IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204149 |

Affordable, Secure, and Anonymous Data Sharing With Forward Security

Amrutha Biradar, Avusali Mani Harshith, Abhiram Reddy, S.Bhagya Rekha

UG Student, Dept. of CSE, Anurag University, Hyderabad, Telangana, India

UG Student, Dept. of CSE, Anurag University, Hyderabad, Telangana, India

UG Student, Dept. of CSE, Anurag University, Hyderabad, Telangana, India

Assistant Professor, Dept. of CSE, Anurag University, Hyderabad, Telangana, India

ABSTRACT: Data sharing has never been easier with the advances of cloud computing, and an accurate analysis on the shared data provides an array of benefits to both the society and individuals. Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to construct an anonymous and authentic datasharing system. It allows a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. Yet the costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. Identity-based (ID-based) ring signature, which eliminates the process of certificate verification, can be used instead. here, we further enhance the security of ID-based ring signature by providing forward security:If a secret key of any user has been compromised, all previous generated signatures that include this user still remain valid.

KEYWORDS: Forward Security, ID-based Ring Signature, Public Key Infrastructure.

I. LITERATURE SURVEY

M. H. Au, J. K. Liu, T. H. Yuen, and D. S. Wong, "ID-based ring signature scheme secure in the standard model," in Proc. 1st Int. Workshop SecurityAdv. Inform. Computer. Security, 2006, vol. 4266, pp. 1–16.

The only known construction of ID-based ring signature schemes which maybe secure in the standard model is to attach certificates to non-ID-based ring signatures. This method leads to schemes that are somewhat inefficient and it is an open problem to find more efficient and direct constructions. In this paper, we propose two such constructions. Our first scheme, with signature size linear in the cardinality of the ring, is secure in the standard model under the computational Diffie-Hellman assumption. The second scheme, achieving constant signature size,is secure in a weaker attack model (the selective ID and selective chosen message model), under the Diffie-Hellman Inversion assumption.
To form a ring signature, a group of users is selected, including the signer and others for anonymity. The signer generates a signature on a chosen message using their private key and the public keys of users in the ring. This signature is craftedto conceal the actual signer's identity while confirming the involvement of one of the ring members. Verifying the signature requires access to the public keys involved, allowing confirmation of the message's authenticity without revealing thesigner's identity.

Security in this scheme is based on concrete cryptographic assumptions like the hardness of factoring or discrete logarithm problems. Rigorous security proofs are provided without relying on idealized assumptions, ensuring robustness against various cryptographic attacks. Additionally, the scheme guarantees non- repudiation, meaning signers cannot deny their involvement in the signing process,bolstering accountability.

M. Abe, M. Ohkubo, and K. Suzuki, "1-out-of-n signatures from a variety of keys," in Proc. 8th Int. Conf. Theory Appl. Cryptol. Inform. Security: Adv. Cryptol., 2002, vol. 2501, pp. 415–432.
This paper addresses how to use public-keys of several different signature schemesto generate 1-out-of-n signatures. Previously known constructions are for either RSA-keys only or DL-type keys only. We present a widely applicable method to construct a 1-out-of-n signature scheme that allows mixture use of different flavorsof keys at the same time. The resulting scheme is more efficient than previous schemes even if it is used only with a single type of keys. With all DL-type keys, it yields shorter signatures than the ones of the previously known scheme based on the witness

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204149 |

indistinguishable proofs by Cramer, et al. With all RSA-type keys, it reduces both computational and storage costs compared to that of the Ring signatures by Rivest, et al.

In this cryptographic scheme, there are n participants or signers, each possessing their own unique private key. The public keys corresponding to these private keys are known to all participants, allowing them to verify signatures generated by others.To create a signature using the "1 out of n" scheme, any one of the n signers can independently generate a partial signature using their private key and the message to be signed. However, this partial signature alone is insufficient forverifying the authenticity of the message.Once the partial signature is created, the signer broadcasts it to all other participants in the group. Each participant then combines the received partial signature with their own partial signature to create an aggregated signature. This aggregation process is typically done using a cryptographic function or algorithm that ensures the resulting signature remains valid and cannot be tampered with.

Once the admin verify the authenticity of the message by checking the aggregated signature segregated signature is computed, any entity with access to the public keys of the signers cat the message and the public keys of the participants. If the verification process is successful, it confirms that at least one of the n signers has endorsed the message, but it does not reveal which specific signer produced the signature.In 2001, Rivest et al. firstly introduced the concept of ring signatures. A ring signature is a simplified group signature without any manager. It protects the anonymity of a signer. The first scheme proposed by Rivest et al. was based on RSA cryptosystem and certificate based public key setting. The first ring signature scheme based on DLP was proposed by Abe, Ohkubo, and Suzuki. Their scheme is also based on the general certificate-based public key setting too. In 2002, Zhang and Kim proposed a new ID-based ring signature scheme using pairings. Later Lin and Wu proposed a more efficient ID-based ring signature scheme. Both these schemes have some inconsistency in computational aspect. In this paper we proposea new ID-based ring signature scheme and a proxy ring signature scheme. Both the schemes are more efficient than existing one. These schemes also take care of the inconsistencies in above two schemes.

M. Bellare and S. Miner, “A forward-secure digital signature scheme,” in Proc.19th Annu. Int. Cryptol. Conf., 1999, vol. 1666, pp. 431–448.

Confidentiality and integrity of sensitive information is paramount. However, the landscape of cybersecurity is constantly evolving, with adversaries continually devising new strategies to breach security measures and compromise data. In this context, forward security emerges as a critical concept, offering a proactive approach to safeguarding confidentiality and mitigating the impact of potential security breaches. This essay delves into the significance of forward security, its underlying principles, implementation strategies, and implications for cybersecurity practices.

Forward security, also known as perfect forward secrecy (PFS), is a cryptographic property that ensures the confidentiality of past communications even if long-term secret keys are compromised in the future. In essence, forward security protects against retroactive decryption of encrypted communications by ensuring that the compromise of a long-term key does not compromise the confidentiality of past sessions. This property is particularly relevant in scenarios where encrypted communications may be intercepted and stored by adversaries for future decryption attempts.

The significance of forward security lies in its ability to limit the impact of security breaches and protect sensitive information from unauthorized access. By regularly refreshing session keys and employing cryptographic techniques that prevent retroactive decryption, forward security enhances the resilience of communication protocols and strengthens the overall security posture of systems and applications.

Principles of Forward Security: At the heart of forward security lies the principle of ephemeral key exchange, wherein session keys are generated dynamically for each communication session and discarded after use. This contrasts with static key exchange methods, where the same long-term keys are used repeatedly for multiple sessions. By using ephemeral keys, forward security ensures that even if a long- term key is compromised, it cannot be used to decrypt past communications encrypted with session keys that have already been discarded.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204149 |

A. K. Awasthi and S. Lal, "Id-based ring signature and proxy ring signature schemes from bilinear pairings," CoRR, vol. abs/cs/ 0504097, 2005.

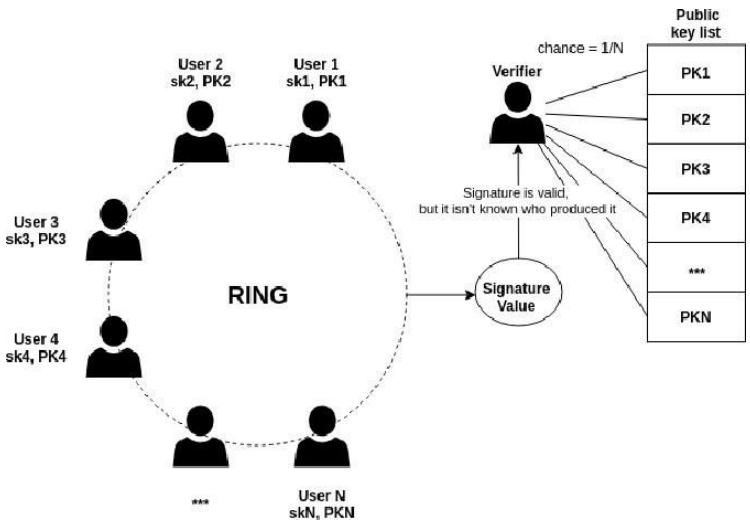
In 2001, Rivest et al. firstly introduced the concept of ring signatures. A ring signature is a simplified group signature without any manager. It protects the anonymity of a signer. The first scheme proposed by Rivest et al. was based on RSA cryptosystem and certificate based public key setting. The first ring signature scheme based on DLP was proposed by Abe, Ohkubo, and Suzuki. Their scheme is also based on the general certificate-based public key setting too. In 2002, Zhang and Kim proposed a new ID-based ring signature scheme using pairings. Later Lin and Wu proposed a more efficient ID-based ring signature scheme. Both these schemes have some inconsistency in computational aspect. In this paper we propose a new ID-based ring signature scheme and a proxy ring signature scheme. Both the schemes are more efficient than existing one. These schemes also takecare of the inconsistencies in above two schemes.

II. METHODOLOGY AND APPROACH

In the realm of ID-based ring signatures, forward security entails that if a user's secret key gets compromised, all previously generated signatures involving this user will remain valid. This characteristic assumes paramount importance in large- scale data sharing systems. Imagine a scenario where a single user's secret key is compromised – in such a case, it becomes impractical to require every data owner to reauthenticate their data.

The essence of forward security is rooted in its ability to maintain the integrity and confidentiality of shared data, despite potential breaches or vulnerabilities. It servesas a safeguard against unauthorized access or tampering, thereby bolstering the trust and reliability of data sharing ecosystems.

Addressing this challenge necessitates innovative solutions that can preserve the integrity and confidentiality of data in the face of evolving security threats. While the specific details of the proposed enhancement are not provided, the overarching objective is clear: to devise a mechanism that ensures forward security within ID- based ring signatures, thereby enhancing the resilience of large-scale data sharing systems.



Modules

Cloud Service Provider

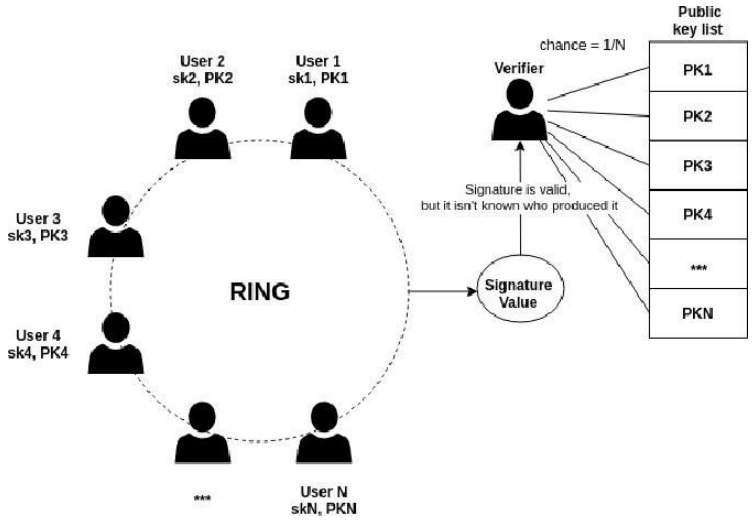
In the first module, we develop the System model of Cloud with the Users.In this module, we develop Cloud Service Provider module. This is an entity that provides a data storage service in public cloud. The S-CSP provides the data outsourcing service and stores data on behalf of the users. In this paper, we assume that S-CSP is always online and has abundant storage capacity and computation power.And also it approves the group.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204149 |

integrity and confidentiality of data in the face of evolving security threats. While the specific details of the proposed enhancement are not provided, the overarching objective is clear: to devise a mechanism that ensures forward security within ID- based ring signatures, thereby enhancing the resilience of large-scale data sharing systems.



Modules
Cloud Service Provider

In the first module, we develop the System model of Cloud with the Users.In this module, we develop Cloud Service Provider module. This is an entity that provides a data storage service in public cloud. The S-CSP provides the data outsourcing service and stores data on behalf of the users. In this paper, we assume that S-CSP is always online and has abundant storage capacity and computation power.And also it approves the group.

Data Owners Module
A data owner is an entity that wants to outsource data storage to the S-CSP and access the data later. The Data owner uploads the file in the cloud.
This module is responsible for overseeing the lifecycle of data assets, ensuring their security, accessibility, and integrity throughout their existence within the cloud environment.
At its core, the data owners module enables users or entities to maintain ownership and control over their data stored and processed in the cloud. This includes functionalities such as uploading, modifying, and deleting data, as well as setting access permissions and sharing preferences. Through an intuitive user interface, data owners can manage their data assets efficiently, organizing them into logical structures, and applying metadata tags for easy retrieval and categorization.

ID-based ring signature

Identity-based ring signatures combine the concepts of ring signatures and identity-based cryptography. Ring signatures allow a user to sign a message on behalf of a group, obscuring the signer's identity within the group. Identity-based cryptography, on the other hand, enables users to be identified by unique identifiers, such as email addresses or domain names, instead of cryptographic keys.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204149 |

In identity-based ring signatures, a trusted authority, known as the Private Key Generator (PKG), generates private keys for users based on their identifiers. These private keys are derived from a master secret key held by the PKG. Users' public keys are then derived from their private keys and distributed as needed.

Implementing a web-based cloud computing project involves several sequential steps that ensure the creation of a robust and functional application. Initially, thorough project planning and requirements gathering are essential to define the project's objectives, scope, and target audience. Stakeholder input is crucial during this phase to ensure alignment with user needs and expectations. Once the requirements are established, the architecture design phase begins, where the overall structure of the cloud-based application is planned. This includes designing the front-end, back-end, and database components, as well as selecting appropriate technologies and frameworks to support the project's goals.

With the architecture design in place, the focus shifts to front-end development, where the user interface (UI) of the web application is created. This involves designing and implementing the visual elements that users interact with, such as menus, buttons, forms, and other UI components. Front-end developers use a combination of HTML, CSS, and JavaScript frameworks like React, Angular, or Vue.js to build responsive and user-friendly interfaces that provide a seamless experience across different devices and screen sizes.

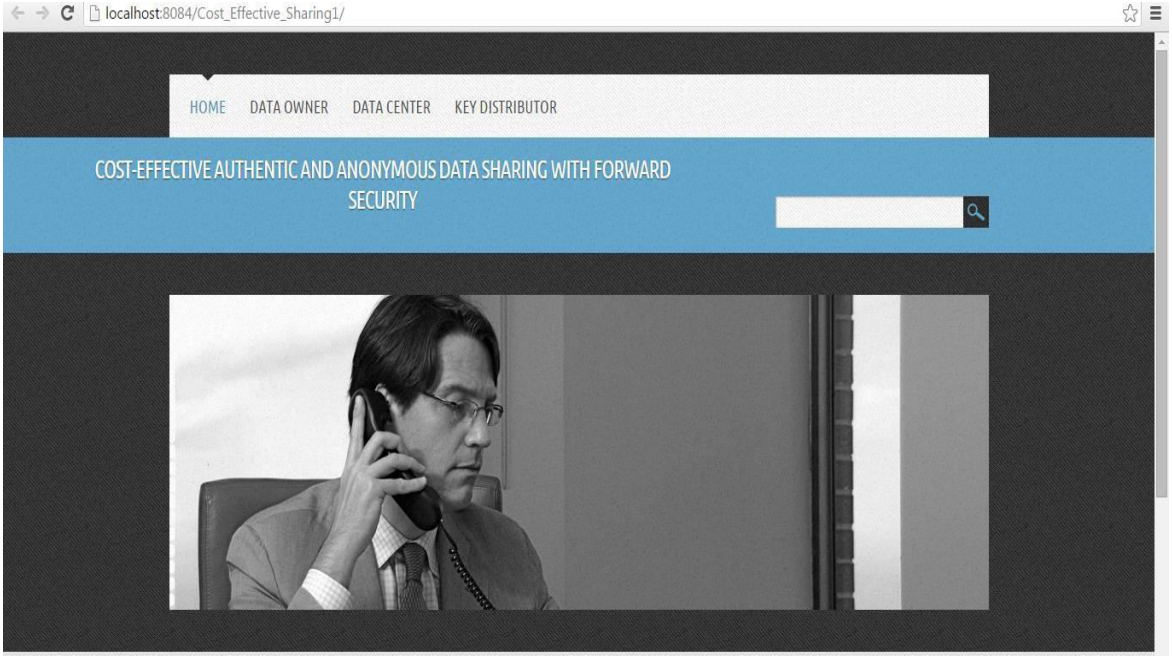
Simultaneously, back-end development takes place, where the server-side logic and functionality of the web application are implemented. This includes handling user authentication, managing data storage and retrieval, processing user requests, and enforcing business logic rules. Back-end developers use programming languages such as Python, Java, Node.js, or PHP, along with frameworks like Django, Spring Boot, Express.js, or Laravel, to build the server-side components ofthe application.

Database design and development are integral parts of the implementation process, where the structure and schema of the database are defined to efficiently store and manage application data. Developers use relational databases like MySQL, PostgreSQL, or SQL Server, or NoSQL databases like MongoDB or Cassandra, depending on the project's requirements and data modeling needs.

III. RESULTS AND DECLARATION

Here you can see the website after redirecting to the web browser

Home Screen



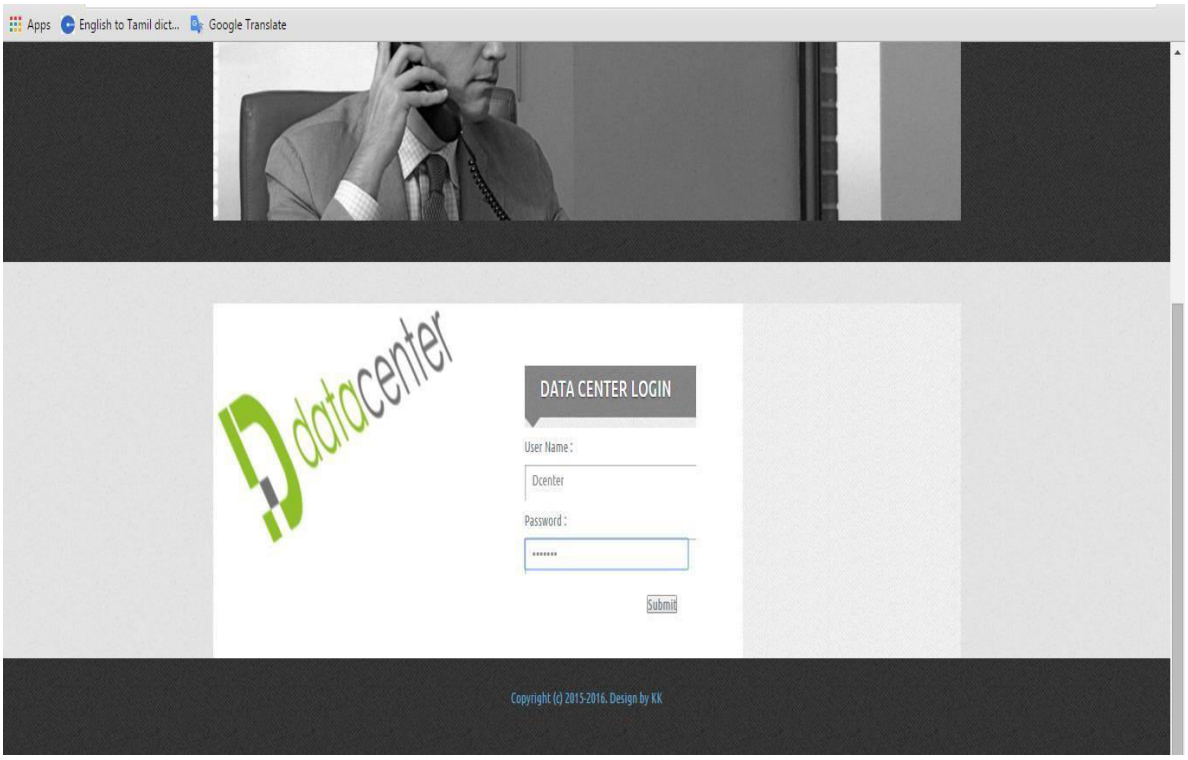
International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

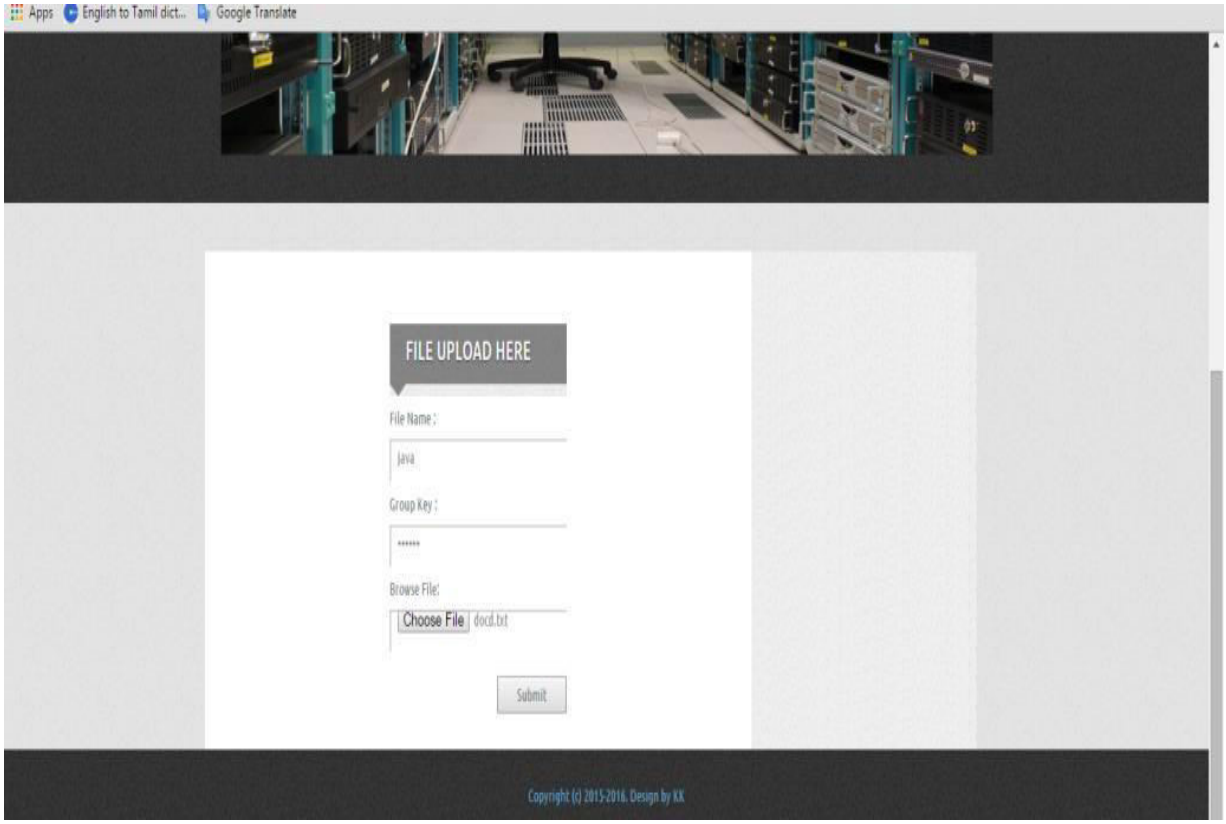
|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204149 |

User Registration



Key Generation

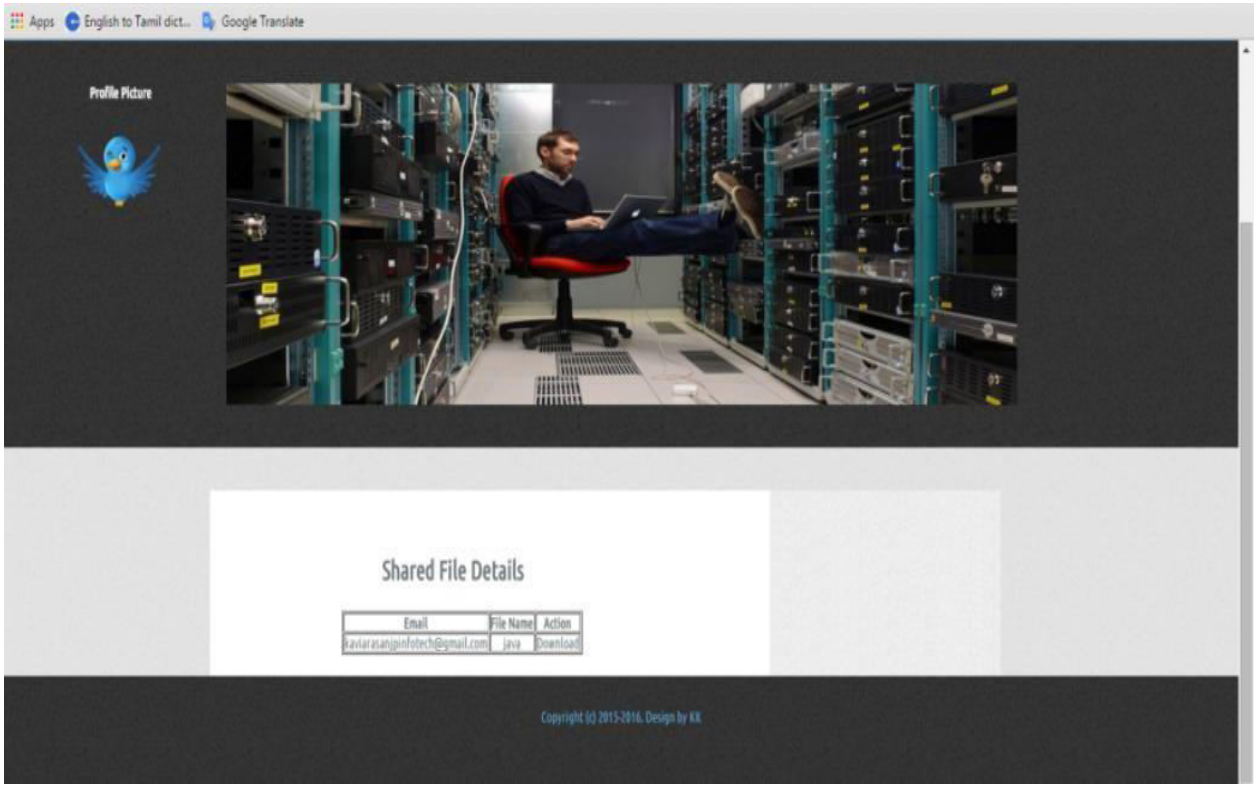


| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204149 |

Download the shared files



V. CONCLUSION

Motivated by the practical needs in data sharing, we proposed a new notion called forward secure ID-based ring signature. It allows an ID-based ring signature scheme to have forward security. It is the first in the literature to have this feature for ring signature in ID-based setting. Our scheme provides unconditional anonymity and can be proven forward- secure unforgeable in the random oracle model, assuming RSA problem is hard. Our scheme is very efficient and does not require any pairing operations. The size of user secret key is just one integer, whilethe key update process only requires an exponentiation. We believe our scheme will be very useful in many other practical applications, especially to those require user privacy and authentication, such as ad-hoc network, e-commerce activities and smart grid. Our current scheme relies on the random oracle assumption to prove its security. We consider a provably secure scheme with the same features in the standard model as an open problem and our future research work.

REFERENCES

1. M. Abe, M. Ohkubo, and K. Suzuki, "1-out-of-n signatures from a variety of keys," in Proc. 8th Int. Conf. Theory Appl. Cryptol. Inform. Security: Adv. Cryptol.,2002, vol. 2501, pp. 415–432.
2. R. Anderson, "Two remarks on public-key cryptology," Manuscript, Sep. 2000.(Relevant material presented by the author in an invited lecture at the Fourth ACMConference on Computer and Communications Security, 1997.)
3. G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A practical and provably secure coalition-resistant group signature scheme," in Proc. 20th Annu. Int. Cryptol.Conf. Adv. Cryptol., 2000, vol. 1880, pp. 255–270.
4. M. H. Au, J. K. Liu, T. H. Yuen, and D. S. Wong, "ID-based ring signature scheme secure in the standard model," in Proc. 1st Int. Workshop Security Adv.Inform. Comput. Security, 2006, vol. 4266, pp. 1–16.
5. K. Awasthi and S. Lal, "Id-based ring signature and proxy ring signatureschemes from bilinear pairings," CoRR, vol. abs/cs/ 0504097, 2005.
6. M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: Formal definitions, simplified requirements and a construction based on general assumptions," in Proc. 22nd Int. Conf. Theory Appl. Cryptographic Techn., 2003,vol. 2656, pp. 614–629.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204149 |

7. M. Bellare and S. Miner, "A forward-secure digital signature scheme," in Proc. 19th Annu. Int. Cryptol. Conf., 1999, vol. 1666, pp. 431–448.
8. J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau, "Security and privacy-enhancing multicloud architectures," IEEE Trans. Dependable Sec. Comput.,vol. 10, no. 4, pp. 212–224, Jul. \Aug. 2013.
9. Boldyreva, "Efficient threshold signature, multisignature and blind signature schemes based on the gap Diffie-Hellman group signature scheme," in Proc. 6th Int. Workshop Theory Practice PublicKey Cryptography: Public Key Cryptography, 2003, vol. 567, pp. 31–46.
10. D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Proc.Annu.Int. Cryptol. Conf. Adv. Cryptol., 2004, vol. 3152, pp. 41–55.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details