GURU NANAK INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering

PoEDDP-A Fast RSA-Based Proof of Possession Accumulator of Dynamic Data on the Cloud

UNDER THE GUIDANCE OF

Mr. D.Srinivas

ASSISTANT PROFESSOR

TEAM MEMBERS

ADKI SAI VINAY - 21831A0504

BHUPALAM LAKSHMI ROHIT - 21831A0524

BUDDE RACHANA - 21831A0529

ABSTRACT

A Fast RSA-Based Proof of Possession Accumulator of Dynamic Data on the Cloud

Cloud computing offers convenient and scalable storage solutions, but ensuring the integrity and security of outsourced data remains a challenge.

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.

INTRODUCTION

- Cloud computing enables scalable and efficient data storage, reducing costs and operational complexities.
- Data integrity verification is crucial for security and trust, ensuring that stored information remains untampered.
- Traditional methods like Merkle Hash Trees (MHT) and Provable Data Possession (PDP) struggle with efficiently handling large-scale dynamic data.
- A robust and efficient proof mechanism is needed to address these concerns and prevent unauthorized data modification.

LITERATURE SURVEY

S.No	Title of the Project	Description
1	An Efficient Dynamic and Distributed RSA Accumulator Michael T. Goodrich, Roberto Tamassia, Jasminka Hasic (2018)	Introduced an RSA-based accumulator enabling efficient updates (add, delete, modify) without full recomputation. Proposed a distributed model to reduce single points of failure. Enables near-instant element verification without scanning the whole dataset. Supports zero-knowledge proof allowing third-party audits without revealing data.
2	Cryptographic Accumulator-Based Scheme for Critical Data Integrity Verification in Cloud Storage Kui Ren, Cong Wang, Qian Wang (2019)	Proposed an RSA-based data integrity verification system (CAPDP Scheme) outperforming traditional PDP schemes. Allows third-party verification without downloading full data, saving bandwidth. Defends against replay, tag forgery, and data pollution attacks. Utilizes RSA accumulators to reduce storage and computation. Outperforms MHT-based schemes by minimizing proof generation time and rehashing.
3	Privacy-Preserving Public Auditing for Secure Cloud StorageCong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, Wenjing Lou (2010)	Introduced a TPA (Third Party Auditor) system for cloud storage using homomorphic authenticators and random masking. Ensures privacy-preserving auditing without revealing data content. Reduces burden on cloud servers, supports batch auditing. Efficient and scalable, suitable for large-scale cloud environments.

EXISTING SYSTEM

Ind-cca requirement of the cipher

- Deducing information about the cipher text, even a minor bit, puts the client's data in a critical situation. To ensure data confidentiality, even from a very secure CSP by any adversary A who could mount active attacks against the cipher text .
- This existing system is used in subsequent checks to verify that a block or a set of blocks of the original data indeed still exists. This satisfies a vital security property called binding.
- Which indirectly means that a malicious program cannot produce two or more valid openings once it commits to a set of data.
- As a consequence, it reduces the communication and storage overhead.
- Disadvantages are it is poor in data integrity verification, unrestricted dynamic data handling and public audit ability.

PROPOSED SYSTEM

- Our System proposes a secure scheme, called Proof of Exponentiation of Dynamic Data Possession PoEDDP based on RSA-Accumulators along with SHA algorithm.

- A cryptographic(RSA) accumulator is a mathematical construct that allows one to "accumulate" a set of values such that you can later prove that a specific value is part of that set without revealing the entire set. RSA-based accumulators utilize the properties of RSA, which is based on the difficulty of factoring large prime numbers.

- **Key Features of RSA-based Accumulators:-**

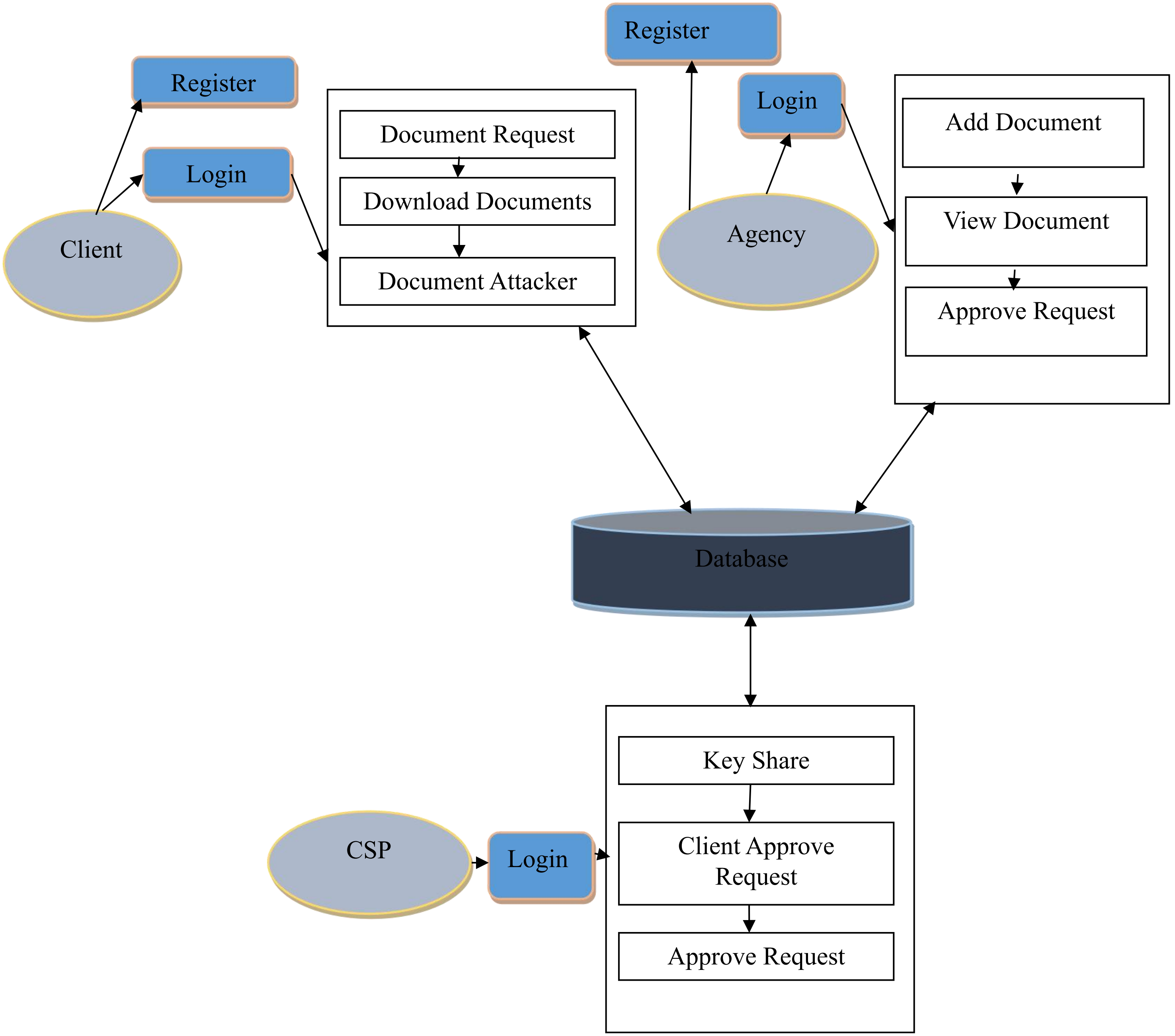
  1. Accumulation: Given a set of values, the accumulator generates a single value (the accumulator value) that represents all the values in the set.

  2. Membership Proof: For any value in the set, one can generate a proof that this value is included in the accumulator without revealing the other values.

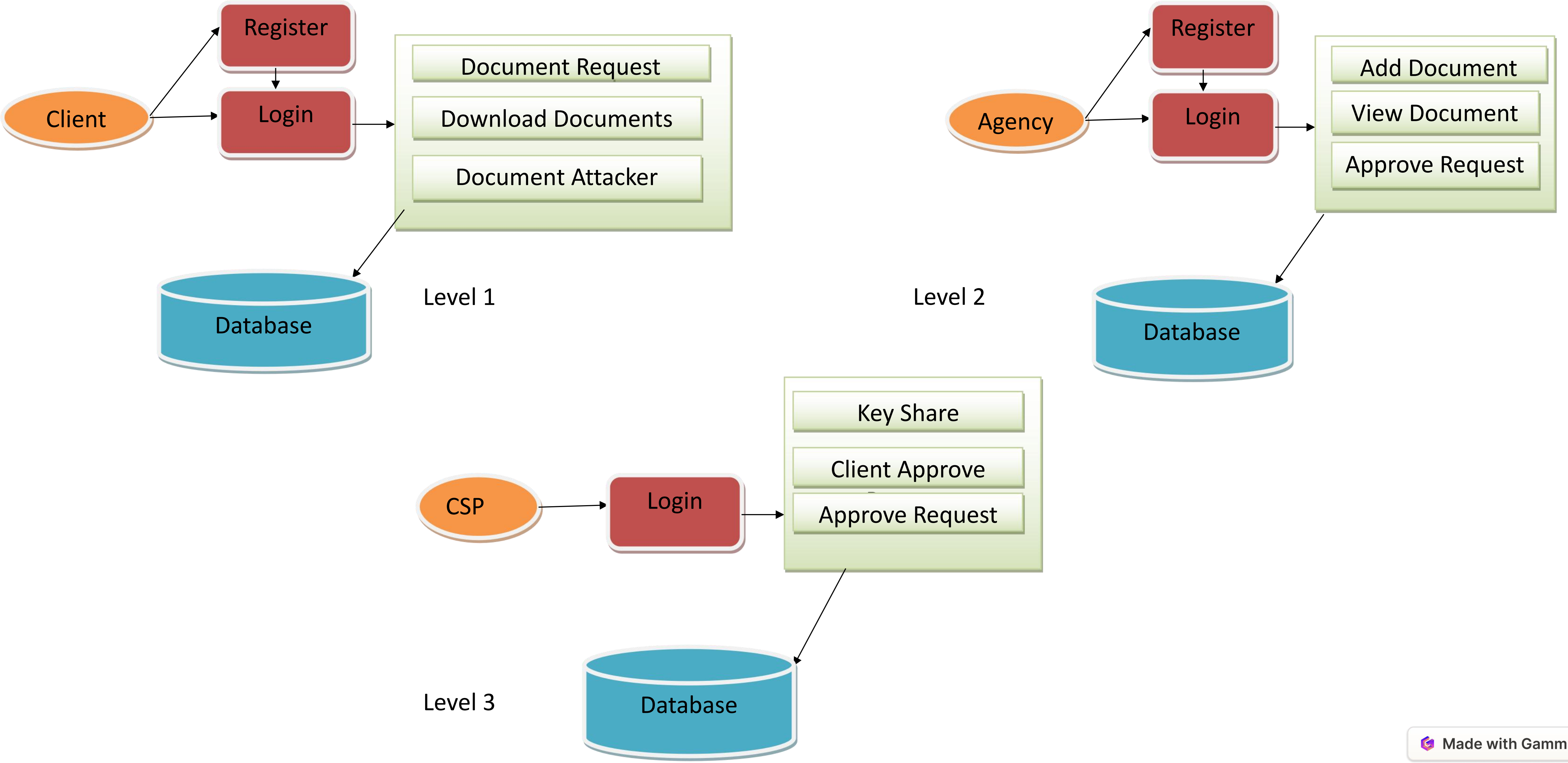
  3. Non-repudiation: The accumulator can be used to prove that a certain value was included at a certain time.

  4. Efficiency: The size of the accumulator does not grow significantly with the number of values added.

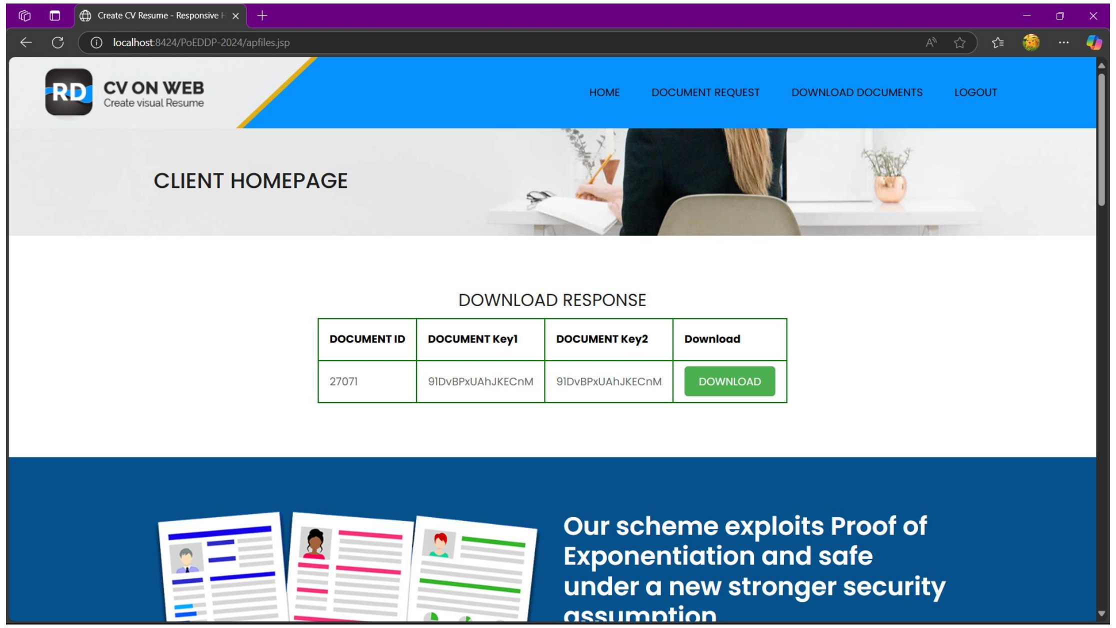
SYSTEM ARCHITECTURE



DATA FLOW DIAGRAM



RESULTS AND DISCUSSIONS

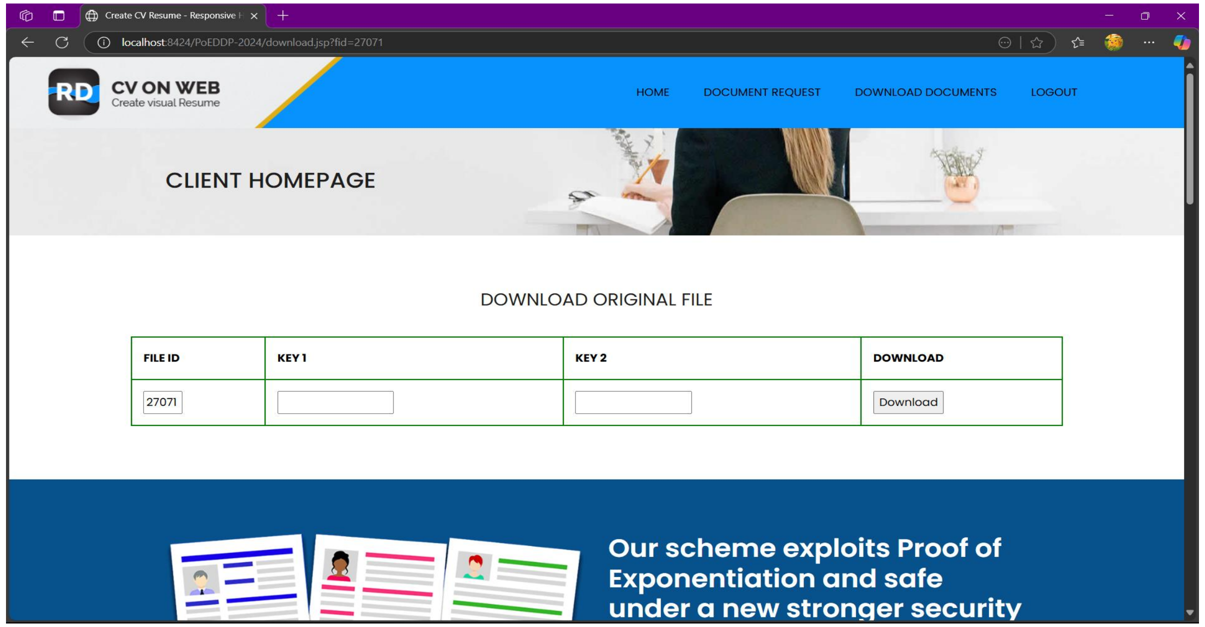


CLIENT HOMEPAGE

DOWNLOAD RESPONSE

DOCUMENT ID	DOCUMENT Key1	DOCUMENT Key2	Download
27071	91DvBPxUAhJKECnM	91DvBPxUAhJKECnM	DOWNLOAD

Our scheme exploits Proof of Exponentiation and safe under a new stronger security assumption

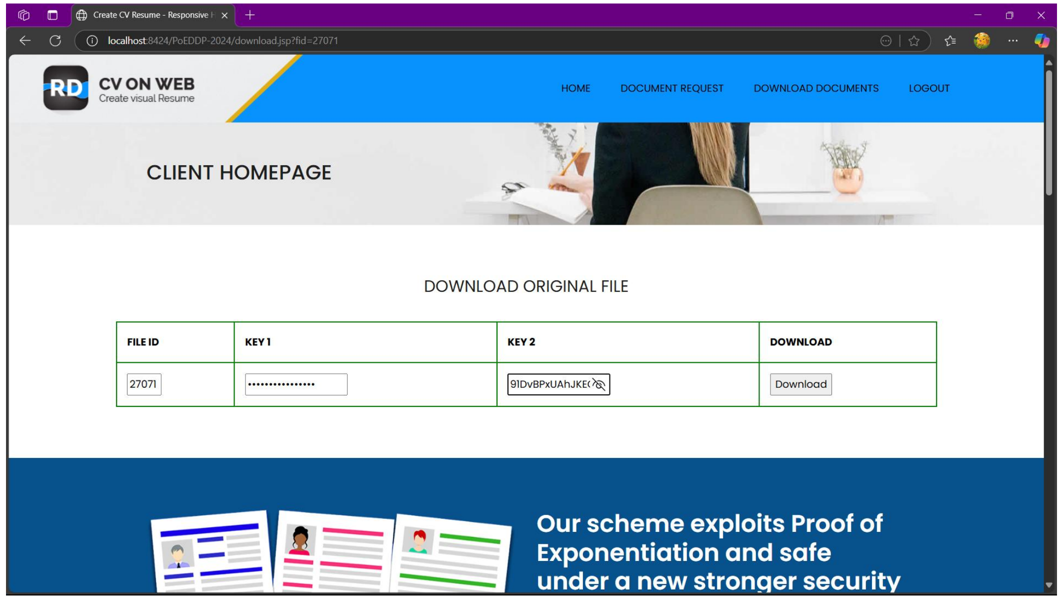

Create CV Resume - Responsive H
localhost:8424/PoEDDP-2024/download.jsp?fid=27071
RD
CV ON WEB
Create visual Resume
HOME
DOCUMENT REQUEST
DOWNLOAD DOCUMENTS
LOGOUT

CLIENT HOMEPAGE

DOWNLOAD ORIGINAL FILE

FILE ID	KEY 1	KEY 2	DOWNLOAD
27071			Download

Our scheme exploits Proof of Exponentiation and safe under a new stronger security


Create CV Resume - Responsive H
localhost:8424/PoEDDP-2024/download.jsp?fid=27071
RD
CV ON WEB
Create visual Resume
HOME
DOCUMENT REQUEST
DOWNLOAD DOCUMENTS
LOGOUT

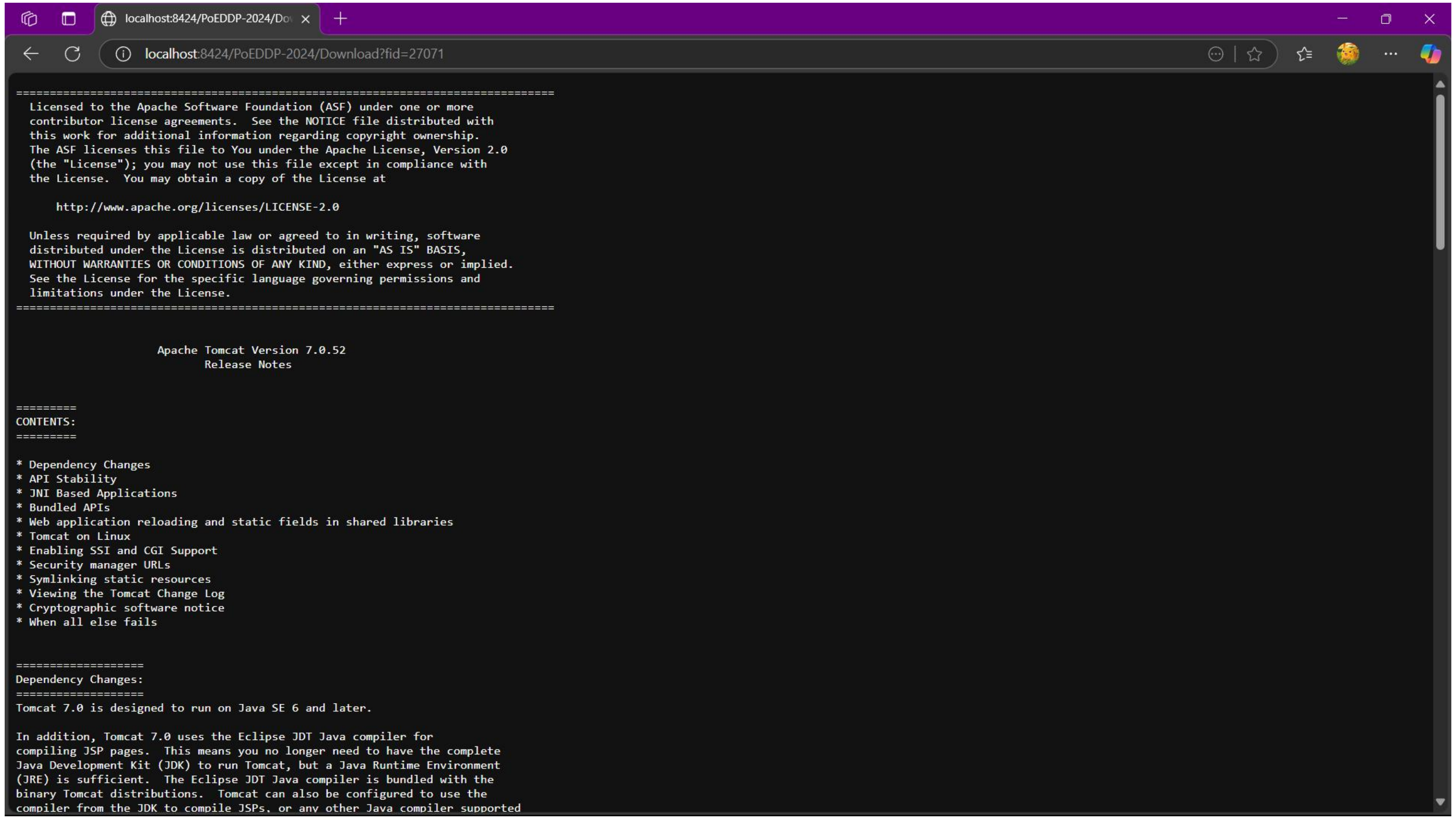
CLIENT HOMEPAGE

DOWNLOAD ORIGINAL FILE

FILE ID	KEY 1	KEY 2	DOWNLOAD
27071	••••••••••••••••	91DvBPxUAhJKE(	Download

Our scheme exploits Proof of Exponentiation and safe under a new stronger security

RESULTS AND DISCUSSIONS


localhost:8424/PoEDDP-2024/Do
localhost:8424/PoEDDP-2024/Download?fid=27071

```
================================================================================
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
================================================================================


                     Apache Tomcat Version 7.0.52
                            Release Notes


=========
CONTENTS:
=========

* Dependency Changes
* API Stability
* JNI Based Applications
* Bundled APIs
* Web application reloading and static fields in shared libraries
* Tomcat on Linux
* Enabling SSI and CGI Support
* Security manager URLs
* Symlinking static resources
* Viewing the Tomcat Change Log
* Cryptographic software notice
* When all else fails


===================
Dependency Changes:
===================
Tomcat 7.0 is designed to run on Java SE 6 and later.

In addition, Tomcat 7.0 uses the Eclipse JDT Java compiler for
compiling JSP pages.  This means you no longer need to have the complete
Java Development Kit (JDK) to run Tomcat, but a Java Runtime Environment
(JRE) is sufficient.  The Eclipse JDT Java compiler is bundled with the
binary Tomcat distributions.  Tomcat can also be configured to use the
compiler from the JDK to compile JSPs, or any other Java compiler supported
```

CONCLUSION

- PoEDDP is a revolutionary approach to cloud data security, offering efficiency, robustness, and flexibility.
- It enhances cloud storage reliability by providing secure, scalable, and verifiable data integrity mechanisms.
- The scheme benefits enterprises, government agencies, and individuals outsourcing sensitive data.

FUTURE ENHANCEMENTS

- Future enhancements may involve optimizing computational efficiency and integrating blockchain technology for further security advancements.

REFERENCES

- 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.
- 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.
- 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.
- W. Guo, H. Zhang, S. Qin, F. Gao, Z. Jin, W. Li, and Q. Wen, “Outsourced dynamic provable data possession with batch update for secure cloud storage,” Future Gener. Comput. Syst., vol. 95, pp. 309–322, Jun. 2019.

THANK YOU