E-Locker

MrunaliWaghmare[#1], AishwaryaLingaware[*2], Neelam Padole[#3,] Priyanka Meghare[#4]
[#]*Department of Computer Technology&SantTukadojiMaharaj Nagpur University, Nagpur, India*

Abstract:
Many times documents lost in certain mishaps like fire mishaps, natural calamities as earthquake, tsunami or any accident. Then it is very difficult to get these lost documents after those mishaps. Also when there is need to submit documents in the college or any office many times it happens that those physical documents may lost and procedure may get delay. Recently in Nepal earthquake people lost their documents and for rehabilitation there was need of documents to build their houses and for jobs. It was not easy to get their documents quickly.

To overcome all these problems there is need of reliable and secure system. For this E-locker is good solution which provides secure dedicated personal electronic space for storing documents of students and staff member of college. It provides a dedicated personal e-storage space to each account linked to their enrollment number. Cloud Based E-Locker is a website where one can create a personalized web Gallery on cloud to store images, audio, video files, and other document.

Keywords:*Cloud computing, Azure Storage,Puzzle Lock,*

I. Introduction

Cloud Based E-Locker is a website where one can create a personalized web Gallery on cloud to store images, audio, video files, and other document. Data stored by the user can marked as public or private. Private data can be accessed only with the permission of data owner. Data can be shared to another user by data owner on request. For secure authentication of user the system will be enabled with a puzzled lock.

Most of our important documents are prevalent in physical form, leading to huge administrative overhead .So that it is difficult for us to submit multiple physical copies of the documents. E-locker is the best solution to minimize the use of physical documents. Uploading your certificates like those related to birth, mark sheets, income and caste certificates on the E-locker will ensure that there is no need to carry them in the physical format when they are needed for educational or job applications. User can also sharee-documents online. It also provides access to the documents anytime and anywhere.

E-locker is implemented with the help of cloud services provided by Microsoft azure. Azure Storage is massively scalable, so you can store and process hundreds of terabytes of data to support the big data scenarios required by scientific, financial analysis and media applications.

II. Background work:

Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting Company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data.

Cloud storage services may be accessed through a co-located cloud computer service, a web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web-based content management systems.

III. Azure

Cloud computing enables new scenarios for applications requiring scalable, durable, and highly available storage for their data – which is exactly why Microsoft developed Azure Storage. In addition to making it possible for developers to build large-scale applications to support new scenarios, Azure Storage also provides the storage foundation for Azure Virtual Machines, a further testament to its robustness.

Azure Storage is massively scalable, so you can store and process hundreds of terabytes of data to support the big data scenarios required by scientific, financial analysis and media applications.[3]or you can store the small amounts of data required for a small business website. Wherever your needs fall, you pay only for the data you're storing. Azure Storage currently stores tens of trillions of unique customer objects, and handles millions of requests per second on average.

Azure Storage is elastic, so you can design applications for a large global audience, and scale those applications as needed - both in terms of the amount of data stored and the number of requests made against it. You pay only for what you use, and only when you use it.[3]

Azure Storage uses an auto-partitioning system that automatically load-balances your data based on traffic. This means that as the demands on your application grow, Azure Storage automatically allocates the appropriate resources to meet them.

Azure Storage is accessible from anywhere in the world, from any type of application, whether it's running in the cloud, on the desktop, on an on-premises server, or on a mobile or tablet device. You can use Azure Storage in mobile scenarios where the application stores a subset of data on the device and synchronizes it with a full set of data stored in the cloud.

Azure Storage supports clients using a diverse set of operating systems (including Windows and Linux) and a variety of programming languages (including .NET, Java, and C++) for convenient development. Azure Storage also exposes data resources via simple REST APIs, which are available to any client capable of sending and receiving data via HTTP/HTTPS.

Azure Premium Storage is now available in preview. Azure Premium Storage delivers high-performance, low-latency disk support for I/O intensive workloads running on Azure Virtual Machines. With Azure Premium Storage, you can attach multiple persistent data disks to a virtual machine and configure them to meet your performance requirements. Each data disk is backed by an SSD disk in Azure Premium Storage for maximum I/O performance.

Azure contain Page blobs which are optimized for representing IaaS disks and supporting random writes, and may be up to 1 TB in size. An Azure virtual machine network attached IaaS disk is a VHD stored as a page blob.

For very large datasets where network constraints make uploading or downloading data to Blob storage over the wire unrealistic, user can ship a hard drive to Microsoft to import or export data directly from the data center using the Azure Import/Export Service. User can also copy blob data within your storage account or across storage accounts.

IV. Methodology:

In E-locker project, user has to register them on the E-locker website.They have to fill basic information like name,email-id, and contact number. After successfully generating the graphical password user's account will get created on the website.There will be two sections for every user i.e. private and public. If users want to show data publically then user can select public section and if users want to send the data to some person only then user have to select private section.After creating account user can login to website and user will get free space on cloud to upload their documents on cloud. User may upload an image, audio, video or any text document. Each user gets 100 MB to store their documents. E-Locker stores the files on cloud. When user uploads files first it goes to server after that there is option, 'submit to cloud', clicking on it, and file store on cloud. When user upload the data, it will first encrypt and the store on server. To encryption of data, AES128 bit algorithm is use. E-Locker uses Azure Storage Services to store the files on cloud. Azure Storage is massively scalable, so you can store and process hundreds of terabytes of data to support the big data scenarios required by scientific, financial analysis and media applications. A standard storage account includes Blob, Table, Queue, and File storage. Blob storage stores file data. A blob can be any type of text or binary data, such as a document, media file, or application installer. Every blob is organized into a container. Containers also provide a useful way to assign security policies to groups of objects. A storage account can contain any number of containers, and a container can contain any number of blobs, up to the 500 TB capacity limit of the storage account.

For sending files to a particular person only, user will type email-id of that person and then user can upload file on cloud server and then send files to that person.There will be a facility of customize selection of files.After sending these files a link will get generated. Anyone can access the public files of user. By clicking on this link user can download files.

At the time of downloading file which receives at sender site will firstly get decrypted by AES128 bit algorithm as sender use AES128 bit to encrypt the file. While downloading file, system server will get that file from cloud then it will send to the receiver. System server will check the session of receiver that if session is null then user will redirect to the default page or if session is not null then new session to the user is assign for downloading. Then only user will be able to download file from link send by sender. After specific time period user will not able to download from that link as link will be time out.

Database

Security is the primary concern while working with database. DOTNET Framework supports two models of Data Access Architecture, Connection Oriented Data Access Architecture and Disconnected Data Access Architecture. In Connection Oriented Data Access Architecture the application makes a connection to the Data Source and then interacts with it through SQL requests using the same connection. In these cases the application stays connected to the database system even when it is not using any Database Operations.[5] E-Locker is designed using disconnected model of database to protect database from hackers. Data Reader is "connected" approach and dataset is "disconnected" approach this concludes that in data reader we need to establish the connection to the database while in dataset there is no need to establish the connection to the data base. By keeping connections open for only a minimum period of time, A DOTNET conserves system resources and provides maximum security

for databases and also has less impact on system performance.

Puzzle Lock

Human factors are often considered the weakest link in a computer security system. Patrick, et al. point out that there are three major areas where human computer interaction is important: authentication, security operations, and developing secure systems.

Here the focus is on the authentication problem. The most common computer authentication method is for a user to submit a user name and a text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also be easily guessed or broken. [2]

According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords. On the other hand, passwords that are hard to guess or break are often hard to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts. [2] To address the problems with traditional username password authentication, alternative authentication methods, such as biometrics, has been used.

In E-Locker, there is use of pictures as passwords. Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text; psychological studies supports such assumption. Pictures are generally easier to be remembered or recognized than text. In addition, if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text based schemes and thus presumably offer better resistance to dictionary attacks. Because of these (presumed) advantages, there is a growing interest in graphical password. In addition to workstation and web log-in applications, graphical passwords have also been applied to ATM machines and mobile devices.

In this project, for secure authentication of user the system is enabled with a puzzled lock. In puzzled lock, there is n X n matrix and each cell has one image with certain three random alphabets. To create a password user have to select images and write code given below it. User can give password of any length provided it is the multiple of 3. This password will act as an OTP (One time password) as every time the code below images will change randomly. This will provide more security to user password.

Encryption

AES achieves the goal of being both secure and practical for real systems. The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data, the data to be encrypted. This array is the state array.[4]

Following are the steps of AES encryption for a 128-bit block:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (cipher text).

The reason that the rounds have been listed as "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others.

The block to be encrypted is just a sequence of 128 bits. AES works with byte quantities so first convert the 128 bits into 16 bytes. It says "convert," but, in reality, it is almost certainly stored this way already. Operations in RSN/AES are performed on a two-dimensional byte array of four rows and four columns. At the start of the encryption, the 16 bytes of data, numbered D0 to D15, are loaded into the array.

Each round of the encryption process requires a series of steps to alter the state array. These steps involve four types of operations called:

- SubBytes
- ShiftRows
- MixColumns
- XorRoundKey

Decryption

As you might expect, decryption involves reversing all the steps taken in encryption using inverse functions:

- InvSubBytes
- InvShiftRows
- InvMixColumns

Conclusion

E-locker has the potential to eliminate carrying physical copies of various certificates.They are also a safeguard against the loss ormisplacement of these papers.They will be ready to download or forwarded anywhere, anytime.No more long queues or procedures to collect the documents.E-documents are easy to share.

This projectcan use for colleges where students can upload all their marksheets and certificates. In government offices also, we can use it by adding some more features and at greater extent.

Acknowledgment

We would like to express our profound sense of deepest gratitude to our guide and motivator Ms.NilimaJichkar, computer technology department YCCE, Nagpur for her valuable guidance and co-operation for providing necessary facilities and sources during the entire period of this project. Her sincere effort and encouragement shows a new direction in technical education and our improvement.

We wish to convey our sincere gratitude to HODProf. Kavita Singh sir computer technology department who have enlightened us during our studies. The faculties and co-operation received from the technical staff of computer department is thankfully of acknowledged.

References

[1] "DigiLocker-Online document storage facility"http://www.indian.gov. 16 July 2015

[2] DipikaKumari, Kumar.NP.Pandey "Survey on Graphical User Authentication"Mechanical Engineering Department MWWWNNIIIIT Australia.

[3] Tamra Myers "Intoduction to Microsoft Azure Storage"http://www.googleweblight.com/azure.microsoft.com/documentation/articles/storage-introduction. 30 June 2015

[4] "Steps in the AES Encryption Process::Appendix A. Overview of AES Block" http://etutorials.or g/Networking/Steps in AES.

[5]Sudhakarchaudhary"Working in a Connected and Disconnected Enviroment" https://www.c-sharpcorner.com/UploadFile/9a3ae2/ Working in a Connected and Disconnected Enviroment. 25July 2012

[6] How does DigiLocker work? – DigiLocker" https://www.digitallocker.in/How does DigiLocker work 22 February 2015

[7] A Kak"Lecture 8:AES: The Advance Encryption Standard Lecture" https://engineering.purdue.edu/compsec 2015

[8] A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp. 41-46, 1999.

[9]Ankita Sharma and Sonia Vatta "Cloud Computing: Taxonomy and Architecture" International Journal of Advance Research in Computer Science and Software Engineering. Volume 3, Issue 5, May 2013.