TWO-FACTOR DATA SECURITY PROTECTION MECHANISM FOR CLOUD STORAGE SYSTEM

Dr T BHARATH KRISHNA[1], Dr A AVANI[2], Y NANCHARI[3], N ROJA[4]

[1, 2]Associate Professor, Department of Computer Science and Engineering, Anu Bose Institute of Technology For Women's,KSP Road, New Paloncha, Bhadradri Kothagudem District, Telangana (TS), 507115

[3, 4]Assistant Professor, Department of Computer Science and Engineering, Anu Bose Institute of Technology For Women's, KSP Road, New Paloncha, Bhadradri Kothagudem District, Telangana (TS), 507115

Submitted: 06-01-2025 *Accepted: 13-02-2025* *Published: 20-02-2025*

ABSTRACT- *In this paper, we propose a two-factor data security protection mechanism with factor revocability for cloud storage system. Our system allows a sender to send an encrypted message to a receiver through a cloud storage server. The sender only needs to know the identity of the receiver but no other information (such as its public key or its certificate). The receiver needs to possess two things in order to decrypt the ciphertext. The first thing is his/her secret key stored in the computer. The second thing is a unique personal security device which connects to the computer. It is impossible to decrypt the ciphertext without either piece. More importantly, once the security device is stolen or lost, this device is revoked. It cannot be used to decrypt any ciphertext. This can be done by the cloud server which will immediately execute some algorithms to change the existing ciphertext to be un-decryptable by this device. This process is completely transparent to the sender. Furthermore, the cloud server cannot decrypt any ciphertext at any time. The security and efficiency analysis show that our system is not only secure but also practical.*

1. INTRODUCTION

CLOUD storage is a model of networked storage system where data is stored in pools of storage which are generally hosted by third parties. There are many benefits to use cloud storage. The most notable is data accessibility. Data stored in the cloud can be accessed at any time from any place as long as there is network access. Storage maintenance tasks, such as purchasing additional storage capacity, can be offloaded to the responsibility of a service provider. Another advantage of cloud storage is data sharing between users.

If Alice wants to share a piece of data (e.g., a video) to Bob, it may be difficult for her to send it by email due to the size of data. Instead, Alice uploads the file to a cloud storage system so that Bob can download it at anytime. Despite its advantages, outsourcing data storage also increases the attack surface area at the same time. For example, when data is distributed, the more locations it is stored the higher risk it contains for unauthorized physical access to the data. By sharing storage and networks with many other users it is also possible for other unauthorized users to access your data.

Enhanced security protection, In a normal asymmetric encryption, there is a single secret key corresponding to a public key or an identity. The decryption of cipher text only requires this key. The key is usually stored inside either a personal computer or a trusted server, and may be protected by a password.

Objectives of the study

In this paper, we propose a two-factor data security protection mechanism with factor revocability for cloud storage system.

1) Our system allows a sender to send an encrypted message to a receiver through a cloud storage ser ver.
2) The sender only needs to know the identity of the receiver but no other information (such as its public key or its certificate).
3) The receiver needs to possess two things in order to decrypt the cipher text. The first thing is his/her secret key stored in the computer.
4) The second thing is a unique personal security device which connects to the computer. It is impossible to decrypt the cipher text without either piece.
5) This can be done by the cloud server which will immediately execute some algorithms to change the existing cipher text to be un-decrypt able by this device.
6) This process is completely transparent to the sender. Furthermore, the cloud server cannot decrypt any cipher text a t any time.
7) The security and efficiency analysis show that our system is not only secure but also practical.

2. LITERATURE SURVEY

Public Key Replacement and Universal Forgery of SCLS Scheme

In this paper, after the detailing the formal of certificate less signature scheme, we show that the Du-Wen's short certificate less signature scheme is insecure that is broken by a type-I adversary who has the ability in replacing users' public keys and accessing to the signing oracles, and also cannot resist on the universal forgery attack for any third user.

Longitude: a Privacy-preserving Location Sharing Protocol for Mobile Applications

In this paper, we propose a new location sharing protocol called Longitude that eases privacy concerns by making it possible to share a user's location data blindly and allowing the user to control who can access her location, when and to what degree of precision.

Unidirectional Chosen-Cipher text Secure Proxy Re-Encryption

In this paper, we present the first construction of unidirectional proxy re-encryption scheme with chosen cipher text security in the standard model (i.e. without relying on the random oracle idealization), which solves a problem left open at CCS'07. Our construction is efficient and requires a reasonable complexity assumption in bilinear map groups.

3. ANALYSIS

Existing System

There exists cryptographic primitive called "leakage-resilient encryption". The security of the scheme is still guaranteed if the leakage of the secret key is up to certain bits such that the knowledge of these bits does not help to recover the whole secret key. However, though using leakage resilient primitive can safeguard the leakage of certain bits, there exists another practical limitation. Suppose we put part of the secret key into the security device. Unfortunately the device is stolen. The user needs to obtain a replacement device so that he can continue to decrypt his corresponding secret key. The trivial way is to copy the same bits (as in the stolen device) to the new device by the private key generator (PKG). This approach can be easily achieved. Nevertheless, there exists security risk. If the adversary (who has stolen the security device) can also break into the computer where the other part of secret key is stored, then it can decrypt all cipher text corresponding to the victim user. The most secure way is to cease the validity of the stolen security device.

Proposed System

In this paper, we propose a novel two-factor security protection mechanism for data stored in the cloud. Our mechanism provides the following nice features: 1) Our system is an IBE (Identity-based encryption)- based mechanism. That is, the sender only needs to know the identity of the receiver in order to send an encrypted data (cipher text) to him/her. No other information of the receiver (e.g., public key, certificate etc.) is required. Then the sender sends the cipher text to the cloud where the receiver can download it at anytime. 2) Our system provides two-factor data encryption protection. In order to decrypt the data stored in the cloud, the user needs to possess two things. First, the user needs to have his/her secret key which is stored in the computer. Second, the user needs to have a unique personal security device which will be used to connect to the computer (e.g., USB, Bluetooth and NFC). It is impossible to decrypt the cipher text without either piece. 3) More importantly, our system, for the first time, provides security device (one of the factors) revocability. Once the security device is stolen or reported as lost, this device is revoked. That is, using this device can no longer decrypt any cipher text (corresponding to the user) in any circumstance. The cloud will immediately execute some algorithms to change the existing cipher text to beun-decryptableby this device. While, the user needs to use his new/replacement device (together with his secret key) to decrypt his/her cipher text; this process is completely transparent to the sender.

External Interface Requirements

User Interface

The user interface of this system is a user friendly Java Graphical User Interface.

Hardware Interfaces

The interaction between the user and the console is achieved through Java capabilities.

Software Interfaces

The required software is JAVA1.6.

Operating Environmen

Windows XP, Linux.

Hardware configuration

- ➢ Processor - Pentium –IV
- ➢ Speed - 1.1 Ghz
- ➢ RAM - 256 MB(min)
- ➢ Hard Disk - 20 GB
- ➢ Key Board - Standard Windows Keyboard
- ➢ Mouse - Two or Three Button Mouse
- ➢ Monitor - SVGA

Software configuration

- ❖ Operating System : Windows XP
- ❖ Programming Language : JAVA

4. SOFTWARE USED

Initially the language was called as “oak” but it was renamed as “java” in 1995.The primary motivation of this language was the need for a platform-independent (i.e. architecture neutral)language that could be used to create software to be embedded in various consumer electronic devices.

- Java is a programmer's language
- Java is cohesive and consistent
- Except for those constraint imposed by the Internet environment. Java gives the programmer, full control

Finally Java is to Internet Programming where c was to System Programming.

Importance of Java to the Internet

Java has had a profound effect on the Internet. This is because; java expands the Universe of objects that can move about freely in Cyberspace. In a network, two categories of objects are transmitted between the server and the personal computer. They are passive information and Dynamic active programs. in the areas of Security and probability. But Java addresses these concerns and by doing so, has opened the door to an exciting new form of program called the Applet.

Applications and applets

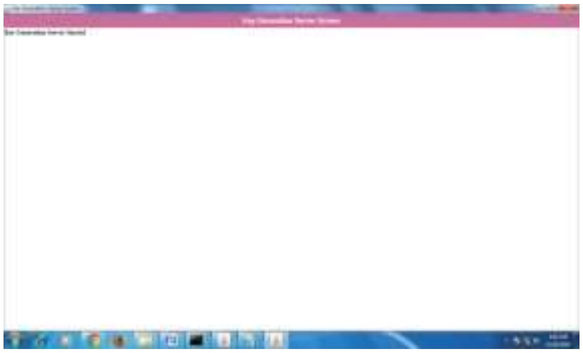
An application is a program that runs on our Computer under the operating system of that computer. It is more or less like one creating using C or C++ .Java's ability to create Applets makes it important. An Applet I san application, designed to be transmitted over the Internet and executed by a Java-compatible web browser. An applet I actually a tiny Java program, dynamically downloaded across the network, just like an image. But the difference is, it is an intelligent program, not just a media file. It can be react to the user input and dynamically change.

5. RESULTS AND ANALYSIS

Cloud server screen:

Keys application:

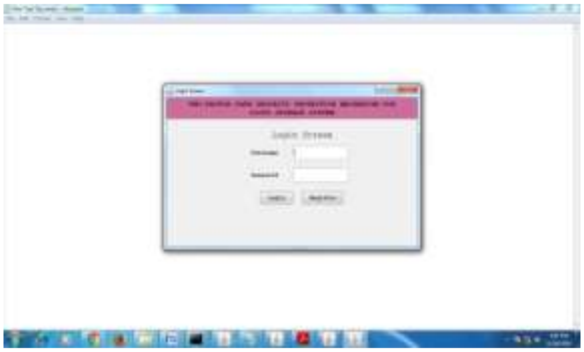
(The first factor is his/her secret key stored in the computer)



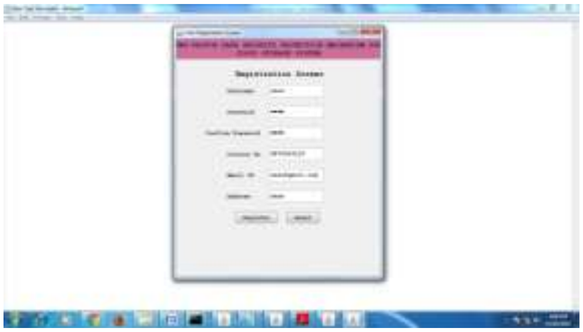
USB application:

(The second factor is a unique personal security device which connects to the computer)

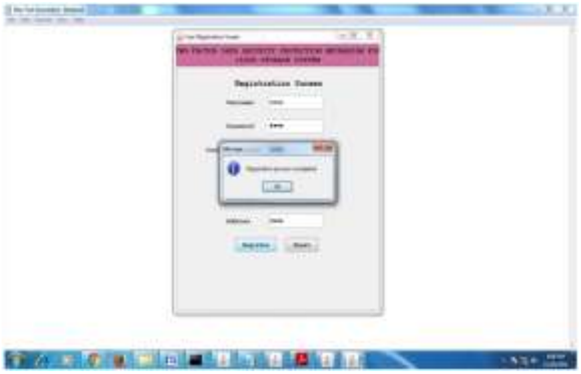
User application:



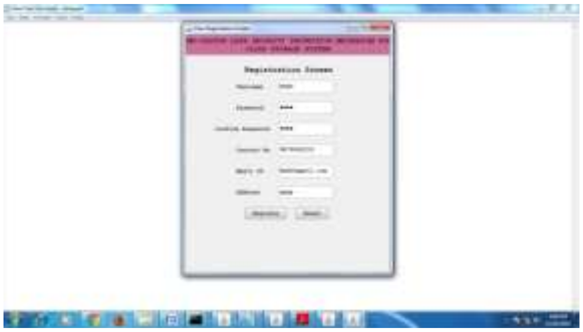
Click on register to register a new user:

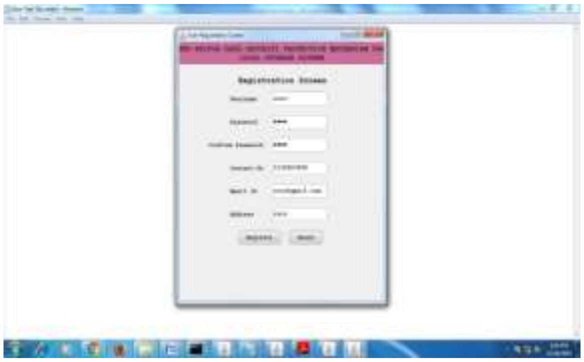


After successful registration:

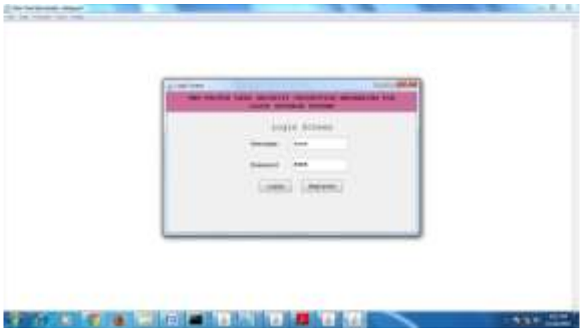


Similarly registering 2 more users:

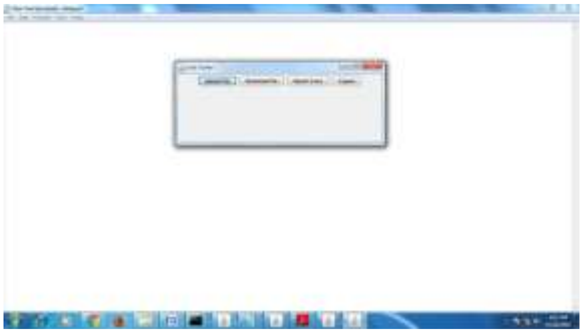




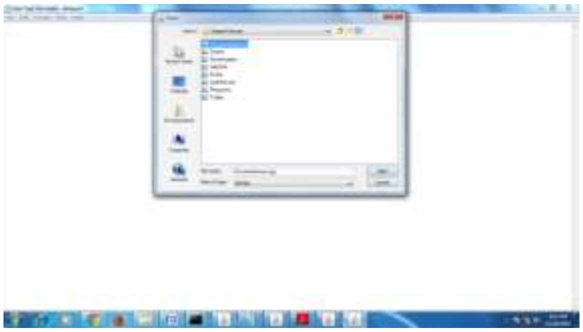
Login as a registered user:



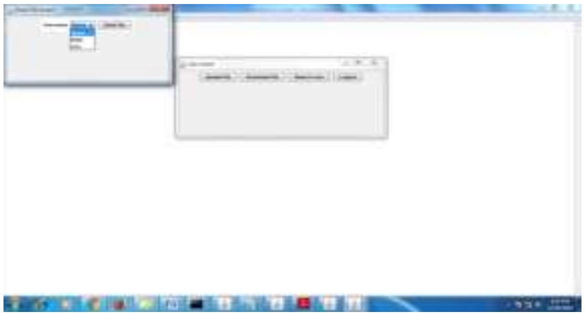
User home screen:



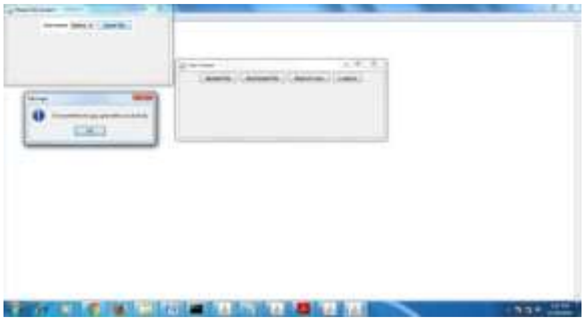
Click on upload file button, to upload the files on to cloud server:



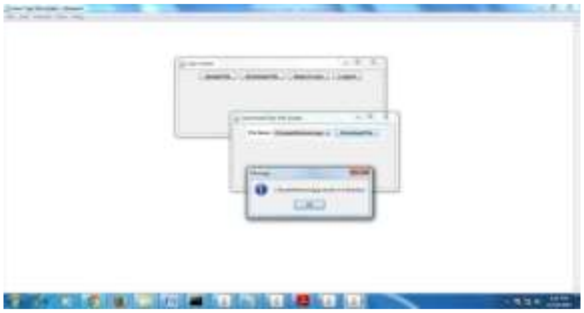
While uploading the data onto cloud, we can create the access policy for users:



After successfully uploading the file onto cloud:

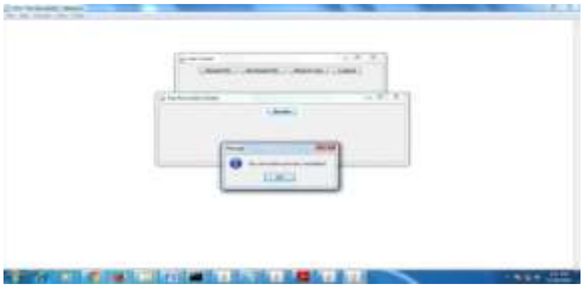


The owner can download the data, click on download file button:

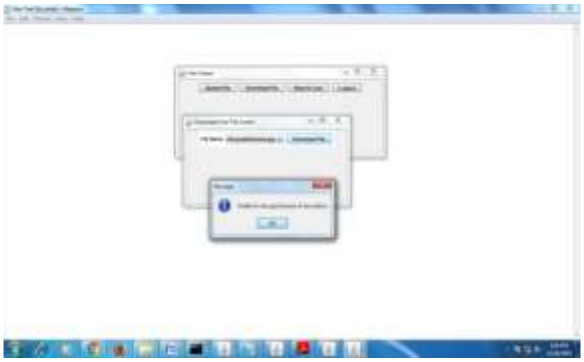


Owner/ user can report the loss of device, if they lost the device then wont able to decrypt the data:

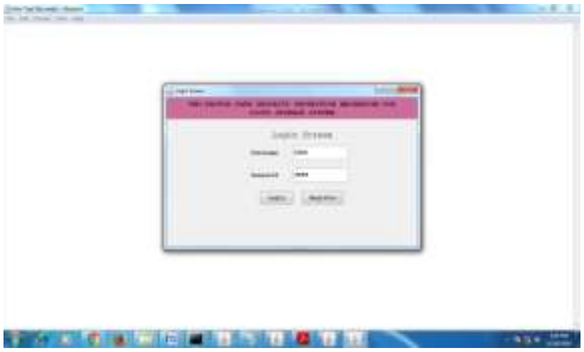
After reporting the loss of device:

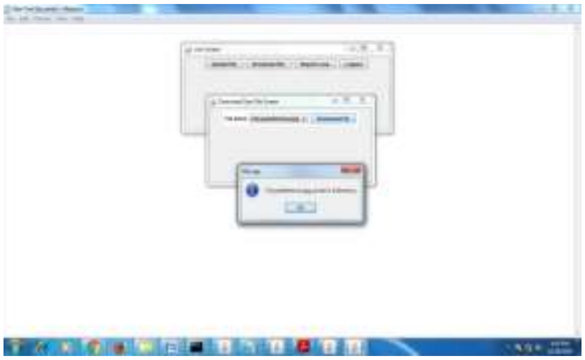


Unable to decrypt the data:

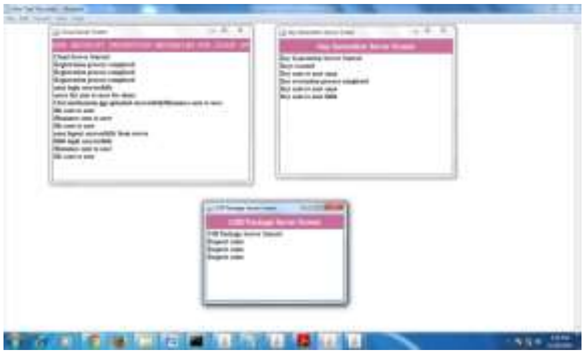


Login as a user and try downloading:





The cloud server, Keys server & USB server



6. CONCLUSIONS

In this paper, we introduced a novel two-factor data security protection mechanism for cloud storage system, in which a data sender is allowed to encrypt the data with knowledge of the identity of a receiver only, while the receiver is required to use both his/her secret key and a security device to gain access to the data. Our solution not only enhances the confidentiality of the data, but also offers the revocability of the device so that once the device is revoked; the corresponding cipher text will be updated automatically by the cloud server without any notice of the data owner. Furthermore, we presented the security proof and efficiency analysis for our system.

REFERENCES

[1]. Akavia, S. Goldwasser, and V. Vaikuntanathan, “Simultaneous hardcore bits and cryptography against memory attacks,” in Proc. 6th Theory Cryptography Conf., 2009, pp. 474–495.

[2]. S. S. Al-Riyami and K. G. Paterson, “Certificateless public key cryptography,” in Proc. 9th Int. Conf. Theory Appl. Cryptol., 2003, pp. 452–473.

[3]. M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen, “Certificate based (linkable) ring signature,” in Proc. Inf. Security Practice Experience Conf., 2007, pp. 79–92.

[4]. Naga Charan Nandigama, “Data-Driven Cyber-Physical Customer Experience Management In Iort-Enabled Banking Infrastructures,” International Journal of Data Science and IoT Management System, vol. 2, no. 3, pp. 22–27, Aug. 2023, doi: 10.64751/ijdim.2023.v2.n3.pp22-27.

[5]. M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang, “Malicious KGC attacks in certificateless cryptography,” in Proc. 2nd ACM Symp. Inf., Comput. Commun. Security, 2007, pp. 302–311.

[6]. Todupunuri, A. (2024). Generative AI For Predictive Credit Scoring And Lending Decisions Investigating How AI Is Revolutionising Credit Risk Assessments And Automating Loan Approval Processes In Banking. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5059403

[7]. Nandigama, N. C. (2016). Teradata-Driven Big Data Analytics For Suspicious Activity Detection With Real-Time Tableau Dashboards. International Journal For Innovative Engineering and Management Research, 5(1), 73–78

[8]. M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 1998, pp. 127–144.

[9]. Todupunuri, A. (2024). Develop Machine Learning Models to Predict Customer Lifetime Value for Banking Customers, Helping Banks Optimize Services. International Journal of All Research Education &amp; Scientific Methods, 12(10), 1254–1259. https://doi.org/10.56025/ijaresm.2024.1210241254

[10]. A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in Proc. ACM Conf. Comput. Commun. Security, 2008, pp. 417–426.

[11]. D. Boneh, X. Ding, and G. Tsudik, “Fine-grained control of security capabilities,” ACM Trans. Internet Techn., vol. 4, no. 1, pp. 60– 82, 2004.