable to deal with qualities that have expressive parameters, however. When encrypting a communication, it is sometimes preferable to not have complete information about the characteristics of the group of recipients. By encrypting based on a set of attributes, Attribute Based Encryption (ABE) allows for communication to be secured without the receivers being fully aware of the fact that they are being encrypted. The value ofthe primary advantage of ABE schemes over standard

PKC primitives is the greater degree of scalability afforded by its one-to-many encryption. In these methods, decryption is only possible if the user-specified private key corresponds with the cipher texts designated with sets of descriptive properties.

For dynamic group keys, Cipher-Policy attribute-based encryption is a method used to overcome administrative and privacy problems.[7]

Tree-based building, which is based on the FlatTable method, is used to maximize the efficiency of cloud-based data storage and transmission. We apply a reduced Boolean function in a sum-of-product-expression (SOPE) to reduce the number of encrypted key-update messages. It is the remaining members' IDs that are used to calculate the SOPE. For the GMs remaining in the group, this means they may use their private keys to decrypt the GK once it has been updated by including the n previously transmitted secrets.

For each given GU 'u,' there exists only one possible set of bit assignments Su that define that GU ID.[8]

2. MATERIAL AND METHODS

Algorithms Used for Encryption and Decryption

- **Setup()**

Each user in an E- ABBE with N users has a unique n-bit binary ID where bi denotes the i'th bit in a user' sID and n = logN. Each user is represented by a unique set of n bit-assignment characteristics called " $Batt_1$,$Batt_2$,....$Batt_n$ where n is the number of users. Figure 3.3 below illustrates a system with 8 potential users and a 3-bit assignment.

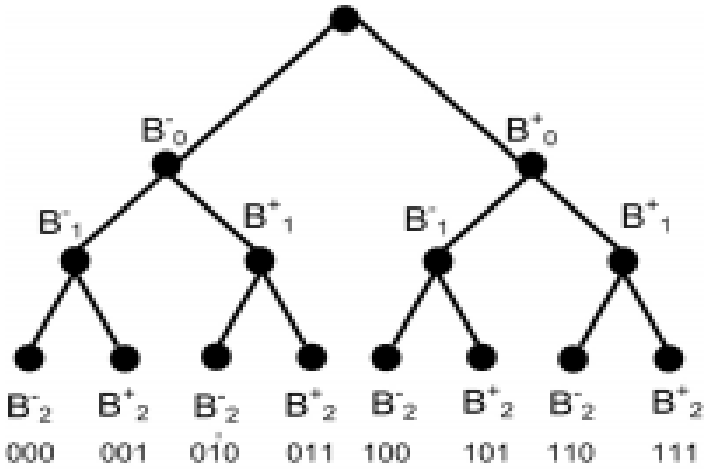

Figure2.1A bitmap having an E-ABBE property

The bit-assignment characteristics are chosen, and the TA also chooses m descriptive attributes. The descriptors stand in for the actual characteristics.

E-A BBE Setup Algorithm

Input: Security Parameter

K Output: Pk & MK

1. Build a generator for a bilinear map e: G0 × G0 →G1 of prime order p.

2. Choose some numbers at random ; α;β ∈ Zp.

3. Determine the system's public key using the formula PK = ⟨e,G0,G1,H,g,h = gβ ,ζ = e(g,g)α ⟩ as well as the secret master key MK = ⟨β ;gα ⟩, where H : {0;1}∗→G0.

4. Picks a random number yB ∈ Zp that isn't a prime, Batti ∈U represents a bit assignment.

If his or her bi value is 1, then good qualities are represented by Batt I +. If the person's bi value is zero, they will be given the Batt - for undesirable characteristics.

A person gets the Batti, the "don't care case of characteristics," if the bi equals 0.

5. Represent the default values for the public parameters as PK = (g,g1,....gK,gK+2...,g2K,v) ∈ G2K+10 :

MK = {γ ,α} is kept secret by the GC or TA

- **KeyGeneration:**

To verify the identities of its members, the Group uses its own identifiers, and the TA then collects the secret key SK for each member, based on their attributes. The user's ID, the master private key pr, and a list of user characteristics, L u, are required inputs for the method. The TA determines the secret key for the identification (ID), and then determines the key that corresponds to the user's characteristics, as shown below. The TA picks at random and calculates for each separate property.

Fig. Algorithm for Generating E-ABBE Keys

Input: Lu, the attribute list of the user.Output: Secret Keys, SK_u.

1. For user i = 1; : : : ;n: with the attribute list Lu = {Lu[i]i□[1;k]
2. Choose k random numbers r_k and $r_j \in Z_p$, ∀ j ∈ S attribute set S
3. Computes $D = g^{\gamma r} = v^r$
4. Calculates $D_i = g^{\gamma(\alpha Lu[i]+ri)} = g^{\gamma} Lu[i] \cdot g^{\gamma ri}$ and $F_i = g^{\gamma(\alpha 2k+i+ri)} = g^{\gamma}{}_{2k+i} \cdot g^{\gamma ri}$.
5. Calculate $SK_i = SKu = (D; \{D_i\}_{i\in[1;k]}; \{F_i\}_{i\in[1;k]})$

- **Encryption:**

The set of recipients is identified for some set S by the membership functions fnS(), written in SOPE form:

$Fns(b^u_1, b^u_2, \ldots\ldots, b^u_n) = 1$ iff $u \in S$;

= 0 iffu ∉ S

Ifthesubgroup$S=\{000;001;011;111\}$,then$fS=b\bar{0}\bar{b}1\bar{b}2+b\bar{0}\bar{b}1b2+b\bar{0}b1b2+b0b1b2$.

E-A BBE Encryption Algorithm

Input: Message M, AP

Output: Ciphertext (CT)

1. Choose random t in Z_p.
2. Sets the one-time symmetric encryption key Ekey= $e(g_k;g_1)^{kt}$3. Sets $C_0 = g^t$, $AP=\{AP_i, 1\le i \le n\}$
4. Computes $C_1= (v\Pi_{j\in AP\ gK+1-j})^t$.
5. Calculates CT=(AP, {M}Ekey, gt, $(v\Pi_{j\in AP\ gK+1-j})^t$) =AP, {M}$E_{Key}$, Header)
6. Broadcast to the receivers'

- **Decryption**

When a ciphertext is encrypted, the decryptor u knows just a subset of the whole access policy that is being enforced on it. In order for u to successfully retrieve the correct plaintext and the access policy, ALu |= AP must hold. Otherwise, all u have is a totally

arbitrary string that's trivially detectable. Users whose identities conform to the access rules included in the CT calculate the key via bilinear pairing with their own secret keys.

AlgorithmDecrypt (PK,CT,SK)

1. ‘TheUserwithCT□Suthen returns
2. For∀i∈[1;k], ucalculatestheT$_0$=e(g$_{AP[i]}$;C1)and
3. ifAP[i]□AL$_u$,ucomputes T$_1$,T$_1$=e(D[i]·Π$_{j\leq AP;j\square=AP[i]}$gK+1−j+AP[i];C$_0$)
4. elseifAP[i]∈{A*}i∈[1,k]
5. computes:T$_1$=e(F[i]·Π$_{j\in AP;j\square=AP[i]}$gK+1−j+P[i],C0)

calculateT$_0$/T$_1$=e(g,g)−tγr$_i$+tαK+1 e(D,C0)=e(g,g)tγr:

6. Decrypts the cipher text and gets by computing

Key= e(g;g)^{kt}αK+1=e(g$_K$;g$_1$)$^{kt'}$

Optimal Storage

ID must not share a prefix with the -bit assignments of any of the other users, so that it may be used to uniquely identify a single user. If user un is given ID000, then user u1 will have prefix 00 while user u2 will have prefix 001. It should also be noted that no group of users may have the same bit assignment.

In order to utilize the bit assignments to refer to the user, it is required to ensure that the criterion for no prefix is met.

A user's likelihood of becoming the final destination is represented here by qi. Attribute bit assignments in the broadcast cipher must use the pi-function.

3. RESULTS

Multiple factors are considered when determining a system's performance, such as the number of cryptographic processes needed to perform operations like encryption and decryption and the size and number of messages generated by leave and join operations (collectively referred to as the overhead communication) (computation overhead). A group's size, marked by N, and the number of members departing the group, indicated by l.

Budgetary Concerns for the GM's Office's Storage Space: Under the context of the current method, the Group Manager (GM) keeps I the CP-ABE system's public key (PK) and master keys (MK) and (ii) a list of Group Users (GU). The current group size, M, determines how much data may be stored in the GC, as CP-public ABE's and master keys are the same size.

Data Retention Expenses (DREs) of a User or Group Member (GU): Each user in the suggested system keeps a secret key(SK) made out of the group's total of (2n+1) items hidden.

Throughout the Joining process, there is an abundance of communication (Join) For the suggested approach to work, just one multicast message encrypting a new key with the previous DEK key has to be sent. A tree-based system has a non-uniform message complexity.

Assume that L is the total number of GMs whose access has been revoked in response to this message. Ignoring the Minimization Function Every departing GM requires 2L.n messages to be sent. One symmetric key is used for each message. Based on the departure of certain GMs, BFM minimizes the volume of communications.

3.1 Security analysis

1) **Data confidentiality:** The suggested system faces two types of danger: those coming from inside, and those from beyond. The Cloud Service Provider poses an internal hazard, while malicious outsiders provide an external one.

   It is a simple matter to ensure that no unauthorized user with insufficient qualities may see the shared data. The CSP will be unable to get (,) s t e g g for the user if the user's set of attributes does not conform to the ciphertext's access policy.

   The peculiar CSP poses a second hazard to the combined stockpile. Nevertheless, the suggested classification encrypts sensitive data using KD and then secures it using an accession policy.

2) **Collusion resistant**: To get the secret key, two or more users may pool their secrets using a cloud service that cannot be trusted completely but does have some good faith operators. Consistent with the defined procedure, it yields the expected results. A user u′ comes to the CSP with his blinded private key SK and a guess as to whether or not the access policy meets an access tree T.

3) DSP is plenty of jargon, such the blinded private key SK u′. However D = gt(+r)= is associated with tr′ and t, and the rest of the component of all private keys, therefore fSK is not a valid private key.

4) Hence, the secret key cannot be determined using DLP hardness over G0 and G1.

5) In this part, we compare the efficiency of E-ABBE to that of many other broadcast encryption schemes, including. Every time a user has an interaction with a user in a subgroup, the communication cost, storage overhead, and compute overhead associated with that interaction is included into the performance evaluation. N denotes how many people are in the group.

Over-the-Air Message Transfer:

When utilizing E-ABBE to control receivers S, the amount of messages transmitted is determined by the minimum number of product statements in fmin S. The authors offer upper and lower bounds on the typical size of the model parameters in the reduced SOPE in. According to the data, the average amount of messages per network is log(N).

3.2 Estimated Total Messages:

Total Message Size

Finally, in Figure, we have a visual representation of a comparison between the message sizes of E-ABBE and CP-ABE, as calculated using the Flat table presented in. In CP-ABE with FT, the ciphertext grows linearly with the number of characteristics in an access policy, as stated. CP-ABE messages with FT begin at 630 bytes in size, growing by an average of 300 bytes for each additional characteristic. Attributes employing FT-CP-ABE cipher text may quantify up to 10 and the message size may huge up to 630+9300=3330 bytes in any organization with 10 bit ID or 1024 users. It is evident that FT-CP-ABE is an extremely efficient protocol (log2N) due to its low communication overhead and the logN-bounded amount of characteristics in the access policy.

Every E-ABBE ciphertext consists of a pair of group members onG0. As a rule of thumb, G0 occupies around 128 bytes of space. Hence, the ciphertext in an E-ABBE cannot be more then 300 bytes, which is significantly smaller than the ciphertext in a CP-ABE that employs FT. E-message ABBE's size may be reduced further with carefully crafted communication protocols, but ComponentC0 in the cipher - text can be revealed by a flood of messages.

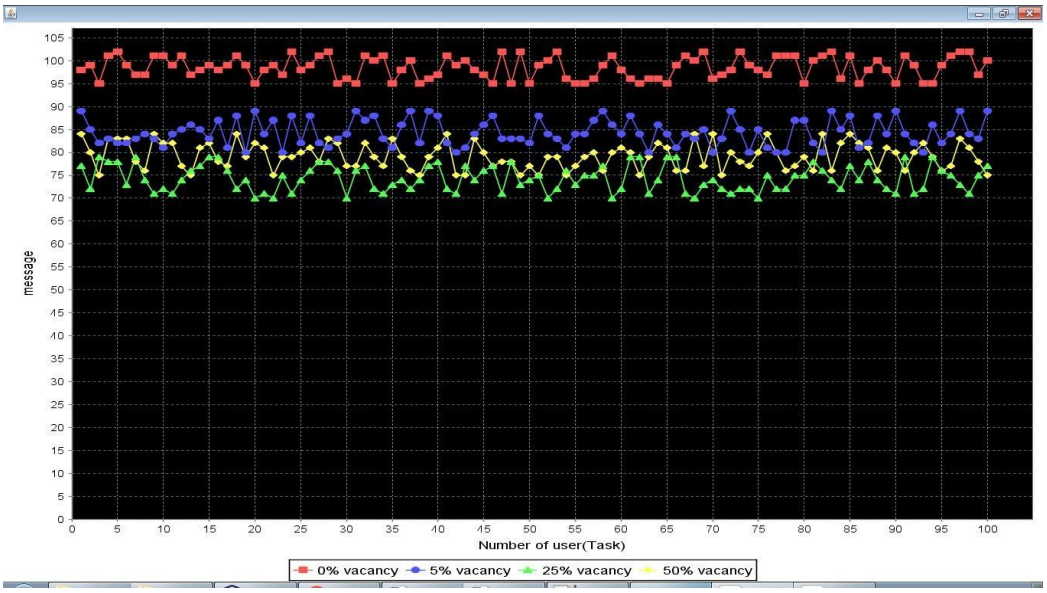

Figure3.1: Dimensions of a complete message in an E-ABBE network

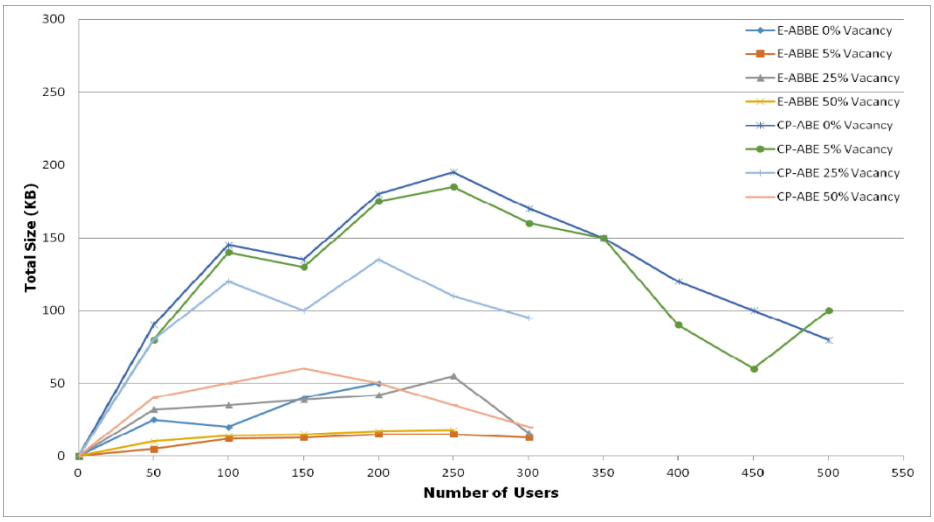

Figure3.2: Dimensional analysis of E-ABBE and CP-ABE messages.

3.2 Overhead Storage

The PK of an E-ABBE has a size of 6logN+1, making up G0. Users should keep track of mN identifying characteristics. Yet, if users don't keep track of their own IDs, the storage cost is just O(logN+m). 'An ID and a list of IDs for which you don't care need to be stored in order for a broadcast cipher to perform Boolean function minimization, however it may be argued that this doesn't add any extra storage cost to the cipher.

Encryptors may save up storage capacity by not storing receiver IDs after a broadcast has occurred.

Table 3.1: The planned system, along with a number of famous works, is being kept in a central location.

Scheme	Storage Overhead
E-ABBE	O(logN+m)
DPP_2	O(l)
Subset-Diff	O(tlogtlogN)
NNL_1	$O(\log_2 N)$
BW_2	$O(N^1)$
BW	$O(N^{1/2})$
DPP_1	O(N)
ACP	O(l)

Where N is the total number of members, l is the total number of users who have left, and t is the most possible number of conspirators who might decipher the ciphertext.

3.3 Computation Overhead

This subsection elaborates on Table, which lists a comparison of the computational burden of inferences using symmetric and asymmetric approaches. BGW methodology demands more processing power and flexibility than ACP method due to the necessity for O(N) operations over the bilinear group, 'Instead, the number of finite field operations in the ACP approach is just O(N2). Decryption from an E-ABBE needs 2logN+1 pairings, logN(logN1)+logN operations onG0, and logN operations onG1. Thus, the difficulties of decryption and encryption can only be increased to a certain point when O is involved (log N). Despite widespread familiarity with the topic and an effective approximation, decreasing SOPE remains an NP-hard challenge.'

Table3.2: Computer Processing Time

Scheme	Computation Overhead	
	Decryption	**Encryption**
E-ABBE	$O(\log N_u)$	$O(\log N_u)$
ACP	O(l)	$O(N_u^2)$
BGW	$O(N_u)$	$O(N_u)$

Several cloud-based data-sharing systems have been compared to this one on a variety of metrics, including the cost of user revocation, the security of data, the privacy of users, and the ease of partial decryption. One coupling operation is represented by PA symbol, single exponentiation by E symbol, characteristics in access policy T of ciphertext quantified by m symbol, and user represented by U symbol.

3.4 RESTRICTIONS SEEN WHILE USING E-ABBE

As a result, the following restrictions on E-ABBE are noted:

- The privacy afforded by Attribute-Based Encryption systems, including E-ABBE, is discussed.
- The suggested method E-adaptability ABBE's means that it may be used with a wide range of abstraction levels and cipher suites.
- All possible user group formations are supported with the minimum amount of storage space.
- The User may safely outsource Cp-ABE encryption and decryption to the cloud without disclosing the private key or the contents of the data being encrypted or decrypted.

4. CONCLUSION

We introduce an Attribute-Based Broadcast Encryption (ABBE) method based on BGKM to solve the problem of key management in collaborative groups that are constantly changing. A variety of BE systems are compared to the E-ABBE scheme. As compared to current BE systems, this method is shown to have a less storage overhead. Analyzing the results, we see that the E-ABBE method is effective in lowering the storage complexity from linear to logarithmic, allowing for expressive attribute-based access restrictions while minimizing the effort required for key management.

We briefly explore the constraints that must be placed on the introduction of the E-ABBE program. Another option for data security is to encrypt the data at the User ide. Hence, the client stores the decryption keys locally, rather than on the cloud. Even if privacy is ensured via encryption. Especially when information is being shared across different groups of active users. It's a challenge, but it gets tougher. Taking into account the possibility of dynamic and adaptable data exchange across many organizations. The E-ABBE method can only be used to keep sensitive information secret. Thus, it is crucial to

preserve user privacy to emphasize that maintaining data secrecy is not just'- the security challenges for sharing data across numerous dynamic groups.

REFERENCES

1. Shamir and Y. Weiss, "A New Scheme for Dynamic Broadcast Encryption," Advances in Cryptology—CRYPTO 2021, Springer Berlin Heidelberg, 2021, pp. 1-13.
2. D. Boneh and M. K. Franklin, "Identity-Based Encryption from the Weil Pairing," Advances in Cryptology—CRYPTO 2020, Springer Berlin Heidelberg, 2020, pp. 213-229.
3. B. Waters, "Efficient Identity-Based Encryption Without Random Oracles," Advances in Cryptology—EUROCRYPT 2019, Springer Berlin Heidelberg, 2019, pp. 114-127.
4. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," IEEE Symposium on Security and Privacy, 2017, pp. 321-334.
5. M. Chase, "Multi-Authority Attribute-Based Encryption," Theory of Cryptography Conference, Springer Berlin Heidelberg, 2017, pp. 515-534.
6. D. Boneh, X. Boyen, and H. Shacham, "Short Group Signatures," Advances in Cryptology—CRYPTO 2004, Springer Berlin Heidelberg, 2019, pp. 41-55.
7. M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Communications, vol. 17, no. 1, pp. 51-58, February 2018.
8. C. Gentry and A. Silverberg, "Hierarchical ID-Based Cryptography," Advances in Cryptology—EUROCRYPT 2022, Springer Berlin Heidelberg, 2022, pp. 548-566.