SECURE PASSWORD-PROTECTED ENCRYPTION KEY FOR DEDUPLICATED CLOUD STORAGE SYSTEM

K.LAKSHANA[1], Dr.S.SAJITHA BANU[2], K.RAMYA[3], M.SABARI RAMACHANDRAN[4]

1, Student, Department of Master of Computer Application. Mohamed Sathak Engineering College.
Ramanathapuram, India.
2, Assistant Professor, Department of Master of Computer Application, Mohamed Sathak Engineering College.
Ramanathapuram, India.
3, Assistant Professor, Department of Master of Computer Application, Mohamed Sathak Engineering College.
Ramanathapuram, India.
4, Assistant Professor, Department of Master of Computer Application, Mohamed Sathak Engineering College.
Ramanathapuram, India.

ABSTRACT

In this project, I propose SPADE, an encrypted data deduplication scheme that resists compromised key servers and frees users from the key management problem. Specifically, we propose a proactivization mechanism for the servers-aided message-locked encryption (MLE) to periodically substitute key servers with newly employed ones, which renews the security protection and retains encrypted data deduplication. We present a servers-aided password-hardening protocol to resist dictionary guessing attacks. Based on the protocol, we further propose a password-based layered encryption mechanism and a password-based authentication mechanism and integrate them into SPADE to enable users to access their data only using their passwords. Provable security and high efficiency of SPADE are demonstrated by comprehensive analyses and experimental evaluations.

INTRODUCTION

In the big data era, the volume of digital data increases explosively. A recent report1 indicates that the data we create and copy are doubling in size every two years, and will reach 175 zettabytes by 2025. As the amount of data has increased exponentially, users suffer from critical problems in data management [2], [3], [4]. With the significant development of cloud storage, people are increasingly outsourcing their data to cloud servers, which enables them to efficiently manage their data without deploying infrastructures and maintaining local devices [5], [6]. Commercial cloud service providers always perform data deduplication across their users to save storage space significantly. Recent literature [7], [8] has demonstrated that such a strategy can save space by more than 65% in electronic health systems and 90% in backup systems. While storage costs can be reduced by data deduplication, the outsourced data are confronted with critical security issues. the encryption (i.e., different users would One of the most important concerns is data confidentiality [9], [10], [11]. From the data owners' perspective, the contents of outsourced data may contain their privacy information [12], [13]. As such, the data are always encrypted by using conventional encryption algorithms before outsourc- Y ing. However, because of the randomness of output different ciphertexts for the same data), deduplication is impeded. Message-locked encryption (MLE) is a special type of symmetric encryption, in which the MLE key (i.e., the encryption and decryption key) is derived from the plaintext itself [14], [15]. This enables different users to output the same ciphertext for the same plaintext and allows the cloud server to perform deduplication over encrypted data across all its users.

PROJECT DESCRIPTION

In the big data era, the volume of digital data increases explosively. A recent report1 indicates that the data we create and copy are doubling in size every two years, and will reach 175 zettabytes by . As the amount of data has increased exponentially, users suffer from critical problems in data management. With the significant development of cloud storage, people are increasingly outsourcing their data to cloud servers, which enables them to efficiently manage their data without deploying infrastructures and maintaining local devices. Commercial cloud service providers always perform data deduplication across their users to save storage space significantly. Recent literature, has demonstrated that such a strategy can save space by more than 65% in electronic health systems and 90% in backup systems. While storage costs can be reduced by data deduplication, the outsourced data are confronted with critical security.

System Testing

Software testing is an important element of software quality assurance and represents the ultimate review of specification, design and coding. It increasing visibility of software as a system element and the costs associates with a software failure are motivating forces for all well planned through testing .The system is tested with giving wrong information. Cascade deletion and, the software developer checks updating. Testing and debugging are different activities, but debugging must be accommodated in any testing strategy.

TYPES OF TESTING

Unit testing

The first step in testing is Unit testing. Individual testing are tested to ensure that they operate correctly. Each component is tested independently, without other system components. The module interface is tested to ensure that information properly flow into and out of the program.These are tested that the module operates at boundary established to limit or restrict processing. Unit testing is normally considered as an adjunct to the coding step. After the coding has been developed, received and verified for correct syntax, unit testing begins. Here each module is tested to provide its correctness, validity and determine any missing operations and to verify whether the objectives have been met, errors are noted down and corrected immediately.

Integration testing

The second step in the testing process is the Integration testing. Integration testing is the systematic technique for constructing the program structure while conducting tests to uncover errors associated with integrating. After the unit test, each module is gradually integrated to form one final system.

Performance testing

A type of Physical test covering a wide range of engineering or functional evaluations where a material, product, or system is not specified by detailed material or component specifications: rather, emphasis is on the final measurable performance characteristics. Testing can be a qualitative or quantitative procedure.

Acceptance testing

The types of acceptance testing are:

- The User Acceptance test: focuses mainly on the functionality thereby validating the fitness-for-use of the system by the business user. The user acceptance test is performed by the users and application managers.

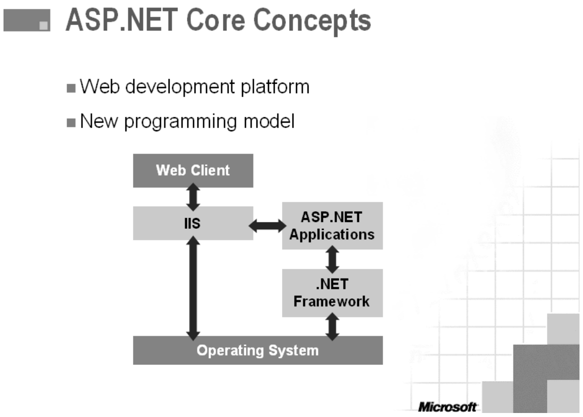
- The Operational Acceptance test: also known as Production acceptance test validates whether the system meets the requirements for operation. In most of the organization the operational acceptance test is performed by the system administration before the system is released. The operational acceptance test may include testing of backup/restore, disaster recovery, maintenance tasks and periodic check of security vulnerabilities

- Contract Acceptance testing: It is performed against the contract's acceptance criteria for producing custom developed software.

SYSTEM DESIGN

SYSTEM ARCHITECTURE

In this section you will get an overview of the .NET Framework architecture, the Web application model, and the configuration system.



ASP.NET Core Concepts

- Web development platform
- New programming model

SYSTEM IMPLEMENTATION

Implementation is used here to mean the process of converting a new or revised system design into operational one; conversion is one aspect of implementation. the other aspect is post implementation review and software and maintenance

There are three type of implementation:

- Implementation of a computer system
- Implementation of new computer system
- Implementation of a modified application

IMPLEMENTATION OF THE COMPUTER SYSTEM

It's should be replace a manual system the problems encountered are converting files, training users creating accurate files, and verifying printouts for integrity

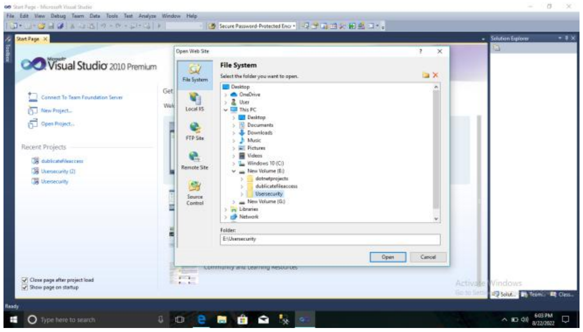
IMPLEMENTATION OF NEW COMPUTER SYSTEM

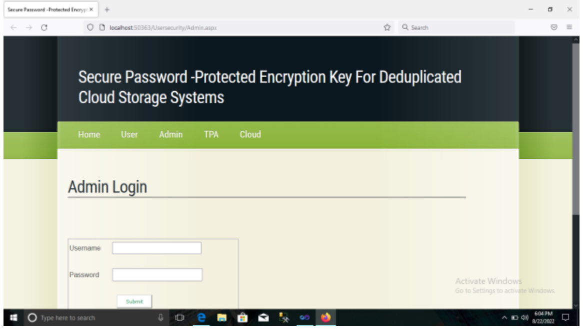
It's should be replace an existing one this is usually a difficult conversion. if not properly planned there can be many problems. Some large computer system have taken even years to convert

IMPLEMENTATION OF A MODIFIED APPLICATION

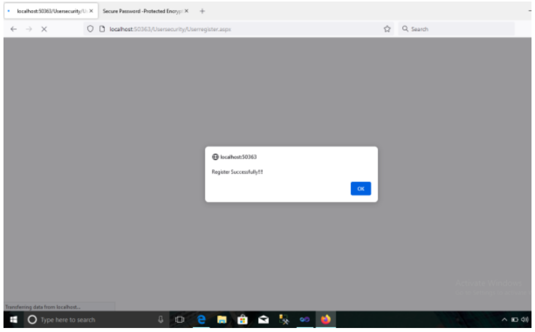
It's should be replace an existing one using the same computer. This type of conversion is relativity easy to handle, provided there are no major changes to the file.

SCREENSHOT:





Secure Password -Protected Encryp
localhost:50363/Usersecurity/Admin.aspx
Search
Secure Password -Protected Encryption Key For Deduplicated Cloud Storage Systems
Home
User
Admin
TPA
Cloud
Admin Login
Username
Password
Submit
Type here to search
6:04 PM
8/22/2022


localhost:50363/Usersecurity/U
Secure Password -Protected Encryp
localhost:50363/Usersecurity/Userregister.aspx
Search
localhost:50363
OK
Transferring data from localhost...
Type here to search

Register Successfully!!!

Conclusion

Cloud computing brings great convenience for people.Particularly; it perfectly matches the increased need of sharing data over the internet. In this paper, to build a cost effective and secure data sharing system in cloud computing.We proposed a nottion called RS-IBE,which supports identity revocation and cipher text update simultaneously such that a revoked user is prevented from accessing previously shared data as well as subsequently shared data.Futhermore,a concrete construction of RS-IBE is presented.The proposed RS-IBE scheme is proved adaptive secure in the standard model,under the decisional ℓ-DBHE assumption.Thecomparsion results demonstrate that our scheme has advantages in terms of efficiency and functionality and thus is more feasible for partical applications.

Future Enhancement

- Social Cloud ought to have low barriers for participation—and therefore vastly increase public access to computing, storage, and services

- A Social Cloud should allow overlapping groups—with members belonging to multiple groups and thereby (to a limited extent) permit the osmosis of resources across groups based on the social relationships and standing of other members

- However, the most critical characteristic is that a Social Cloud uses social relationships to ensure desirable behavior within the system

- One major area of future work is adapting the market protocols to a social context and also looking at other ways to define and exploit social incentives (and disincentives) in a resource sharing scenario

- Use in adapted scenarios

- In particular, we aim to explore system performance and user interactions on a much larger scale

REFERENCE

1. Al-Shaikhly MH, El-Bakry HM & Saleh AA 2018, ‘Cloud security using Markov chain and genetic algorithm’, International Journal of Electronics and Information Engineering, vol. 8,no. 2, pp. 96-106.
2. Belguith S, Kaaniche N, Laurent M, Jemai A & Attia R 2018, ‘Phoabe: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted iot’, Computer Networks, vol. 133, pp. 141-156.
3. Choi C, Choi J & Kim P 2014, ‘Ontology-based access control model for security policy reasoning in cloud computing’, The Journal of Supercomputing, vol. 67,no. 3, pp. 711-722.