EFFICIENT AGGREGATABLE DKG BASED DISTRIBUTED ATTRIBUTE AUTHORITY FOR CPABE IN PATIENT CENTRIC DATA

Ronanki Chandra Sekhar[1]*, Ravinder Reddy B[2]

Abstract:

In today's digital world, the healthcare sector is undergoing a rapid transformation, and healthcare data is growing at an exponential rate. Attribute-based encryption (ABE) has become a potential approach for securing patients' sensitive data and privacy. Although there are many parties engaged in the process, managing access control regulations in healthcare environments is difficult. To address this challenge, a distributed attribute authority (DAA) has been used to manage access control policies but the main disadvantage of the DABE scheme is the overhead involved in managing the distributed authorities. For ciphertext-policy attribute-based encryption (CPABE) with patient-centric data, an effective aggregatable distributed key generation (DKG) based DAA is proposed in this work. With the help of our suggested approach, DKG-based CPABE schemes' computational and communication overhead should be reduced. This technique allows multiple data owners to collaboratively generate a single access policy, thereby reducing the number of policies that need to be managed. The proposed system also supports revocation of users and attributes, which is an essential feature in healthcare settings. The proposed system stimulates the performance and show that, in terms of computing and communication costs, it performs better than the DKG-based CPABE systems that are already in use.

Keywords: Distributed Attribute Authority, Ciphertext policy Attribute-based Encryption, Distributed key generation, Patient-centric data.

[1]*M.Tech Student, Department of CSE, Anurag University, Venkatapur, Ghatkesar, Medchal District, Hyderabad 500088, Email: ronanki.cs@gmail.com

[2]Assistant Professor, Department of CSE, Anurag University, Venkatapur, Ghatkesar, Medchal District
Hyderabad 500088, Email: ravinderreddycse@anurag.edu.in

Corresponding Author: - Ronanki Chandra Sekhar

*M.Tech Student, Department of CSE, Anurag University, Venkatapur, Ghatkesar, Medchal District, Hyderabad 500088, Email: ronanki.cs@gmail.com

DOI: 10.48047/ecb/2023.12.10.420

1. Introduction

As healthcare systems have become more and more digital, electronic health records (EHRs) as well as other health information technology (HITs) have multiplied in recent years. These technologies have enabled the collection, storage, and sharing of large amounts of patient-centric data, which plays a crucial role in providing high-quality healthcare services. However, the sensitive nature of patient data requires secure storage and sharing mechanisms that enforce access control. For the secure sharing and storage of patient-centric data in the healthcare system, Attribute-based encryption (ABE) is a viable method. ABE provides granular access control by encrypting data and only users with right attributes can access the data.

Two popular access control techniques are role-based access control (RBAC) and discretionary access control (DAC) enables more flexible access control regulations. However, traditional CPABE schemes [1] rely on centralized attribute permissions, which can be a point of failure and access policy is public which leads to security and privacy issue. If attribute permissions are compromised, an attacker can access all encrypted data. In addition, the appointing authority may have access to sensitive patient data, which may compromise patient privacy.

To address these issues Müller, Sascha, Stefan Katzenbeisser [6] proposed a distributed attribute-based encryption (DABE) scheme. However, most DABE schemes require complex key generation protocols, resulting in high computation and communication overheads.

In this paper the proposed work is an efficient aggregatable distributed key generation (DKG) based distributed attribute authority (DAA) for ciphertext-policy ABE (CPABE) in patient-centric data. Our scheme eliminates the need for a centralized attribute authority, ensuring better privacy and security. The suggested technique makes use of an effective Aggregatable DKG protocol that lowers the system's computation and communication overheads, making it appropriate for usage in real-world applications. This protocol also increases the system's efficiency by minimizing the size of the decryption keys.

2. Related works

For safe data storage and sharing in healthcare systems, Numerous ABE-based plans have been proposed. Sahai and Waters[1] first developed the most advanced approach to encrypted access control is attribute-based encryption (ABE). In comparison to traditional public key cryptography, attribute-based encryption has no requirement that ciphertext be encrypted for a specific user. Instead, a set of characteristics or an attribute policy will be linked to each user's private key and ciphertext. The user is able to decode the information if their secret key and the encrypted text “match”. Sahai and Waters [2] created a threshold ABE system in their initial system where the private key of the user is attached to both threshold and ABE whereby ciphertexts are marked with a set of features S. However, the majority of these strategies rely on one primary attribute authority, which can be a privacy risk and a single point of failure.

Distributed attribute-based encryption (DABE) schemes [6] have been proposed to eliminate the need for a centralized attribute authority. For instance, the work of [4] proposed a DABE scheme that used secret sharing to distribute the key generation process among multiple servers and it uses a threshold cryptography to distribute the key generation process among multiple servers. However, the majority of these systems call for intricate key generation procedures, which raises the overheads of computation and communication.

In address these issues Zhang, Liang, Feiyang Qiu, Feng Hao, and Haibin Kan [11] have been proposed a DKG-based CPABE scheme and also to get around these restrictions Liu et al. developed a CPABE system based on DKG that allows ciphertext encryption and effective key generation. However, the considerable communication overhead during key distribution makes their technique ineffective.

Similarly, Wei et al. suggested a tree-based DKG method for CPABE to reduce the communication overhead. The amount of communication necessary for key creation and distribution is decreased by their plan.

To get around the drawbacks of conventional DABE schemes, DKG-based DABE schemes have been proposed that uses Pedersen commitment scheme to achieve better efficiency. Most of the DKG concepts are built on the fundamentals of Shamir Secret Sharing (SSS) scheme to achieve better efficiency.

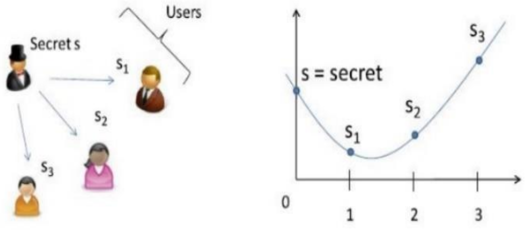


Fig. 1 DAA using Shamir Secret Sharing Scheme

As shown in Fig 1 a graph of secret keys at y-intercepts with S_1, S_2 and S_3 where as to construct a graph A, B are sufficient there isn't required of C. This is a problem of Secret sharing (SS) to overcome this Verifiable Secret Sharing Schemes are proposed using this model of distributed sharing allows S_1 and S_2 to be assured that S_3 has a share whereas S_1, S_2 and S_3 are independently verified by the recipient's although the problem still exists by the one who knows the initial secret S in Fig 1. when you drew a graph (y-intercepts) then you were aware of the secret Fig 2.

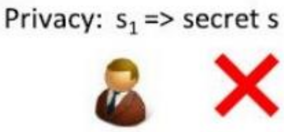


Fig. 2 DKG Drawback

To overcome this issue an Aggregatable DKG is proposed by having every single person is involved in secret sharing and summing up the shares of these secret sharing.

Fig. 3 Summing up Secret shares

3. Cryptographic Preliminaries

3.1 CPABE

Access structure:

Consider a set of components as A_1, A_2, ..., A_n. If B and C are true and B ∈A and B ∈C, then the collection M⊆2 A_1, A_2, ..., A_n is monotonic. An access structure, also known as a corresponding monotonic access structure, is a set (sometimes known as a monotonous set), M, made up of non-empty subsets of A_1, A_2, ..., A_n, or M⊆2 A_1, A_2, ….., A_n. The sets in S are referred as approved sets, whilst the sets outside of S are referred to as prohibited sets.

Setup. The default security parameters are the only input the configuration algorithm requires. It offers MK and PK respectively.

Key Generation (MK, S). The master key and a set of attributes S that describe the key are inputs into the key generation algorithm, which outputs the secret key SK.

Encryption (PK, M, A). The message M can only be decoded once it has been encrypted into a ciphertext CT by the user who holds a number of attributes that complies with the framework of access. The message M, the public parameters PK, and the access structure A on the set of attributes are all inputs to the encryption algorithm.

Decryption (PK, CT, SK). The input for the decryption technique consists of the publicly visible parameters PK, an access policy A-containing ciphertext CT, and a secret key SK that acts as a secret key for a set of S features. The algorithm decrypts the ciphertext and returns the message M when the access format A is met by the collection of S attributes.

3.2 DKG

A distributed key generation (DKG) technique is used to generate cryptographic keys among a group of participants without disclosing individual private keys of the participants. For secure communication among the participants these keys generated using DKG can be utilized.

f(x) = ∑ (i=1 to k) y_i * ∏ (j=1 to k, j≠i) (x - x_j) / (x_i - x_j)

where: f(x) is the polynomial being interpolated. yi is the secret value of participant i. xi is the unique point on the polynomial generated by participant i.

3.3 ADKG

Aggregatable distributed key generation (ADKG) is an extension of distributed key generation (DKG) that enables the efficient aggregation of the private keys generated by multiple groups of participants. This allows for the creation of a single shared key that can be used for secure communication among all groups. The formula used in ADKG is similar to that used in DKG, with the addition of an aggregation step. Each group of participants generates their own polynomial and secret values using the same formula as in DKG.

Once each group has generated their private keys, they can be aggregated using a homomorphic encryption scheme, such as Paillier encryption. The encrypted private keys are then sent to a trusted aggregator who can compute the aggregate key without ever seeing the individual private keys.

Key Generation in ADKGs: The total of the Master Secret keys, along with a set of attributes S that describe the key, are the method's inputs for the key creation phase. The algorithm's result is the Secret key SK.

The formula used for aggregatable distributed key generation is:

f(x) = ∑ (i=1 to m) (∑ (j=1 to k) $y_{i,j}$)* ∏(l=1 to m, l≠i) (x - xi) / (xi - xl)

where f(x) is the interpolating aggregated polynomial, m is for number of groupings. k is for number of individuals in each group and the participant's secret value in the group is $y_{i,j}$. x_i is the sole point on the polynomial that group i created.

In this formula, each group generates its own polynomial and secret values as in DKG. The encrypted private keys are then aggregated using homomorphic encryption, and the trusted aggregator can compute the aggregate key using the shared polynomial coefficients and the encrypted private keys.

The resulting aggregate key can be used for secure communication among all groups. This approach offers significant advantages over traditional DKG, as it allows for the efficient aggregation of private keys from multiple groups, without revealing any individual private keys to the aggregator.

4. Proposed System

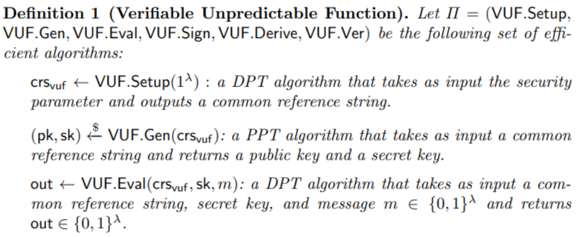
This work proposes an efficient aggregatable DKG-based distributed attribute authority for CPABE in patient centric data. Our scheme eliminates the need for a centralized key generation by attribute authority's, ensuring better privacy and security. The proposed scheme uses an efficient DKG protocol that reduces the computation and communication overheads of the system, making it practical for real-world applications. We provide information on a distributed key generation protocol (DKG) for creating a key pair (pk, sk) with the following structure.

$$\mathsf{pk} = (g_1^a, \hat{u}_1^a) \in \mathbb{G}_1 \times \mathbb{G}_2 \quad \text{and} \quad \mathsf{sk} = \hat{h}_1^a \in \mathbb{G}_2, \text{ where } a \in \mathbb{F}$$

Verification keys vk_i are added to all parties P_i. Our work is broadly analogous to the DKG verifiable secret sharing system, where each M_i party uses PVSS to distribute the secret $h\hat{}c_i^1$ to every other party. For each party's contribution the respected weights we_i of must be recorded for every aggregated PVSS.

$((we_1, ..., we_n), (C_1, ..., C_n), PVSS)$.

The proposed scheme of Aggregating DKG, which enhances the efficiency of the system by reducing the size of the decryption keys. The suggested system is intended to deliver patient-centric data with fine-grained access control, guaranteeing that only authorized individuals can access the data.



Definition 1 (Verifiable Unpredictable Function). *Let* $\Pi = (\mathsf{VUF.Setup}, \mathsf{VUF.Gen}, \mathsf{VUF.Eval}, \mathsf{VUF.Sign}, \mathsf{VUF.Derive}, \mathsf{VUF.Ver})$ *be the following set of efficient algorithms:*

$\mathsf{crs_{vuf}} \leftarrow \mathsf{VUF.Setup}(1^\lambda)$: *a DPT algorithm that takes as input the security parameter and outputs a common reference string.*

$(\mathsf{pk}, \mathsf{sk}) \overset{\$}{\leftarrow} \mathsf{VUF.Gen}(\mathsf{crs_{vuf}})$*: a PPT algorithm that takes as input a common reference string and returns a public key and a secret key.*

$\mathsf{out} \leftarrow \mathsf{VUF.Eval}(\mathsf{crs_{vuf}}, \mathsf{sk}, m)$*: a DPT algorithm that takes as input a common reference string, secret key, and message* $m \in \{0,1\}^\lambda$ *and returns* $\mathsf{out} \in \{0,1\}^\lambda$.

Fig. 4 ADKG Access Structure

The proposed ADKG access structure for sensitive access of CT using DKG scheme similar to that proposed by Wei et al. However, we introduce several modifications to their scheme to reduce the computation and communication overhead and aggregation of access policies.

Our proposed scheme includes four phases:

1. ***Setup (γ, S) → (PK, MK)***

   The KGC produces PK and MK, which are determined by γ and S, respectively.

2. ***Key Generation***

   This phase has involved three rounds

   2.1 DKG

   At first DAA's will generate keys $PVSS_i$ with the combination of (PK, SA, MK) → $PVSSS_i$.

   KGC generates SK_n with the help of M, PK, Mk and S.

   2.2 Aggregating DKG:

   Then we aggregate the $PVSS_i$ into PVSS.

   $(we_{i,1}, ..., we_{i,n}), (C_{i,1}, ..., C_{i,n}), PVSS_i, b\in \{1, 2\}$

   Then a single DKG is formed by aggregating all of them.

   $(we_1, ..., we_n), (C_1, ..., C_n)$, PVSS

   ***2.3 Construction of secret key*:**

   The last key pair, as stated at the beginning of this section, will be

   $$\mathsf{pk} = (g_1^{f(0)}, \hat{u}_2) = (g_1^{f(0)}, \hat{u}_1^{f(0)}) \text{ and } \mathsf{sk} = \hat{h}_1^{f(0)}$$

   The sk construction functions as described since the final DKG is simply an improved PVSS.

3. ***Encryption (PK, SA, M) → CT***

The PK, Attributes, and M are inputs to the encryption process, which outputs CT, where CT is a Cypher Text.

4. ***Decryption (CT, SK) → M***
When CT and SK inputs are received, then the receiver decrypts as a result it provides a message, CT and M as output, respectively.

The IBM Clinical Hub provides clinical data components that, when connected to patient identity data, enable vertical storage, production, and access to patient records, taken into consideration the ADKG for PCD was developed for testing. A more thorough workflow template is provided by the IBM Clinical Hub, which also provides access to consumer procedures and systems as well as patient demographics and clinical data components. A series of HL7 incidents and information pertaining to patient related information like test reports, visiting info, admission, transfer and discharge incidents form the longitudinal patient record. a variety of acute and emergency settings around the hospital. The longitudinal patient record includes information on medications, immune sensitive, test reports, challenges, procedures, and ancestry, to name a few things. Table 1 offers a list of sensitive properties.

S No	Attributes	Transactional IDs
1.	Name Of Patient	NP
2.	Date Of Birth	DOB
3.	Gender	G
4.	Home Address HA	HA
5.	Billing Address BA	BA
6.	Email	EM
7.	Mobile Phone	MP
8.	Primary Physician	PP
9.	E-Patient ID	PID
10.	Medical Record Number	MRN
11.	Patient Blood Group	PBG
12	Insurance Number	IN
13.	Allergies	AL
14.	Immunizations	IM
15.	Vitals	V
16.	Family History	FH
17.	Visit info	VI
18.	Diagnosis	DI
19.	Patient Drugs	PD
20.	Patient Study	PS
21.	Patient Risk Factors	PRF
22.	Patient Symptoms	PSY
23.	Patient Treatment	PT
24.	Patient Outcomes	PO
25.	Organizational Info	OI
26.	Physician Info	PI

Table 1: Patient Health Record attributes of IBM Clinical Hub

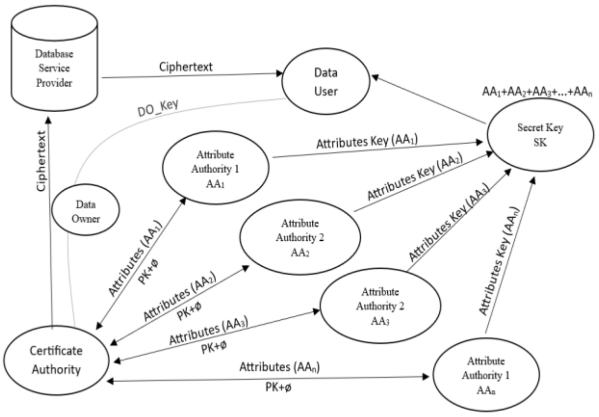


Fig. 5 Aggregatable DKG based Distributed Attribute Authority for CPABE in Patient Health Data

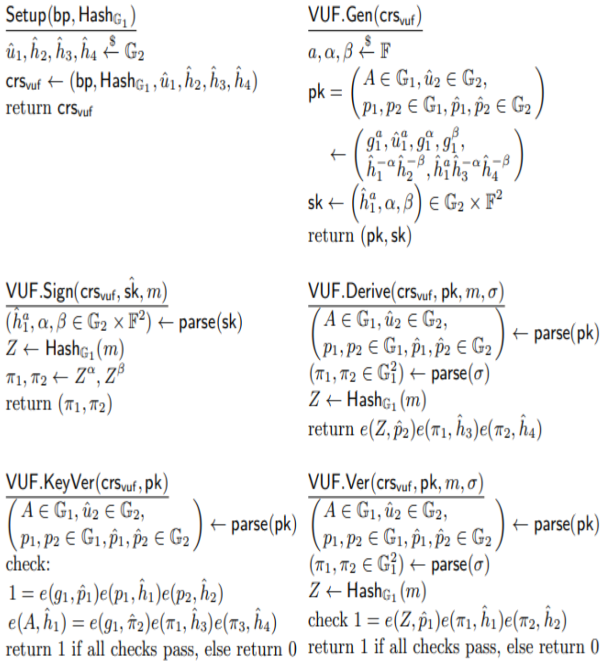
5. Security Analysis

ABE systems currently in use lack adequate security. Decisional Bilinear Diffie-Hellman (DBDH) premise is typically used to construct these systems.

BDH assumption: Assume that A is an attacker with time k in polynomial, the measure of security. A tuple (t,t_a,t_b,t_c) is given where a, b, and c are Z-p. The BDH problem's solution is something that attacker A tries to calculate. When solving the BDH issue, A has an advantage that we characterize as

$$Adv_A^{BDH}(k)=Pr[A(t,t_a,t_b,t_c)=e(t,t)^{abc}]$$

However, as soon as the DBDH assumption is compromised, all affected ABEs are exposed to danger. to solve this issue. We now provide evidence that the BDH assumption forms the foundation of our suggested strategy. Under the random oracle model's SXDH and BDH assumptions, the procedure in Fig. 6 is a secure VUF.



```
$\underline{\mathsf{Setup}(\mathsf{bp}, \mathsf{Hash}_{\mathbb{G}_1})}$
$\hat{u}_1, \hat{h}_2, \hat{h}_3, \hat{h}_4 \xleftarrow{\$} \mathbb{G}_2$
$\mathsf{crs}_{\mathsf{vuf}} \leftarrow (\mathsf{bp}, \mathsf{Hash}_{\mathbb{G}_1}, \hat{u}_1, \hat{h}_2, \hat{h}_3, \hat{h}_4)$
return $\mathsf{crs}_{\mathsf{vuf}}$

$\underline{\mathsf{VUF.Gen}(\mathsf{crs}_{\mathsf{vuf}})}$
$a, \alpha, \beta \xleftarrow{\$} \mathbb{F}$
$\mathsf{pk} = \begin{pmatrix} A \in \mathbb{G}_1, \hat{u}_2 \in \mathbb{G}_2, \\ p_1, p_2 \in \mathbb{G}_1, \hat{p}_1, \hat{p}_2 \in \mathbb{G}_2 \end{pmatrix}$
    $\leftarrow \begin{pmatrix} g_1^a, \hat{u}_1^a, g_1^\alpha, g_1^\beta, \\ \hat{h}_1^{-\alpha}\hat{h}_2^{-\beta}, \hat{h}_1^a\hat{h}_3^{-\alpha}\hat{h}_4^{-\beta} \end{pmatrix}$
$\mathsf{sk} \leftarrow \left(\hat{h}_1^a, \alpha, \beta\right) \in \mathbb{G}_2 \times \mathbb{F}^2$
return $(\mathsf{pk}, \mathsf{sk})$

$\underline{\mathsf{VUF.Sign}(\mathsf{crs}_{\mathsf{vuf}}, \hat{\mathsf{sk}}, m)}$
$(\hat{h}_1^a, \alpha, \beta \in \mathbb{G}_2 \times \mathbb{F}^2) \leftarrow \mathsf{parse}(\mathsf{sk})$
$Z \leftarrow \mathsf{Hash}_{\mathbb{G}_1}(m)$
$\pi_1, \pi_2 \leftarrow Z^\alpha, Z^\beta$
return $(\pi_1, \pi_2)$

$\underline{\mathsf{VUF.Derive}(\mathsf{crs}_{\mathsf{vuf}}, \mathsf{pk}, m, \sigma)}$
$\begin{pmatrix} A \in \mathbb{G}_1, \hat{u}_2 \in \mathbb{G}_2, \\ p_1, p_2 \in \mathbb{G}_1, \hat{p}_1, \hat{p}_2 \in \mathbb{G}_2 \end{pmatrix} \leftarrow \mathsf{parse}(\mathsf{pk})$
$(\pi_1, \pi_2 \in \mathbb{G}_1^2) \leftarrow \mathsf{parse}(\sigma)$
$Z \leftarrow \mathsf{Hash}_{\mathbb{G}_1}(m)$
return $e(Z, \hat{p}_2)e(\pi_1, \hat{h}_3)e(\pi_2, \hat{h}_4)$

$\underline{\mathsf{VUF.KeyVer}(\mathsf{crs}_{\mathsf{vuf}}, \mathsf{pk})}$
$\begin{pmatrix} A \in \mathbb{G}_1, \hat{u}_2 \in \mathbb{G}_2, \\ p_1, p_2 \in \mathbb{G}_1, \hat{p}_1, \hat{p}_2 \in \mathbb{G}_2 \end{pmatrix} \leftarrow \mathsf{parse}(\mathsf{pk})$
check:
$1 = e(g_1, \hat{p}_1)e(p_1, \hat{h}_1)e(p_2, \hat{h}_2)$
$e(A, \hat{h}_1) = e(g_1, \hat{\pi}_2)e(\pi_1, \hat{h}_3)e(\pi_3, \hat{h}_4)$
return 1 if all checks pass, else return 0

$\underline{\mathsf{VUF.Ver}(\mathsf{crs}_{\mathsf{vuf}}, \mathsf{pk}, m, \sigma)}$
$\begin{pmatrix} A \in \mathbb{G}_1, \hat{u}_2 \in \mathbb{G}_2, \\ p_1, p_2 \in \mathbb{G}_1, \hat{p}_1, \hat{p}_2 \in \mathbb{G}_2 \end{pmatrix} \leftarrow \mathsf{parse}(\mathsf{pk})$
$(\pi_1, \pi_2 \in \mathbb{G}_1^2) \leftarrow \mathsf{parse}(\sigma)$
$Z \leftarrow \mathsf{Hash}_{\mathbb{G}_1}(m)$
check $1 = e(Z, \hat{p}_1)e(\pi_1, \hat{h}_1)e(\pi_2, \hat{h}_2)$
return 1 if all checks pass, else return 0
```

Fig.6 Optimized verifiable unpredictable function

DKG satisfies the need for key express ability. To do this, we build a simulator that can set the output to be the value $pk_1 + pk_2 + ... + pk_n$, where pk_1 is provided as the input and =!0. This signature scheme of aggregation would be susceptible to rogue key attacks, just like the BLS system.

Rogue Public Key Attack: The Rogue Key Attack is then rather straightforward [13,14]. Eve generates a public key with the formula: $pk_2 = (-pk_1)$ and is then able to generate a combined public key that equals zero (or the point at infinity). Consequently, the signature check will be:

$$e(G_2,\sigma) ==e([0].G_2,H(m)) \text{ and will equal:}$$

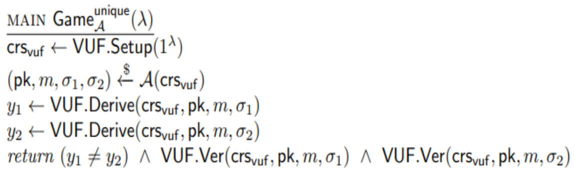
$$e(G_2,[0].\sigma) ==e(G_2,H(m)).$$

Therefore, it is crucial to offer simulation-extractable evidence of secret key knowledge as a component of a public key infrastructure. This does not explicitly show that the DKG upholds security instead, we must demonstrate that it satisfies the requirements for uniqueness and unpredictability.

Definition 1 (Uniqueness). The ADKG meets uniqueness within the random oracle model according to the SXDH assumption.

Let Adv_A^{unique} () = Pr [$Game_A^{unique}$ ()] for a VUF and an opponent A.

where $Game_{A()}^{unique}$ has the following definition:

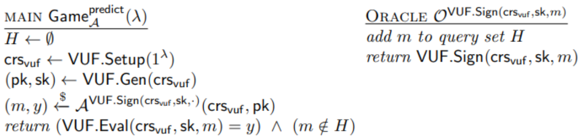


```
$\underline{\textsc{main}\ \mathsf{Game}_{\mathcal{A}}^{\mathsf{unique}}(\lambda)}$
$\mathsf{crs}_{\mathsf{vuf}} \leftarrow \mathsf{VUF.Setup}(1^\lambda)$
$(\mathsf{pk}, m, \sigma_1, \sigma_2) \xleftarrow{\$} \mathcal{A}(\mathsf{crs}_{\mathsf{vuf}})$
$y_1 \leftarrow \mathsf{VUF.Derive}(\mathsf{crs}_{\mathsf{vuf}}, \mathsf{pk}, m, \sigma_1)$
$y_2 \leftarrow \mathsf{VUF.Derive}(\mathsf{crs}_{\mathsf{vuf}}, \mathsf{pk}, m, \sigma_2)$
$\mathit{return}\ (y_1 \neq y_2)\ \wedge\ \mathsf{VUF.Ver}(\mathsf{crs}_{\mathsf{vuf}}, \mathsf{pk}, m, \sigma_1)\ \wedge\ \mathsf{VUF.Ver}(\mathsf{crs}_{\mathsf{vuf}}, \mathsf{pk}, m, \sigma_2)$
```

If we have that $Adv_{A()negl()}^{unique}$, A is a common adversary in PPT, thus we declare that to be special. If the output of the function VUF cannot be predicted by the adversary, so that VUF is said to be unpredictable. Evaluating a message for which no authentic signatures have been detected.

Definition 2 (Unpredictability).

In the random oracle paradigm, the ADKG satisfies unpredictability under the SXDH and BDH assumptions.



```
$\underline{\textsc{main}\ \mathsf{Game}_{\mathcal{A}}^{\mathsf{predict}}(\lambda)}$
$H \leftarrow \emptyset$
$\mathsf{crs}_{\mathsf{vuf}} \leftarrow \mathsf{VUF.Setup}(1^\lambda)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{VUF.Gen}(\mathsf{crs}_{\mathsf{vuf}})$
$(m, y) \xleftarrow{\$} \mathcal{A}^{\mathsf{VUF.Sign}(\mathsf{crs}_{\mathsf{vuf}}, \mathsf{sk}, \cdot)}(\mathsf{crs}_{\mathsf{vuf}}, \mathsf{pk})$
$\mathit{return}\ (\mathsf{VUF.Eval}(\mathsf{crs}_{\mathsf{vuf}}, \mathsf{sk}, m) = y)\ \wedge\ (m \notin H)$

$\underline{\textsc{Oracle}\ \mathcal{O}^{\mathsf{VUF.Sign}(\mathsf{crs}_{\mathsf{vuf}}, \mathsf{sk}, m)}}$
$\mathit{add\ m\ to\ query\ set\ H}$
$\mathit{return}\ \mathsf{VUF.Sign}(\mathsf{crs}_{\mathsf{vuf}}, \mathsf{sk}, m)$
```

By knowing the $Adv_{predict}$ A()negl() of all PPT adversaries A, then it can be argued as unpredictable.

6. Results

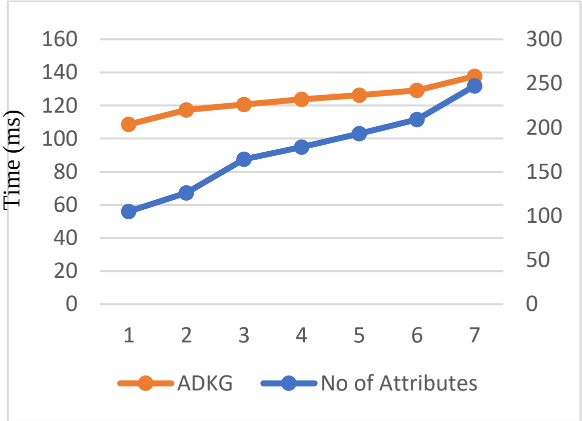


Fig.6 No of Attributes and Encryption Time

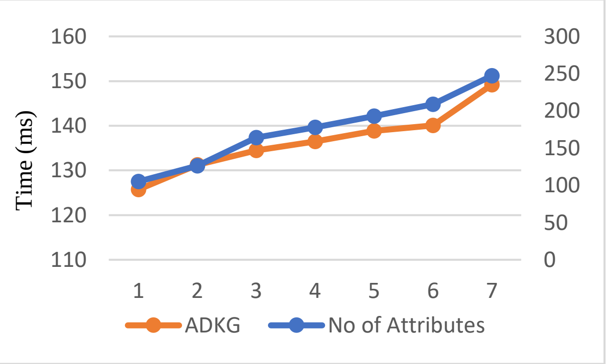


Fig.6.1 Time taken for Generating Keys

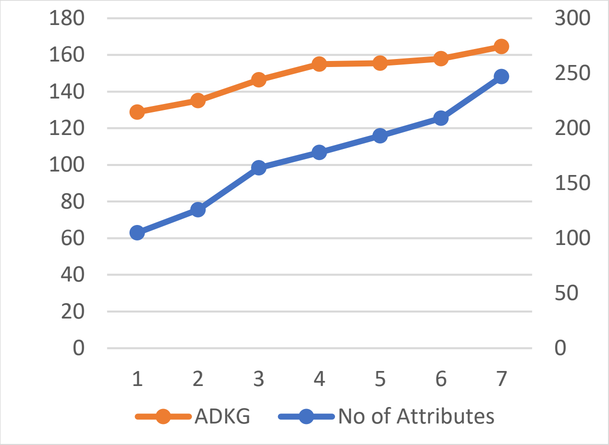


Fig.6.2 Time taken for Decrypting No of attributes

Overall, without sacrificing on privacy and security, the proposed ADKG model offers an effective and secure solution for patient-centric data sharing across healthcare. Future research can explore the integration of the proposed scheme with other healthcare systems, such as electronic health records and telemedicine systems, to provide better healthcare services to patients.

7. Appendix A: Symbols Table

S No	Symbol	Description
1.	S	Set of Attributes
2.	PK	Public Key
3.	MK	Master Key
4.	CT	Cipher Text
5.	KGC	Key Generation Centre
6.	SK	Secret Key
7.	γ	Security Variables
8.	M	Input Message
9.	HL7	Health Level 7
10.	ABE	Attribute Based Encryption
11.	PCD	Patient-Centric Data
12.	DAA	Distributed Attribute Authority
13.	DKG	Distributed Key Generation
14.	ADKG	Aggregatable Distributed Key Generation
15	SSS	Shamir's Secret Sharing
16	PVSSS	Publicly Verifiable Shamir's Secret Sharing
17	SXDH	Symmetric External Diffie Hellman
18	BDH	Bilinear Diffie Hellman

Table 2. Symbols Table

8. Conclusion

In this study, a distributed attribute authority for CPABE in patient-centric data using an effective aggregatable DKG-based model is proposed. The proposed scheme eliminates the need for a centralized attribute authority, ensuring better privacy and security. The method employs a realistic Aggregatable DKG protocol that lowers the efficiency of the system by minimizing the quantity of decryption keys, making it appropriate for usage in practical applications.

9. Reference

[1] Bethencourt, John, Amit Sahai, and Brent Waters. "Ciphertext-policy attribute-based encryption." In *2007 IEEE symposium on security and privacy (SP'07)*, pp. 321-334. IEEE, 2007.

[2] Sahai, Amit, and Brent Waters. "Fuzzy identity-based encryption." In *Advances in Cryptology–EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005. Proceedings 24*, pp. 457-473. Springer Berlin Heidelberg, 2005.

[3] Lewko, Allison, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption." In *Advances in Cryptology–EUROCRYPT 2010*: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings *29*, pp. 62-91. Springer Berlin Heidelberg, 2010.

[4] Müller, Sascha, Stefan Katzenbeisser, and Claudia Eckert. "Distributed attribute-based encryption." In *Information Security and Cryptology–ICISC 2008: 11th International Conference, Seoul, Korea, December 3-5, 2008, Revised Selected Papers 11*, pp. 20-36. Springer Berlin Heidelberg, 2009.

[5] Lewko, Allison, and Brent Waters. "New techniques for dual system encryption and fully secure HIBE with short ciphertexts." In *Theory of Cryptography: 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010. Proceedings 7*, pp. 455-479. Springer Berlin Heidelberg, 2010.

[6] Lewko, Allison, Amit Sahai, and Brent Waters. "Revocation systems with very small private keys." In *2010 IEEE Symposium on Security and Privacy*, pp. 273-285. IEEE, 2010.

[7] Lai, Junzuo, Robert H. Deng, and Yingjiu Li. "Fully secure cipertext-policy hiding CPABE." In *Information Security Practice and Experience: 7th International Conference, ISPEC 2011, Guangzhou, China, May 30– June 1, 2011.*

Proceedings 7, pp. 24-39. Springer Berlin Heidelberg, 2011.

[8] Li, Qi, Jianfeng Ma, Rui Li, Ximeng Liu, Jinbo Xiong, and Danwei Chen. "Secure, efficient and revocable multi-authority access control system in cloud storage." *Computers & Security* 59 (2016): 45-59.

[9] Liu, Xin, Man Guo, Bin Zhang, and Xuzhou Li. "A lightweight attribute-based authentication system with DAA." In *Journal of Physics: Conference Series*, vol. 1601, no. 3, p. 032025. IOP Publishing, 2020.

[10] Zhang, Leyou, Gongcheng Hu, Yi Mu, and Fatemeh Rezaeibagha. "Hidden ciphertext policy attribute-based encryption with fast decryption for personal health record system." *IEEE Access* 7 (2019): 33202-33213.

[11] Shi, Jian, Xinwen Wang, Jenny-Hoa Nguyen, Barry E. Bleske, Yan Liang, Li Liu, and HaoJie Zhu. "Dabigatran etexilate activation is affected by the CES1 genetic Polymorphism G143E (rs71647871) and gender. *"Biochemical pharmacology* 119 (2016): 76-84.

[12] Zhang, Liang, Feiyang Qiu, Feng Hao, and Haibin Kan. "1-round distributed key generation with efficient reconstruction using decentralized cp-abe." *IEEE Transactions on Information Forensics and Security* 17 (2022): 894-907.

[13] Boneh, Dan, Manu Drijvers, and Gregory Neven. "BLS multi-signatures with public-key aggregation." *URL: https://crypto. stanford. edu/~dabo/pubs/papers/BLSmultisig.html* (2018).

[14] Boneh, Dan, Sergey Gorbunov, Hoeteck Wee, and Zhenfei Zhang. *Bls signature scheme*. Technical Report draft-boneh-bls-signature-00, Internet Engineering Task Force, 2019.

[15] Kokoris Kogias, Eleftherios, Dahlia Malkhi, and Alexander Spiegelman. "Asynchronous Distributed Key Generation for ComputationallySecure Randomness, Consensus, and Threshold Signatures." In Proceedings of the 2020 *ACM SIGSAC Conference on Computer and Communications Security*, pp. 1751-1767. 2020.

[16] Gurkan, Kobi, Philipp Jovanovic, Mary Maller,Sarah Meiklejohn, Gilad Stern, and Alin Tomescu. "Aggregatable distributed key generation. *"In Advances in Cryptology–EUROCRYPT 2021:40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia*, October 17–21, 2021, Proceedings, Part I, pp. 147-176. Cham: Springer International Publishing, 2021.

[17] Li, Qi, Hongbo Zhu, Jinbo Xiong, Ruo Mo, Zuobin Ying, and Huaqun Wang. "Fine-grained multi-authority access control in IoT-enabled mHealth." *Annals of Telecommunications* 74 (2019): 389-400.

[18] Chaudhary, Chandan Kumar, Richa Sarma, and Ferdous Ahmed Barbhuiya. "RMA-CPABE: A multi-authority CPABE scheme with reduced ciphertext size for IoT devices." *Future Generation Computer Systems* 138 (2023): 226-242.

[19] Zhang, Moli, Feijiao Shao, Ruijuan Zheng, Muhua Liu, and Zhihang Ji. "An Efficient Encryption Scheme with Fully Hidden Access Policy for Medical Data." *Electronics* 12, no. 13 (2023): 2930.

[20] Adjih, Cédric, Daniele Raffo, and Paul Muhlethaler. "Attacks against OLSR: Distributed key management for security." In *2nd OLSR Interop/Workshop, Palaiseau, France*, vol. 14, pp. 1-5. 2005.

[21] Lemnouar, Noui. "Security limitations of Shamir's secret sharing." *Journal of Discrete Mathematical Sciences and Cryptography* (2022): 1-13.

[22] Andreou, Athanasios, Oana Goga, and Patrick Loiseau. "Identity vs. attribute disclosure risks for users with multiple social profiles." In *Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017*, pp. 163-170. 2017.

[23] Li, Jiguo, Shengzhou Hu, and Yichen Zhang. "Two-party attribute-based key agreement protocol with constant-size ciphertext and key." *Security and Communication Networks* 2018 (2018).