International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 21 No. 3 (1) 2025

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 3(1), 2025

Research Paper

ANONYMOUS DATA LEAKAGE-RESILIENT IN MULTI-RECEIVER HYBRID DATA ENCRYPTION IN PUBLIC KEY SYSTEM

Sameena Begum[1], Samreen Sultana[2]
[1]PG Scholar, Department of CSE, Shadan Women's College of Engineering and Technology, Hyderabad, sameenabegum0821@gmail.com
[2]Assistant Professor, Department of CSE, Shadan Women's College of Engineering and Technology samreencme@gmail.com

ABSTRACT: A small portion of the secret keys used in cryptographic algorithms may be disclosed to attackers through side-channel attacks. In order to crack these current cryptographic systems, attackers have recently developed workable side-channel attacks. Researchers have made investments and put out a sound defense against these kinds of attacks, which is known as leakage-resilient cryptography. Recently, a number of public-key-based leakage-resilient anonymous multi-receiver encryption (LR-AMRE) techniques have also been developed. These LR-AMRE techniques, however, are not appropriate for a heterogeneous public-key environment, where a group of authorized receivers comprises a variety of receivers with different PKS configurations and secret/public key pairs. The first leakage-resilient anonymous heterogeneous multi-receiver hybrid encryption method (LR-AHMR-HE) for heterogeneous public-key system settings is proposed in this work. The LR-AHMR-HE technique is defined along with a novel framework and related adversary games. Adversaries are permitted to continuously intercept a small portion of secret keys during adversary games. Formal security proofs are presented under the adversary games to demonstrate that the suggested method is safe from two kinds of adversaries (malicious authorities and unauthorized users). The advantages of our method are illustrated through comparisons with a number of analogous prior designs.

KEYWORDS: leakage-resilient anonymous multi-receiver encryption (LR-AMRE), leakage-resilient anonymous heterogeneous multi-receiver hybrid encryption (LR-AHMR-HE)

Received: 16-7-2025 Accepted: 23-8-2025 Published: 30-8-2025

1. INTRODUCTION

Not even a small portion of the secret keys of all participants—including trusted authorities and regular users—are acknowledged to have been disclosed to enemies in the current classical cryptography. Adversaries have, however, recently developed workable side-channel attacks [1], [2] to intercept a small portion of the secret keys. Adversaries could continuously intercept fractional portions of these secret keys when they are used in repeated computations, allowing the secret keys to be entirely guessed. Therefore, the current conventional cryptographic techniques might no longer be secure against side-channel attacks. In order to address this issue, scholars have made investments and put up a strong Defence against such attacks, known as leakage robust cryptography. Many leakage-resilient cryptographic algorithms have been suggested in the last ten years. Many secure applications in real life call for sending a confidential message to several recipients inside an approved group. A sender can use a one-to-one public key encryption strategy for each recipient to meet this criterion, but doing so comes with a high computational cost because of the numerous encryptions. in the cryptography that uses public keys. Multi-receiver encryption (MRE) methods [11], [12] offer the capability of allowing a sender to use their public keys to encrypt and transmit a secret message to numerous recipients of an authorized group. The communication can be decrypted by any member of this authorized group using their own secret key. Certain sensitive applications, like personal pay-per-view television, must, nevertheless, safeguard the privacy of the receiver, meaning that other receivers cannot see who they are. As a result, the anonymous multi-receiver encryption (AMRE) scheme combines the features of identity privacy (anonymity) and MRE systems. Numerous AMRE techniques have been developed in the past by researchers [13], [14], and [15] based on different public-key system (PKS) settings, such as certificate-less (CL)-based [18], identification (ID)-based [17], and public key infrastructure (PKI)-based [16]. However, the problem of fending off side-channel attacks was not addressed by these AMRE systems. As a result, these schemes could be broken, as was previously described. LR-AMR-PKISC is a leakage-resilient anonymous multi-receiver signcryption system based on the PKI-based PKS setup that was presented by Tsai et al. [19] in 2022. Recently, Xie et al. also introduced LR-AMR-CLE, a leakage robust AMRE technique based on the CL-based PKS setup.

The following is an example of how AMRE schemes might be used in a heterogeneous public-key environment. These receivers will have different kinds of secret/public key pairs when an authorized group consists of heterogeneous multiple receivers

under different PKS configurations. In particular, a receiver may belong to a PKI-based, ID-based, or CL-based PKS setup in a heterogeneous public-key environment. The current AMRE, LR AMR-CLE, and LR-AMR-PKISC methods are not appropriate for a diverse public-key environment, as far as we are aware. Designing the first leakage-resilient anonymous heterogeneous multi-receiver hybrid encryption (LR-AHMRHE) method for a heterogeneous public-key environment using both PKI-based and CL-based PKS settings is the goal of the research

OBJECTIVE

The purpose of When an authorized group comprises heterogeneous multiple receivers under different PKS configurations, these receivers will have distinct types of secret/public key pairs. In leakage-resilient cryptography, there are two types of leakage models based on the strength of the leaking resistance. The first is the bounded leakage model, which allows attackers to intercept a portion of the secret keys used in each cryptographic operation but has a predefined size limit on the total number of leaked fraction parts (times).

RESEARCH SCOPE

This study indicates that sending a secret message to several recipients inside an authorized group is a common practice in real-world secure applications. To satisfy this requirement, a sender can employ a one-to-one public key encryption technique for every recipient; but, due to the large number of encryptions, this approach has a high computational cost.

In public-key cryptography, multi-receiver encryption (MRE) techniques provide the ability for a sender to encrypt and send a secret message to several recipients inside a pre-approved group using their public keys. Using their individual secret key, each member of this authorized group can decrypt the transmission.

STATEMENT OF THE PROBLEM

Any secure applications in real life include sending a secret message to several recipients inside an approved group. A sender can use a one-to-one public key encryption strategy for each recipient to meet this criterion, but doing so comes with a high computational cost because of the numerous encryptions. in cryptography using public keys. Using their public keys, a sender can encrypt and distribute a secret message to several recipients within an authorized group. The communication can be decrypted by any member of this authorized group using their own secret key.

The difficulty lies in creating a hybrid encryption system that allows a sender to safely deliver a message to several recipients, each of whom uses a distinct public-key cryptosystem, while simultaneously making sure.

Existing System

The AMRE, LR-AMR-CLE, and LR-AMR-PKISC schemes are not appropriate for the applications in the heterogeneous public-key environment, as was previously noted. The first leakage-resilient anonymous heterogeneous multi-receiver hybrid encryption (LR-AHMR-HE) technique for a heterogeneous public-key environment with PKI-based and CL-based PKS settings will be implemented under the unbounded leakage model.

To ensure leakage resistance, we use the multiplicative blinding technique in conjunction with a key renewal mechanism in the LR-AHMR-HE scheme. Each secret key in the scheme is divided into two parts.

Disadvantages of Existing System

- No proper user check. Anyone can try to access,
- No strong login system.
  Data not safeHackers can steal or see the data.
- Keys can leak. Secret keys can bepartly stolen.
  Not for all users.
- It doesn't work well if users have different types of keys.
- No Security authentication
- It cannot be secure for the data

Proposed System

The first leakage-resilient anonymous heterogeneous multi-receiver hybrid encryption method (LR-AHMR-HE) for the heterogeneous public-key system environment is proposed in this work.

The LR-AHMR-HE technique is defined along with a novel framework and related adversary games. Adversaries are permitted to continuously intercept a small portion of secret keys during adversary games. Formal security proofs are presented under the adversary games to demonstrate that the suggested method is safe from two kinds of adversaries (malicious authorities and unauthorized users).

The first LR-PKE technique that is secure in the unbounded leakage model was proposed. The suggested technique can provide unbounded leakage resilience because any two released fraction parts of a secret key are mutually independent during the key renewal process.

Proposed System Advantage

- Strong user check – Only the right users can access the system. Fake users are blocked.
- Data is safe – The system keeps your data protected from hackers.
- Works for all types of users – Even if users use different key types, the system still works smoothly.
- Stops key leakage – If some part of the secret key leaks, attackers still can't break the system.
- Stronger authentication
- It can have access to data security

2. RELATED WORKS

The crucial public-key cryptography known as the certificate-less public-key system (CL-PKS) solves the problems of key escrow and certificate management. The cloud revocation server (CRS) in combination with an outsourced revocable certificate less public-key system (ORCL-PKS) not only provides a revocation mechanism but also outsources the revocation functions to the CRS in order to reduce the computational load on the key generation center (KGC). Lately, side-channel attacks have threatened several types of conventional encryption, including CL-PKS. In fact, adversaries can use side-channel attacks to extract fractional parts of private (or secret) keys, so undermining the security of some cryptographic protocols (or schemes). To stave off such attacks, leakage-resilient cryptography is a desired tactic. Nevertheless, there hasn't been much focus on leakage-resistant certificateless cryptography. The first leakage-resilient outsourced revocable certificateless signature (LR-ORCLS) method is presented in this work. The proposed method allows adversaries to continually infer fractional components of private (or secret) keys and has an overall unbounded leaking feature. In the generic bilinear group (GBG) paradigm, we show that our method is existentially unforgeable against adversaries. Finally, comparisons with previous revocable certificateless signature methods demonstrate the benefits of the proposed scheme. **[1]**

The authenticated key exchange (AKE) protocol for client-server settings is a crucial cryptographic foundation that provides mutual authentication and communication confidentiality between clients and servers. Customers typically utilize low-processing-power IoT devices to connect to servers online in an Internet of Things (IoT) environment. Numerous AKE protocols that are suitable for IoT devices have been developed; they are frequently referred to as AKE-IoT protocols. Recently, side-channel attacks have been used to breach common cryptographic protocols because they allow an attacker to recover partial content of either long-term or short-term secret keys. Several leakage-resilient AKE (LRAKE) protocols were developed in order to stop these kinds of attacks. Unfortunately, the present LRAKE protocols are not suitable for IoT devices due to the expensive pairing operations required for client sides. The first successful LRAKE protocol for IoT devices, LRAKE-IoT, is introduced in this study. By employing the unbalanced computing method, our method does not require client-side pairing procedures. Security analysis is performed in the generic bilinear pairing group model to demonstrate the security of the proposed protocol in the continuous-leakage-resilient extended-Canetti–Krawczyk model. Finally, computational experiences on two IoT devices show that the proposed protocol is suitable for IoT devices. **[2]**

A ciphertext can be sent to a specific set of recipients by a data source using anonymous multi-receiver encryption (AMRE). By decrypting this ciphertext, any recipient belonging to the selected group can obtain the plaintext while keeping their identity hidden from other recipients. Previously, a number of anonymous Mult receiver certificate less encryption (AMR-CLE) schemes based on certificate less public-key cryptography (CL-PKC) were proposed to solve the key escrow issue of AMR-IBE schemes based on ID-based public-key cryptography as well as the certificate management issue of AMRE schemes based on conventional public-key cryptography. Lately, the current cryptographic systems, such as AMRE, AMR-IBE, AMR-CLE, etc., are at risk from side-channel attacks. One innovative method to fend against such attacks is leakage-resilient cryptography. But as of right moment, neither AMRE nor Mult receiver encryption are immune to side-channel attacks. We introduce the first anonymous Mult receiver certificateless encryption technique that is leakage-resilient (LR-AMR-CLE) in this work. Without compromising the initial security of AMR-CLE methods, our scheme allows attackers to periodically extract fractional content of each secret key used**. [3]**

Mobile edge computing (MEC), which provides processing and data storage capabilities within the range of a wireless access network close to users, is driving the need for new security technologies. Due to the increasing needs of user experience and the rapid increase of traffic, the existing security schemes are no longer able to meet the new requirements of lightweight and real-time security. Novel techniques that don't require complex calculations, like identity-based cryptography, are of special interest to researchers. To meet these needs, we developed a new authentication architecture for the MEC environment that provides secure and efficient communication.

This authentication architecture suggests an anonymous identity-based approach for lightweight devices. In the meantime, user privacy is fully protected. The proposed method is demonstrated to be secure under a particular security paradigm. We also describe the security aspects that our method meets. Comparisons of communication costs and time consumption are included at the end of the paper to demonstrate how effectively our method works compared to several previous approaches. **[4]**

A certificateless public-key system (CLPKS) has been proposed to solve the problems of certificate management and key escrow. A revocation mechanism must be included in a CLPKS setup in order to revoke compromised users. A revocable certificateless public-key system (RCLPKS) was presented as a solution to the revocation problem; in this system, the revocation capacity is managed by the key generation center (KGC). To lessen the computational load on the KGC, it was also

recommended to employ an outsourced revocation authority (ORA) in an RCLPKS option known as the RCLPKS-ORA configuration. Only recently has it been discovered that adversaries have been using side-channel attacks to undermine these well-known conventional public-key systems (including CLPKS, RCLPKS, and RCLPKS-ORA).

Fortunately, leakage-resilient cryptography is a means of preventing such assaults. The LR-RCLE-ORA system, the first leakage-resilient revocable certificateless encryption method utilizing an ORA, is proposed in this work. Formally, the proposed method is shown to be semantically secure against three types of adversaries in the RCLPKS and RCLPKS-ORA scenarios and robust against side-channel attacks. Even though adversaries can continuously extract partial components of secret keys utilized in various computing techniques, the proposed system remains secure. **[5]**

The fundamental premise of the earlier adversarial versions of public key cryptography is that both temporary and permanent secret (private) keys must be kept safe, as well as internal secret states. On the other hand, a recent threat called "side-channel attacks" makes it difficult to actually stop all possible disclosures of private information. Some of the currently used adversary models are insufficient since an adversary could only learn a fraction of these secret data through side-channel assaults. Indeed, the topic of side-channel attack-resistant leakage-resilient encryption has garnered a lot of attention recently. The continual leaking model has not yet been used to construct leaking-resilient certificateless key encapsulation (LR-CL-KE) or public key encryption (LR-CL-PKE) systems. In this work, we introduce the first LR-CL-KE technique under the constant leakage scenario. Additionally, in the generic bilinear group (GBG) model, we formally show that the proposed LR-CL-KE approach is semantically secure against chosen ciphertext attacks for both Type I and Type II adversaries. **[6]**

The signcryption system should be able to withstand a range of leakage threats in practical situations. This paper presents a unique leakage-resilient certificateless sign encryption (LR-CLSC) method without bilinear pairing. The security of this approach is based on the discrete logarithm (DL) problem and the computational Diffie-Hellman (CDH) assumption. When accounting for computational costs, our proposed method outperforms traditional certificateless encryption methods in terms of efficiency, security, and ciphertext length. The proposed approach in the random oracle model is semantically safe against adaptive posteriori chosen-ciphertext key-leakage attacks (IND-KL-CCA2) and existentially unforgeable against chosen-message key-leakage attacks (EUF-KL-CMA) based on the difficulty of the CDH assumption. Furthermore, if the attacker uses side channel attacks to learn even a small amount about the secret key, it will maintain the original security. Both the key leakage parameter λ and the message length m are impacted by $\lambda \leq \log q - m - 2\log(1\omega)$. As a dependency between λ and m is undesired, a novel version is provided that also works against IND-KL-CCA2 and EUF-KL-CMA. The leakage resilient length of λ can reach up to $\lambda \leq \log q - 2\log(1\omega)$, and its size is constant regardless of the message length m. Our proposed method is the first LR-CLSC system with an independent leakage parameter and may be employed with mobile internet. **[7]**

We describe a Hierarchical Identity Based Encryption (HIBE) system where the ciphertext consists of only three group components and decryption requires only two bilinear map computations, regardless of the hierarchy depth. Encryption works just as well as earlier HIBE systems. We show that the method is selective-ID secure in the standard model and completely secure in the random oracle model. Our approach gives an effective mechanism for encrypting to the future and provides very efficient forward secure public key and identity-based cryptosystems (with short ciphertexts), in addition to transforming the NNL broadcast encryption system into an effective public key broadcast system.

The system's limited delegation capabilities include the ability to provide users with restricted private keys that only allow delegation to a limited depth. The HIBE system can be modified to support private keys of sublinear size at the cost of some ciphertext expansion. **[8].**

The crucial public-key cryptography known as the certificateless public-key system (CL-PKS) solves the problems of key escrow and certificate management. An outsourced revocable certificateless public-key system (ORCL-PKS) with a cloud revocation server (CRS) not only provides a revocation mechanism but also further outsources the revocation functionality to the CRS to reduce the computational load on the key generation center (KGC). Lately, side-channel attacks have threatened several types of conventional encryption, including CL-PKS. In fact, adversaries can use side-channel attacks to extract fractional parts of private (or secret) keys, so undermining the security of some cryptographic protocols (or schemes).

To stave off such attacks, leakage-resilient cryptography is a desired tactic. Nevertheless, there hasn't been much focus on leakage-resistant certificateless cryptography. This work presents the first leakage-resilient outsourced revocable certificateless signature (LR-ORCLS) method. The proposed method allows adversaries to continually infer fractional components of private (or secret) keys and has an overall unbounded leaking feature. In the generic bilinear group (GBG) paradigm, we show that our method is existentially unforgeable against adversaries. Finally, comparisons with previous

revocable certificateless signature techniques are provided to show the benefits of the proposed method. **[9]**

Side-channel attacks have recently become a danger to all traditional cryptography systems. Conventional encryption frequently makes the assumption that adversaries won't be able to see the private or secret keys. However, side-channel attacks could be used by an attacker to obtain the contents of these private/secret keys. An effective defense against side-channel assaults is leakage-resilient cryptography. The identity-based public-key system (ID-PKS) is one attractive public-key ecosystem. ID-PKS settings also remove the need to construct the public-key infrastructure, in addition to the certificate requirement.

In order to address the problem of user revocation in ID-PKS configurations, the revocable ID-PKS (RIDPKS) setting has attracted a lot of attention. Numerous cryptographic methods based on RIDPKS settings have been introduced. However, in RID-PKS conditions, neither an encryption method nor a leakage-resilient signature is recommended. This paper presents the first leakage-resilient revocable ID-based signature (LR-RIBS) technique with cloud revocation capability (CRA) in the continuous leakage model. Furthermore, a new adversary model is defined for LR-RIBS schemes with CRA. Security research under this innovative adversary model demonstrates that our LR-RIBS scheme with CRA is provably secure in the generic bilinear group (GBG) scenario. In order to determine whether our solution is appropriate for mobile devices, a performance study was finally conducted. **[10]**

3. METHODOLOGIES

The proposed system integrates several advanced cryptographic techniques to ensure strong security and efficiency. Leakage-Resilient Cryptography protects against side-channel attacks, while Hybrid Encryption combines public and private key methods to securely transmit data to multiple users. To further enhance security, Multiplicative Blinding makes the key appear different in every use, preventing attackers from guessing even if partial information is exposed, and Key Renewal ensures that secret keys are regularly updated. The system also supports Anonymous Multi-Receiver Encryption (AMRE), allowing data to be sent to multiple recipients without revealing their identities, thus preserving anonymity. Its modular design separates functionalities across different components—Authority, Data Provider, Receiver, and Attacker—each handling distinct responsibilities. Finally, a Flask-based web application is implemented to simulate and test the system in real-world scenarios, demonstrating its practicality and robustness.

MODULE DESCRIPTION:

1. Design of User Interfaces

We create the project's windows in this module. All users can securely log in using these Windows. Users must enter their username and password in order to connect to the server; only then may they do so. The user can log in to the server directly if they have already left; if not, they must register their information, including their username, password, and email address. To maintain the upload and download speeds, the server will generate an account for every user. The user ID will be assigned to the name. Usually, logging in allows you to access a certain page.

2. Authority

This is the first module authority has a user ID and a password. The authority has the data provider's details. The authority has the receiver's details. The authority has a request for keys. The authority has an attacker detect details

3. Data Provider

This is the Second module of this project. The data provider has a register with an ID. Then log in with a mail ID and password. A data provider has data to transfer to a stored a data.

4. Side Channel

This is the third module of this project. In this project data holder has a register with all details and login with a user ID and password. The owner data holder has a store a file, the file has an upload with a text file to the data.

5. Receiver

This is the fourth module of this project. The receiver has a register with all details, and then logs in with an email id and password. The receiver has a search the Receiver has a store we can search a data. Data receiver has a key verification the keys are verify the correct, then it will have a decrypt a file download.

4. ALGORITHM

MRE schemes (Multi-Receiver Encryption)

Many secure applications require transmitting a secret message to multiple receivers of an authorized group. For this requirement, a sender can employ a one-to-one public key encryption scheme for each receiver, but the required computation load of the sender is large due to multiple encryptions. In public-key cryptography.

Multi-receiver encryption (MRE) schemes provide the functionality in the sense that a sender may encrypt and send a secret message to multiple receivers of an authorized group using their public keys. Each receiver of this authorized group can use her/his own secret key to decrypt the message. However, some sensitive applications. Therefore, anonymous multi-receiver encryption (AMRE) schemes possess the functionalities of both the MRE schemes and identity privacy (anonymity). In the past, researchers have proposed numerous AMRE schemes based on various public-key system (PKS) settings that include public

key infrastructure (PKI)-based, identity (ID)-based, and certificate-less (CL)-based PKS settings. However, these AMRE schemes did not address the issue of resisting side-channel attacks. When an authorized group includes heterogeneous multiple receivers under various PKS settings, these receivers will have various types of secret/public key pairs.

(1) It is the first AMRE scheme suitable for heterogeneous multiple receivers under various PKS settings in a heterogeneous public-key environment.

(2) It is the first LR-AHMR HE scheme with unbounded leakage resilience.

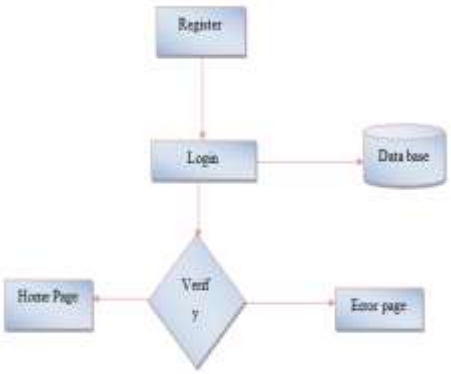
(3) The decryption computation cost of each heterogeneous receiver is constant

AMRE, LR AMR-CLE, and LR-AMR-PKISC schemes

The existing AMRE, LR AMR-CLE, and LR-AMR-PKISC schemes are not suitable for a heterogeneous public-key environment. In the paper, we aim to design the first leakage-resilient anonymous heterogeneous multi-receiver hybrid encryption (LR-AHMR HE) scheme for a heterogeneous public-key environment with the PKI-based and the CL-based PKS settings. The existing AMRE and leakage resilient AMRE (LR-AMRE) schemes are not suitable for sending a message to heterogeneous receivers in a heterogeneous public-key environment. The point is that our scheme is the first LR-AHMR-HE scheme for a heterogeneous public-key environment with the PKI-based and the CL-based PKS settings.

5. DATA FLOW DIAGRAM

Level 0



Level 1

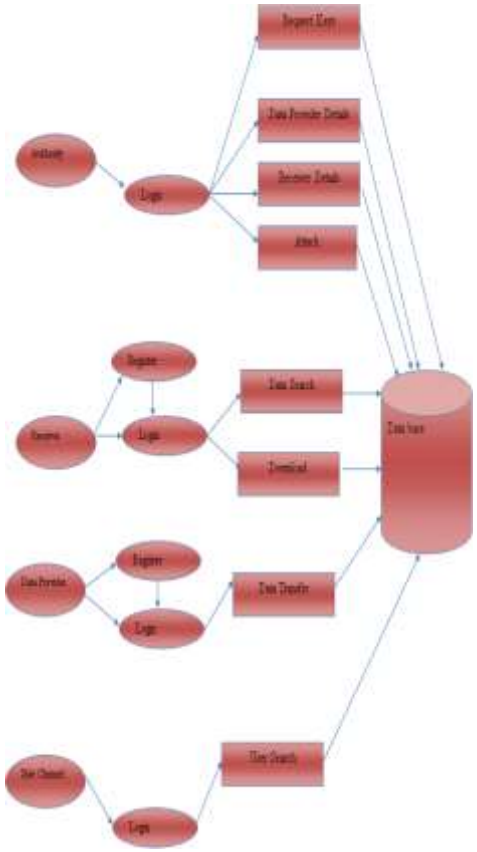


Fig. 5: Data Flow Diagram

6. SYSTEM ARCHITECTURE

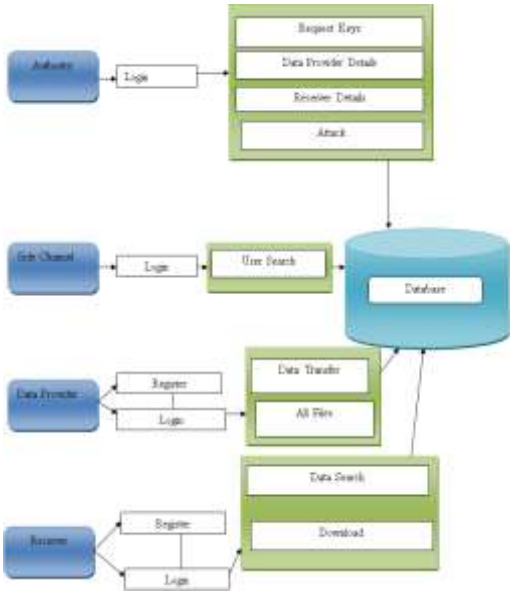


Fig 6: SYSTEM ARCHITECTURE

7. RESULT

The proposed LR-AHMR-HE scheme successfully overcomes the drawbacks of existing systems by ensuring strong authentication, secure data protection, and resilience against secret key leakage in heterogeneous public-key environments. By

combining multiplicative blinding with a key renewal mechanism, the scheme achieves unbounded leakage resistance and allows secure access for all types of users, even with different key settings. Formal security proofs validate its strength against both malicious authorities and unauthorized users, proving that the system is reliable, practical, and highly secure for real-world applications.

8. CONCLUSION

In this paper, we have proposed the first AMRE scheme with both leakage-resilience and heterogeneous multiple receivers, termed as the LR-AHMR-HE scheme. In the LR-AHMR-HE scheme, we employed the key renewing process with the multiplicative blinding technique to achieve leakage resilience. Under the DL assumption in the GBG model and the SOWHF assumption, we have proved that the proposed scheme is EC-CCA-LR-AHMR-HE and EA-CCA-LR-AHMR-HE secure against the chosen cipher text adversaries A (illegitimate user and malicious authority), namely, it possesses both encryption confidentiality and encryption anonymity. Finally, the comparisons between several previous schemes and ours were made to show that our scheme possesses the following merits. (1) It is the f first AMRE scheme suitable for a heterogeneous public-key environment (the PKI-based and the CL-based PKS settings). (2) It is the first LR-AHMR-HE scheme with unbounded leakage resilience. (3) The decryption computation cost of each heterogeneous receiver is constant.

9. FUTURE ENHANCEMENT

For potential attack vectors, future work could focus on further exploring other potential attack vectors, such as insider attacks, collusion attacks, or denial-of-service attacks, to enhance the overall security of the scheme. Through more in-depth analysis and testing, we can develop more robust defense schemes to counter different forms of attacks. Additionally, regarding the scheme's applicability and optimization, future work should delve into a deeper investigation of its effectiveness in specific application scenarios. We can further optimize the scheme to make it more suitable for various practical use cases, such as those in healthcare and finance sectors.

10. REFERENCES

[1] D. Brumleyand D. Boneh, Remote timing attacks are practical," Comput. Netw., vol. 48, no. 5, pp. 701–716, Aug. 2005.

[2] E. Biham, Y. Carmeli, and A. Shamir, "Bug attacks," in Proc. Crypto, 2008, pp. 221–240. [3] E. Kiltz and K. Pietrzak, "Leakage resilient Elgamal encryption," in Proc. Asiacrypt, 2010, pp. 595–612.

[4] D. Galindo and S. Virek, "A practical leakage-resilient signature scheme in the generic group model," in Selected Areas in Cryptography (Lecture Notes in Computer Science), vol. 7707. Berlin, Germany: Springer, 2013, pp. 50–65.

[5] D. Galindo, J. Großschädl, Z. Liu, P. K. Vadnala, and S. Vivek, "Implementation of a leakage-resilient ElGamal key encapsulation mechanism," J. Cryptograph. Eng., vol. 6, no. 3, pp. 229–238, Sep. 2016.

[6] J.-D. Wu, Y.-M. Tseng, S.-S. Huang, and W.-C. Chou, "Leakage-resilient certificateless key encapsulation scheme," Informatica, vol. 29, no. 1, pp. 125–155, 2018.

[7] J.-D. Wu, Y.-M. Tseng, and S.-S. Huang, "An identity-based authenticated key exchange protocol resilient to continuous key leakage," IEEE Syst. J., vol. 13, no. 4, pp. 3968–3979, Dec. 2019.

[8] Y. Tseng, J.-D. Wu, S.-S. Huang, and T.-T. Tsai, "Leakage-resilient outsourced revocable certificateless signature with a cloud revoca tion server," Inf. Technol. Control, vol. 49, no. 4, pp. 464–481, Dec. 2020.

[9] A.-L. Peng, Y.-M. Tseng, and S.-S. Huang, "An efficient leakage-resilient authenticated key exchange protocol suitable for IoT devices," IEEE Syst. J., vol. 15, no. 4, pp. 5343–5354, Dec. 2021.

[10] Y.-M. Tseng, S.-S. Huang, T.-T. Tsai, Y.-H. Chuang, and Y.-H. Hung, "Leakage-resilient revocable certificateless encryption with an outsourced revocation authority," Informatica, vol. 33, no. 1, pp. 151–179, 2022.

[11] K. Kurosawa, "Multi-receiver public-key encryption with shortened ciphertext," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 2274. Berlin, Germany: Springer, 2002, pp. 48–63.

[12] M. Bellare, A. Boldyreva, and D. Pointcheval, Multi-receiver encryption schemes: Security notions and randomness re-use," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 2567. Berlin, Germany: Springer, 2003, pp. 85–99.