Secure Medical Data Sharing and Storage with Identity-Based Encryption

Souhardya Halder
Computer Science and Engineering
Indian Institute of Technology
Guwahati, India
souhardya@iitg.ac.in

***Abstract*—In today's digital age, the management and privacy of medical data are paramount concerns. Healthcare record systems require a delicate balance between easy access for authorized users and stringent protection against unauthorized access. This project presents an innovative approach to addressing this challenge by leveraging the power of Identity-Based Encryption (IBE) to create a secure and user-centric medical data storage and sharing solution.The proposed application revolves around the idea of a Personal Health Record system that empowers individuals to manage their healthcare-related information securely and effortlessly. Unlike traditional systems that rely on complex key management and distribution mechanisms, the implemented solution harnesses the inherent simplicity of IBE. Private Key Generator (PKG) technology is utilized to generate private keys based on user identities, eliminating the need for users to manage their own keys.**

***Index Terms*—Identity-Based Encryption (IBE), Private Key Generator (PKG)**

I. Introduction

The core functionalities of the application include secure medical data storage, data sharing with authorized parties, and communication between users and healthcare professionals. By integrating IBE, the system enables users to securely store their medical records, share specific records with trusted entities, and maintain the confidentiality of their communications. Furthermore, the project explores the dynamic nature of IBE, allowing users to grant and revoke access to their medical data on-demand. This facilitates a fine-grained access control mechanism that ensures only authorized parties can access specific data categories, enhancing privacy and security. Identity-Based Encryption is a modern cryptographic paradigm that offers a solution to some of the shortcomings of traditional PKI. IBE enables the generation of cryptographic keys based on easily recognizable user attributes, such as email addresses, usernames, or other personal information. This eliminates the need for complex key distribution mechanisms, making it a suitable candidate for secure communication in various applications.

II. Related Work

A. *Efficient Key Revocation*

The research of Alexandra Boldyreva, Vipul Goyal, and Virendra Kumar [1], which introduced an Identity-Based Encryption (IBE) scheme with efficient revocation processes. Their work significantly reduces the complexity of key updates, transitioning from a linear to logarithmic scale with respect to the number of users. Their contributions encompass various security levels, enhancing the field of cryptographic research. Their insights on constructing attribute-based encryption schemes with efficient revocation mechanisms have broader implications, particularly in scenarios with a large user base where scalability is paramount.[1]

B. *Improved User Privacy*

In the context of preserving patient privacy, research work by Carlisle Adams [2] endeavours to minimize the trust required in the Private Key Generator (PKG) for deploying identity-based encryption (IBE). By leveraging digital credentials and bilinear maps, our fundamental framework introduces a separation between the PKG and an intermediate Certification Authority (ICA). This separation not only replicates the functionalities but also aligns with the privacy standards outlined in previous studies [1,3]. Additionally, our advanced framework extends this separation to encompass multiple ICAs. This innovation empowers individuals like Alice to significantly diminish the likelihood of any entity compromising her anonymity or gaining access to her IBE private key, reducing it to an infinitesimal probability.

C. *Patients' Mata management System Through Identity Based Encryption*

In the healthcare sector, patient identification and the secure management of medical records represent significant challenges. This research addresses these critical issues.The Reseacrh work of [3] established mutual authentication between the server and healthcare workers through a challenge-response protocol that relies on an Identity-Based Encryption (IBE) cryptosystem. Moreover, to ensure the confidentiality of data, we implement the FullIdent scheme developed by Boneh and Franklin. Additionally, patient identification is facilitated using NFC wristbands, which employ a HMAC scheme for added security.[3]

III. Proposal

In this project, we leverage cryptographic pairings, a fundamental tool in modern cryptography. Pairings enable us to connect elements from different algebraic groups and perform complex computations. This mathematical concept plays a pivotal role in our proposed Identity-Based Encryption (IBE) system.

This project focuses on adapting the renowned Boneh-Franklin IBE scheme to enhance secure medical data management [4]. We aim to ensure fine-grained access control, user-friendly key management, and secure communication in the context of healthcare data sharing and storage. This adaptation is central to our mission of providing a robust solution for safeguarding sensitive medical records.

A. An IBE Scheme

An IBE scheme is defined in terms of four algorithms Setup, Key Derivation, Encryption and Decryption:

- Setup: The "Setup" phase is the initial step in an Identity-Based Encryption system, responsible for configuring the foundational parameters and creating the necessary components to enable secure communication .During this phase
  A trusted entity, often referred to as the Private Key Generator (PKG), generates essential cryptographic parameters, including group structures and security parameters. These parameters lay the foundation for secure key derivation and encryption.
  The PKG creates the master secret key, a highly sensitive cryptographic key used to generate private keys for users. It is crucial to safeguard this key since it serves as the root of trust in the system.
- Key Extraction: This phase is the process of deriving a user's private key based on their identity. The user's identity, which could be an email address or any unique identifier, is mapped to an appropriate element within the established group structure. This mapping connects the identity with a specific element within the cryptographic system.Using the mapped identity and the master secret key, the user's private key is derived. This private key is unique to the user and is required for decryption.
- Encryption: A sender encrypts a message to ensure that only the intended recipient can access its contents.The sender identifies the recipient by their identity, which may be an email address or another identifier, to determine which user's public key to use for encryption.Using the recipient's public key and a chosen encryption algorithm, the sender encrypts the message to create a ciphertext. Only the corresponding private key, which the recipient can derive, can decrypt this ciphertext.
- Decryption:The Decryption phase is executed by the recipient to recover the original message from the ciphertext.The recipient, using their identity and the master secret key, derives their unique private key. This private key corresponds to the public key used for encryption.The recipient utilizes their private key to decrypt the ciphertext received from the sender. This operation results in the recovery of the original message.

B. Basic Properties

Let G, G_{T} are two groups which hold cyclic property with order q for a large prime number. Our IBE system makes use of a bilinear map e : G × G $\rightarrow G_{\mathrm{T}}$ between these two groups [8]. The map must satisfy the following properties:

- Bilinear: For all $Q, P \in$ G$_{\mathrm{q}}$ and for $x, y \in Z$ we have e(xQ , yP) = $e(Q, P)^{xy}$.

- Non degenerate: If P is a generator in G_{q} then e(P,P) is a generator in G_{T}, i.e, $e(P, P) \neq 1$

- Computable: For all P_1, $P_2 \in G_{\mathrm{q}}$ the value e(P_1, P_2) is easy to compute.

C. Equations

- Setup: In the Setup phase we choose
  1. (q, G , G_{T} ,g ,e)
  q is large prime number.
  G , G_{T} = Cyclic Group.
  g is a generator in G_{T}
  e is a bilinear pairing.

  2.We define parameters as
  param = (q, g, Q, H_1, H_2) , where
  Q = g^{α} , α is Master Secret Key of PKG.
  $H_1 : \{0,1\}^* \rightarrow G.$
  $H_2 : G_T \rightarrow \{0,1\}^l$, l is length of the plaintext.

- Extract: In the Extract phase User i, U_{i} sends ID_{i} to the PKG , which then furthur generates SK_{i} secret key of User i.

  SK_i = $(H_1(ID_i))^{\alpha}$

- Encryption: We have the param=(q, g, Q, H_1, H_2) and Message m= $\{0,1\}^l$, where l is length of the message.

  We generate ciphertext (C_1, C_2)
  Where C_1 = g^r , r is a random number from Z_p
  and C_2 =$m \bigoplus H_2(e(H_1(ID_i), Q)^r)$

  Note : $(H_1(ID_i)$ is an element in G and Q is an element in G and $e(H_1(ID_i), Q)^r$ is an element in G_T.

- Decryption: On the operation of
  $C_2 \bigoplus H_2(e(SK_i, C_1))$ the plaintext message will be generated.
  m=$C_2 \bigoplus H_2(e(SK_i, C_1))$

- Correctness: We replace C in the Decryption equation and we get

  $m \bigoplus H_2(e(H_1(ID_i), Q)^r) \bigoplus H_2(e(SK_i, C_1)$
  =$m \bigoplus H_2(e(H_1(ID_i), Q)^r) \bigoplus H_2(e(H_1(ID_i)^{\alpha}, g^r))$

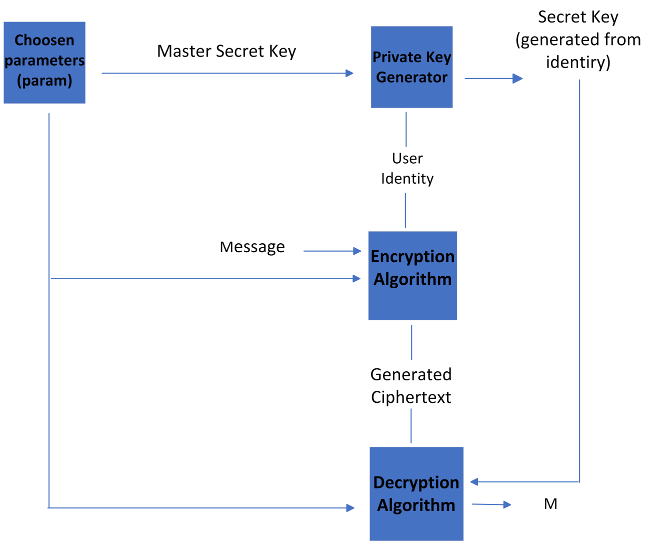


Fig. 1. Adapted IBE Scheme

$$
\begin{aligned}
&= m \bigoplus H_2(e(H_1(ID_i), g^{\alpha})^{r}) \bigoplus H_2(e(H_1(ID_i)^{\alpha}, g^{r})) \\
&= m \bigoplus H_2(e(H_1(ID_i), g)^{r\alpha}) \bigoplus H_2(e(H_1(ID_i), g)^{r\alpha}) \\
&= \mathrm{m}
\end{aligned}
$$

D. Application Framework

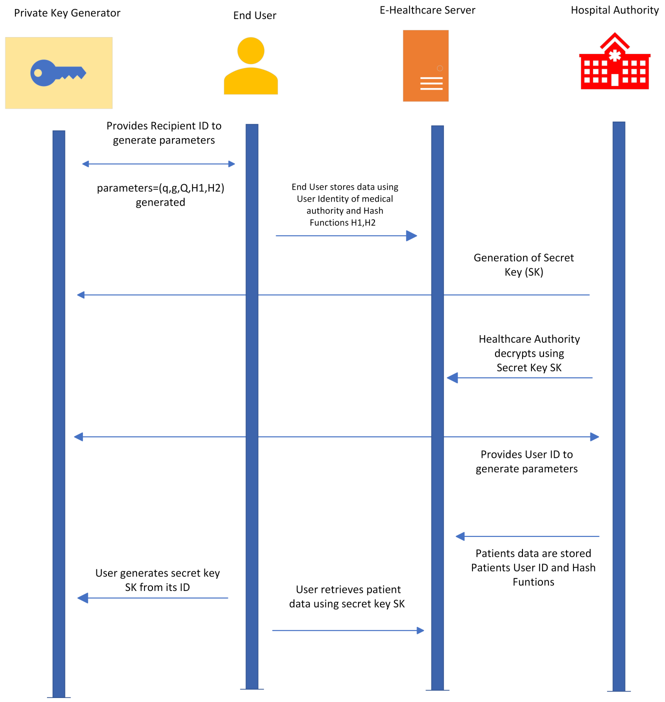
The implementation of our secure medical data sharing and storage system is centered around a user-friendly application framework. This framework provides a seamless user experience while ensuring the privacy and security of medical data. In this section, we discuss how the system functions and the steps involved in using it.

- User Authentication: The first step in our system is user authentication. Users, including end-users and hospital authorities, are required to log in using their unique email addresses. This login process ensures that only authorized individuals gain access to the system.

- Identity-Based Encryption (IBE): Our system leverages Identity-Based Encryption (IBE) to enable secure and efficient data sharing. IBE allows us to generate user-specific cryptographic keys based on their email addresses. This simplifies key management and enhances the overall user experience.

- Data Upload: Once authenticated, users can upload medical data reports to the system. This is a straightforward process that involves specifying the recipient's email address and attaching the relevant medical data. Hospital authorities can efficiently share patient records with other authorized parties, including other hospitals or specialists.

- Data Encryption: Before the data is stored in our system, it is encrypted using the recipient's email-based public key. This encryption ensures that the data remains confidential during storage and transit. Only the intended recipient, who can derive their private key from their email-based identity, can decrypt and access the data.



Private Key Generator
End User
E-Healthcare Server
Hospital Authority
Provides Recipient ID to generate parameters
parameters=(q,g,Q,H1,H2) generated
End User stores data using User Identity of medical authority and Hash Functions H1,H2
Generation of Secret Key (SK)
Healthcare Authority decrypts using Secret Key SK
Provides User ID to generate parameters
Patients data are stored Patients User ID and Hash Funtions
User generates secret key SK from its ID
User retrieves patient data using secret key SK

Fig. 2. Application Process Flow

- Data Decryption: On the recipient's side, the decryption process is initiated by generating their private key based on their identity (email address). This private key, combined with the recipient's email-based identity, allows them to decrypt the data and access the medical reports securely.

- Key Management: Key management is an essential aspect of our system. The Private Key Generator (PKG) is responsible for securely generating master secret keys, while users can derive their private keys based on their email-based identities.

IV. Result

Users successfully authenticated using their email-based identities.Key generation based on identity (email) was implemented, simplifying key management.Users, including hospital authorities, could efficiently upload medical data reports. Data was encrypted using recipient-specific public keys derived from email identities.Recipients could derive their private keys based on their email identities and decrypt the data. Fine-grained access control ensured that only authorized users could access specific medical records.The system demonstrated robust performance with minimal computational overhead. Medical data was securely transmitted and stored without compromising efficiency.Users commended the user-friendly application framework, which simplified the sharing and access of medical data.

Conclusion

This project introduced an end-to-end solution that combines user authentication, cryptographic key management, and efficient data sharing, all within a user-friendly application framework. The core premise of our project is the use of identity-based email addresses as the basis for cryptographic key generation and secure data exchange. By harnessing the power of IBE, we have significantly streamlined the process of securely sharing and storing medical records.

References

[1] Alexandra Boldyrev, Vipul Goyal, Virendra Kumar ”Identity-based encryption with efficient revocation”

[2] Carlisle Adams ”Improving User Privacy in Identity-Based Encryption Environments”

[3] Alexandra Rivero,Candelaria Hernández-Goya,Santos-González, Pino Caballero-Gil ”Patients’ Data Management System Through Identity Based Encryption”

[4] Boneh, D., Franklin, M. (2001). Identity-Based Encryption from the Weil Pairing. In: Kilian, J. (eds) Advances in Cryptology — CRYPTO 2001. CRYPTO 2001. Lecture Notes in Computer Science, vol 2139. Springer, Berlin, Heidelberg.

[5] Kannan Balasubramanian, M. Rajakani ”Implementation of Algorithms for Identity Based Encryption and Decryption”