International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

POEDDP-A FAST RSA-BASED PROOF OF POSSESSION ACCUMULATOR OF DYNAMIC DATA ON THE CLOUD

E. MOUNIKA REDDY [1], BANDARU BHARATH KUMAR REDDY [2], DILLI PAVAN KALYAN [3], BANDI VINAY KUMAR [4], KUMMARIKUNTA VARSHITH KRISHNA [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— The ease of usage and the convenience of cloud computing come with considerable responsibility. The latter, consists of carefully addressing different security aspects of this technology. The integrity and availability of the outsourced data constitute essential considerations for adopters' final decisions. However, the most critical factor is the efficiency of integrity checks, which must prioritize restricted-resource data owners without affecting the performance of the Cloud Service Provider. This paper proposes a secure scheme, called Proof of Exponentiation of Dynamic Data Possession PoEDDP based on RSA-Accumulators. The proof of concept demonstrates that this scheme is 20 times faster compared to other RSA-based cryptographic accumulator schemes. It could be improved to achieve great results with proper optimizations on the larger integer multiplication side.

Index Terms – Cloud computing, data integrity, Proof of Exponentiation of Dynamic Data Possession (PoEDDP), RSA accumulators, cryptographic accumulators, cloud security, data auditing, dynamic data possession, secure cloud storage, data availability, cryptography.

I. INTRODUCTION

At the forefront of modern technology, Cloud Computing provides a vital ecosystem to streamline operations and enhance efficiency across diverse industries. The Everything as-service (XaaS) model ranging from

Infrastructure-as-a- Service to Function-as-a-Service, has become an integral component of the contemporary innovative business landscape [1], [2]. This model features cost-effectiveness, agility, and scalability. Cloud storage accepts a massive amount of data at a rate of terabytes per second, driven by the ease of accessibility, effortless programmability, and seamless integration of various components with cloud platforms, especially from the rapidly growing market of connected resource-restricted devices [3]. However, data integrity is a major concern for adopters when outsourcing data to Cloud Service Providers [4]. Many data owners (generators) cannot trust Cloud Service Providers and their associated third parties to take control of their outsourced data without any guarantees, especially for governments and classified security agencies.

In this paradigm of delegating personal and organizational private data, extensive research has been deployed to secure each component of the cloud ecosystem. Provable Data Possession (PDP) and Proof of Retrievability (PoR) constitute the main integrity verification mechanisms used in this regard. Both mechanisms can be implemented in a deterministic or probabilistic mode. PDP ensures that the data owner can efficiently, periodically, and securely verify the integrity of outsourced data. On the other hand, PoR focuses on proving that the data can be efficiently retrieved from the cloud. While the deterministic mode in both mechanisms ensures total correctness, the probabilistic one only checks the partial correctness of the outsourced data. In scenarios where absolute data integrity is critical, probabilistic methods may fall short of providing the level of assurance required.

They introduce an element of uncertainty, making them less robust compared to deterministic ones. Practically, the Merkle Hash Tree is the most used structure to handle the proof of dynamic data possession [5]. It constitutes a Tree-based cryptographic one-way accumulator used to commit to a set of dynamic data blocks distributed over the Merkle Tree leaves. Nevertheless, as the generated data scales from moderate to very large, the efficiency of Merkle Hash Trees becomes a pressing concern [6]. In response to this challenge, group-based accumulators [7], an alternative cryptographic structure, have gained traction for efficient data handling and their support for fast batch verification [8]. Recently, [9] leveraged group-based accumulators for deterministic integrity check-only in the cloud storage. It proposes a new BlockGen algorithm, using a

technique to avoid primality tests and collisions. However, the scheme introduces high computation overhead when performing large integer multiplication and modular exponentiation, using the generated blocks.

To address the partial correctness of the probabilistic PDP, the efficiency problem of, using Merkle Hash Tree, and the drawbacks of the deterministic PDP scheme [9], we propose a deterministic proof of data possession scheme, using RSA accumulators. Our scheme exploits Proof of Exponentiation and safe under a new stronger security assumption, called the Adaptive Root assumption [10]. Unlike [9], our Block Gen algorithm significantly reduces the computation overhead by reducing the size of the generated blocks used in large integer multiplication. As a consequence, it reduces the communication and storage overhead. Therefore, the scheme is considered to be fast and efficient.

It supports data integrity verification characteristics, blockless verification, unrestricted challenge frequency, dynamic data handling, and public auditability. This scheme is secured against different data attacks such as tag forgery attacks, data leakage attacks, replace attacks, replay attacks, and pollution attacks. It can also be deployed on a trusted or untrusted environment in which we regard the accumulator manager's existence or absence.

II. RELATED WORK

A. Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure

The exponential growth of the Internet of Things (IoT) technologies requires high data security. Here, data security is very critical as all IoT devices transfer data over the Internet. The fine-grained access control provided by the ciphertext policy attribute-based encryption (CP-ABE) technique can be considered as a potential solution to this issue. However, most of the CP-ABE schemes use bilinear pairing operations for its internal working, which is expensive for any resource constraint device. An elliptic curve cryptography (ECC) based CP-ABE scheme can be well suited for resource constraint IoT framework because ECC takes less computational time. This article proposes a novel CP-ABE technique based on ECC to achieve fine-grained access control over data or resources. The proposed technique includes multiple attribute authorities to manage attributes and key generation, which can reduce the work overhead of having a single authority in

traditional CP-ABE systems. In addition, the proposed scheme outsources the decryption process to a user assistant entity to reduce the decryption overhead of the end-users. To prove the efficiency of the proposed scheme, both formal security analysis and performance comparisons are presented in this article. The result and findings prove the effectiveness of the proposed scheme over some well-known schemes.

B. *Extracting spatial information of IoT device events for smart home safety monitoring*

Smart home IoT devices have been widely deployed and connected to many home networks for various applications such as intelligent home automation, connected healthcare, and security surveillance. The network traffic traces generated by IoT devices have enabled recent research advances in smart home network measurement. However, due to the cloud-based communication model of smart home IoT devices and the lack of traffic data collected at the cloud end, little effort has been devoted to extracting the spatial information of IoT device events to determine where a device event is triggered. In this paper, we examine why extracting IoT device events' spatial information is challenging by analyzing the communication model of the smart home IoT system. We propose a system named IoTDuet for determining whether a device event is triggered locally or remotely by utilizing the fact that the controlling devices such as smartphones and tablets always communicate with cloud servers with relatively stable domain name information when issuing commands from the home network. We further show the importance of extracting spatial information of IoT device events by exploring its applications in smart home safety monitoring.

C. *Verifiable outsourced attribute-based encryption scheme for cloud-assisted mobile e-health system*

The cloud-assisted mobile electronic health (e-health) system facilitates e-health data sharing between healthcare providers and patients, but also raises the security and privacy concerns of e-health data. Although Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has been a promising technique to achieve fine-grained access control over encrypted e-health data, it still incurs high encryption and decryption burdens on mobile users such as smartphones and sensors. In addition, malicious cloud servers may conduct incorrect operations due to various interest incentives (e.g., leaking sensitive information to illegal users, saving

computation and storage costs). To solve the above issues, in this paper we first propose an Outsourced CP-ABE (OABE) with verifiable encryption scheme by splitting secret keys corresponding to an attribute set and using the short signature, which not only reduces the encryption and decryption complexities of mobile users but also guarantees that cloud servers correctly perform encryption operations. Then, we extend OABE to construct outsourced CP-ABE with verifiable decryption (OABE+) by utilizing the verifiable tag mechanism, which guarantees that cloud servers correctly conduct the ciphertext transformation. Formal security analysis proves that our schemes are selectively secure against unauthorized accesses and malicious operations. Extensive experiments using various real-world datasets demonstrate that our schemes are efficient and feasible in real applications.

D. Puncturable ciphertext-policy attribute-based encryption scheme for efficient and flexible user revocation

Cloud computing, which provides a brand-new service model, has become an important infrastructure in the information age, and has been widely used in numerous fields. The Key-Policy Attribute-Based Encryption (KP-ABE) scheme allows the encrypted data with fine-grained access control in the cloud environment. However, achieving large-scale user revocation in the application scenario of KP-ABE becomes one of the thorny problems. Furthermore, the computation and communication costs of the previous user revocation schemes were generally high, especially when a large number of users were revoked. To address these problems, an enhanced high-performance user-revocable KP-ABE scheme combined with the puncture method was proposed. In this article, the user could be revoked by the fine-grained restriction policy. When revoking the user, the cloud would run the puncture algorithm to embed the restriction policy defined by the data owner into the ciphertext. This method could effectively omit the re-encryption and key updating processes, by which the computation and communication overhead of the user revocation are efficiently reduced, and the user revocation becomes more flexible and efficient. Moreover, the Chosen-Plaintext Attack (CPA) security proof and extensive simulation results demonstrate the reliability and efficiency of the proposed scheme for user revocation in a cloud environment.

III. PROPOSED METHODOLOGY

This paper proposes a secure scheme, called Proof of Exponentiation of Dynamic Data Possession PoEDDP based on RSA-

Accumulators. RSA-based homomorphic hash function scheme proposed to overcome the aforementioned. This scheme supports queries but lacks the support of dynamic data. as well as induces high computation costs.

In contrast, our proposed scheme encrypts each, it with the corresponding tag, and then applies. While this step a requires additional processing time, we gain in terms of performance and efficiency.

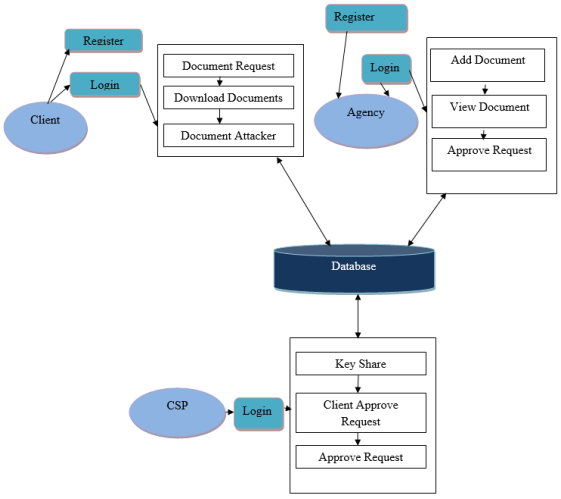
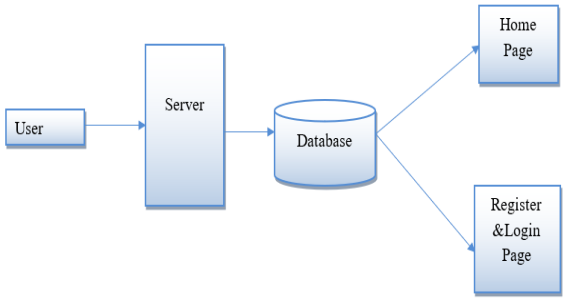


Fig. 1: System Overview

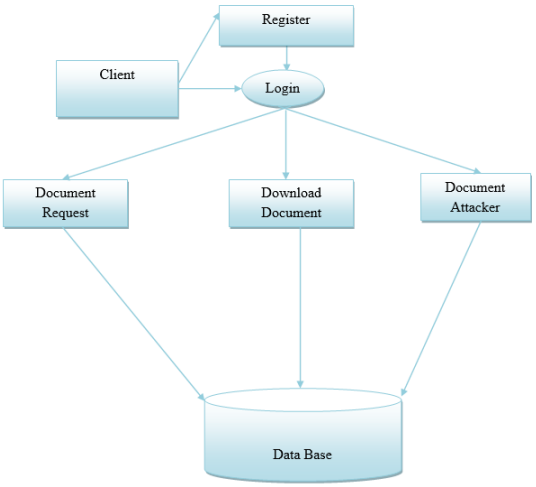
1. User Interface Design

In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.



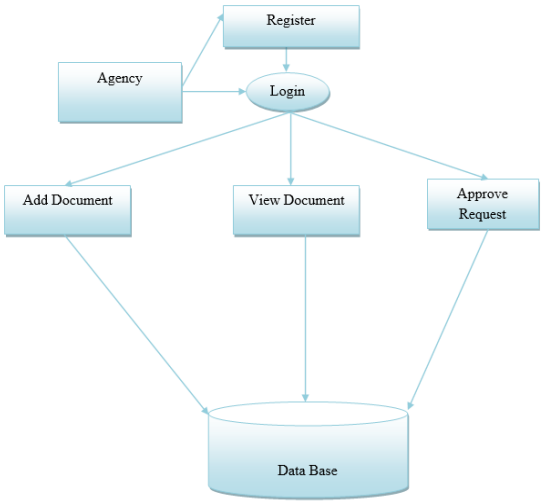
2. Client

The client has a register and then login. Client has a document request to a agency. The agency will get a request and then the download a document. The client has got a document attacker to attack a file.



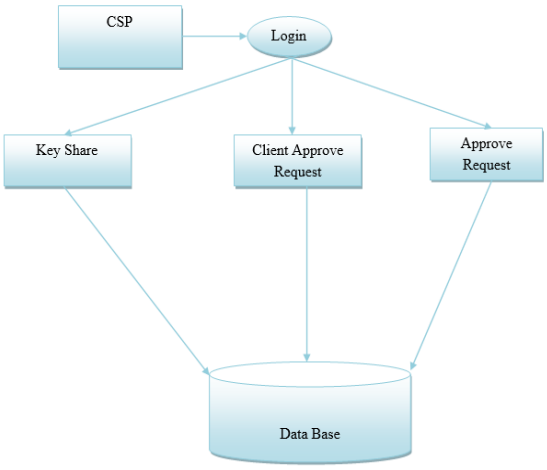
3. Agency

The agency has a register and login with a details. The agency after login a add a document. The document has a stores in a database. The agency has a view uploaded a document. The agency has a approve a request to a share a document to a client.



4. CSP

The CSP has a login with a user id and password. The CSP has a key share to a clients. The CSP has a client approve a request. The CSP has a approve a request to a database. The CSP has a approve request to the data.



IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed PoEDDP scheme provides efficient and secure data integrity verification for cloud storage using RSA-based cryptographic accumulators. The proof-of-concept demonstrates that PoEDDP is approximately 20 times faster than existing RSA accumulator-based approaches while maintaining secure dynamic data possession verification. The scheme is particularly suitable for resource-constrained users without affecting cloud service provider performance.

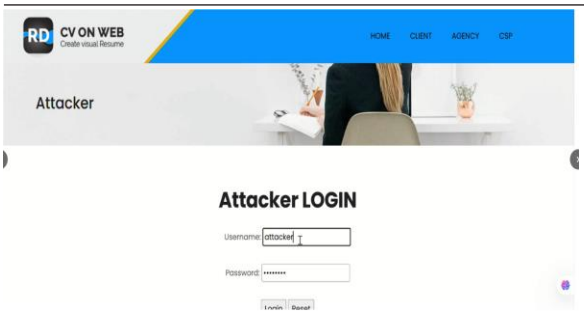


Fig. 2: Attacker Login



Fig. 3: CSP Login

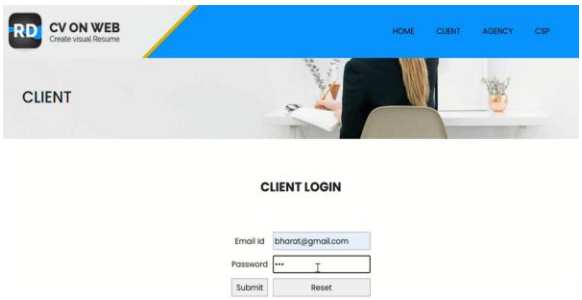


Fig. 4: Client Login

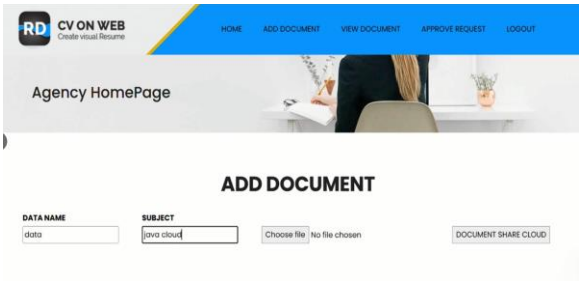


Fig. 5: Add Document

V. CONCLUSION

We introduce PoEDDP, a member of the Proof of Data Possession (PDP) family is implemented, using a variant of RSA-Accumulators based on Proof of Exponentiation PoE. The scheme allows data owners to continuously audit the integrity and availability of the outsourced data. The audit guarantees that the CSP deterministically uses the stored data to compute the proof of data possession. This proof is then verified against a single accumulated value αt computed from small footprints of tags stored in HPM. Additionally, the scheme offers dynamic capabilities to execute various operations on the outsourced data, including additions, updates, and deletions within the CSP′*s* end. Comparatively, our scheme significantly outperforms Khadr's scheme To provide a practical example, our proof generation phase, conducted on a dataset of 100k blocks, each consisting of 416 bytes, requires a mere. In contrast, Khadr's scheme takes under the same conditions.

REFERENCES

[1] Public Cloud Infrastructure Spending Worldwide 2015–2026, Statista, Hamburg, Germany, 2017.

[2] Cloud Computing Market Size & Share | Growth Analysis,

Fortunebusinessinsights, Maharashtra, India, 2030.

[3] Number of Connected IoT Devices Growing 9% to 12.3 Billion Globally, Cellular IoT Now Surpassing 2 Billion, IoT.Business.News, Paris, France, Sep. 2021.

[4] F. Zafar, A. Khan, S. U. R. Malik, M. Ahmed, A. Anjum, M. I. Khan, N. Javed, M. Alam, and F. Jamil, ‘‘A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends,’’ Comput. Secur., vol. 65, pp. 29–49, Mar. 2017.

[5] R. C. Merkle, ‘‘A digital signature based on a conventional encryption function,’’ in Advances in Cryptology—CRYPTO ’87, Santa Barbara, CA, USA. Cham, Switzerland: Springer, Aug. 1987, pp. 369–378.

[6] A. Ozdemir, R. S. Wahby, B. Whitehat, and D. Boneh, ‘‘Scaling verifiable computation using efficient set accumulators,’’ in Proc. 29th USENIX Conf. Secur. Symp., 2020, Paper 117. [Online]. Available: https://dl.acm.org/doi/proceedings/10.5555/3489212

[7] J. Camenisch and A. Lysyanskaya, ‘‘Dynamic accumulators and application to efficient revocation of anonymous credentials,’’ in Proc. Annu. Cryptol.-CRYPTO Annu. Int. Cryptol. Conf. Santa Barbara, CA, USA: Springer, Aug. 2002, pp. 61–76.

[8] D. Boneh, B. Bünz, and B. Fisch, ‘‘Batching techniques for accumulators with applications to IOPs and stateless blockchains,’’ in Advances in Cryptology—CRYPTO 2019, vol. 11692. Cham, Switzerland: Springer, 2019, pp. 561–586.

[9] W. I. Khedr, H. M. Khater, and E. R. Mohamed, ‘‘Cryptographic accumulator-based scheme for critical data integrity verification in cloud storage,’’ IEEE Access, vol. 7, pp. 65635–65651, 2019.

[10] B. Wesolowski, ‘‘Efficient verifiable delay functions,’’ in Advances in Cryptology—EUROCRYPT 2019. Cham, Switzerland: Springer, 2019, pp. 379–407.

AUTHORS Profile



Mrs. E. MOUNIKA REDDY has received her B.Tech from JNTUH, Hyderabad in 2015, M.Tech degree in

Computer science from JNTUH, Hyderabad in 2017. She is dedicated to teaching field from the last 8 years. At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Mr. BANDARU BHARATH KUMAR REDDY pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. DILLI PAVAN KALYAN pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr.JOGINI PREMSAI pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. KUMMARIKUNTA VARSHITH KRISHNA pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.