Implementation of security for cloud backed files of note-taking application

A.Rajakrishnammal
PG Scholar, Department of CSE,
Saveetha Engineering College,
Thandalam, Chennai, India

R.Mervin
Associate Professor, Department of CSE,
Saveetha Engineering College,
Thandalam, Chennai, India

Abstract—**The act of taking notes is nature to most people. In the business and academic world note-taking can play a variety of important roles such as aiding memory recall of events, idea capture, problem solving or visualization of complex systems.With the concepts through the use of diagrams or sketches, attachments such as text, audio, video files and exporting notes to other applications with captured digital media. The digital form of this proposed system designed and developedwith the ability to format through notes, back them up, providing security, and ubiquitous access to them. The cloud storage is integrated with the note-taking application to store the confidential notes through Application Program Interface. To secure notes before storing to the cloud storage data encryption techniques are used.Encrypted files stored on cloud drive in CloudMe and it can be accessed programmatically.These digital enhancements implementation presents a challenge especially when combined with a requirement to provide a highly secure storage environment to protect confidential notes at rest.**

Key words—*Note-taking,Cloud drive, CloudMe.*

I. INTRODUCTION

Cloud Computing refers to manipulating, configuring and accessing the hardware and software resources remotely by offering online data storage, infrastructure, and application. It provides the access to storage as utilities over the internet that allows us to store and retrieve the data from any place. Now a days security is also be a part of cloud services. It provides the security to the files stored in the cloud servers. In the proposed system, the note-taking files that are created by the user is stored,retrieved in the CloudMe storage, using their CloudMe account. Generally CloudMe offers the password protection. It doesn't offer any encryption technique before storing the files in to it. And the proposed note-taking applications offer the security to the notes created. In this system User's notes files are encrypted and stored to the CloudMe account. The files are encrypted using the Advanced Encryption Standard Technique, in which the design and strength of all key lengths of the AES algorithm are sufficient to protect classified information up to the secret level.Private data should be securely used on every point alongthe path which the data needs to be password protected, encrypted. Additionally any sharing of data needs to be limited to same encrypted and contained environment. The basic business requirements from users were the ability to digitally take notes and pictures and share them with the corporation or community. The corporate security requirements state that data at rest, data in motion, and sharing or exporting must be limited to the corporate applications that follow the same security models. Security by design in a corporate IT setting, means that it is easier for an employee to keep data secure them to expose that data. Digital note-taking provides a very simple well designed and easy to use application.

A primary requirement of enterprise applications in recent times is the need to adapt and respond quickly to requirements from the business. This might be to suddenly support a new group of users with slightly different demands or to provide some new market driven feature to all users. Being able to adapt and respond quickly depends on the ability to meet several key requirements such as portability, scalability and availability.Further section consists of II. Related work, III. Architecture, IV. Implementation and V. conclusion.

II. RELATED WORK
Design thinking

Nigel Cross proposed the concept[2] of Design Thinking: Understanding how designers think and work. It explores and explains this apparently mysterious design ability. Focusing on what designers do when they design, Design Thinking is structured around a series of in-depth case studies of outstanding and expert designers, interwoven with overviews and analyses. The range covered reflects the breadth of design, from hardware and software design to architecture and Formula One. The book offers new insights into and understanding of design thinking, based on evidence from observation and investigation of design practice. Design Thinking is the distillation of the work of one of design's most influential scholars. Nigel Cross goes to the heart of what it means to think and work asdesigner. The book is an ideal guide for anyone who wants to be a designer or to know how good designers work in the field of contemporary design.

It consists of the related concepts like asking designers about what they do about designing, design ability, designing process, working methods, motivation, attitude, designstrategies, design expertise, design intelligence, interactive design and graphic design for computer software, case studies and so on. usually been focused on one particular design project at a time, with observers recording the progress and development of the project either contemporaneously or post hoc. Both participant and non-participant observation methods have been included, and varieties of real, artificially constructed and even re-constructed design projects have been studied. Although there is so much design activity going on in the world, the ways in which people design were rather poorly understood for rather a long time. Design ability has been regarded as something that perhaps many people possess to some degree, but only a few people have a particularly strong design 'gift'. Some people are better designers than others. Ever since the emergence of designers as professionals, it has appeared that some people have a design ability that is more highly developed than other people – either through some genetic endowment or through social and educational development. To meet the cloud architecture requirements it was decided that the container solution Docker [4] should be used. Docker would provide the base upon which the portability, scalability and ease of deployment requirements would be met.

Enriching the user experience

Brett S Gardner presents[3], Responsive Web Design: Enriching the User Experience, as a greater selection of devices become able to access the Internet, website designers are finding it harder to predict user context [3]. Traditional best practice for website design advocates using a minimum target resolution a kind of low-end catchall for the browsing windows on various devices. The idea is to gather statistics on website visitors and their screen resolutions and use the results to identify the lowest resolution that would accommodate some acceptably high number of users. It states that images that work in a flexible context, whether fluid themselves or perhaps controlled through overflow mechanisms. Layouts based on percentages resize gracefully according to the size of the browser window rendering them. Responsive web design's flexible architecture and powerful media queries have many advantages, but they come with some implementation issues. A major one is that older browsers don't support media queries. However, nearly all newer versions offer full support.

It presents several emerging technologies, design patterns, and digital interaction channels that will comprise the future user-centric digital ecosystem. These articles demonstrate how organizations can effectively apply user experience not only to respond to future technology trends and refreshment cycles but also to rapidly evolve with the ever changing user. In a blog entry, outlined a method for creating fluid layouts that are screen-resolution agnostic and "future proof," capable of dynamically changing according to user context. He described responsive design as having three parts: a fluid layout that uses a flexible grid, which in turn ensures that a website can scale to a browser's full width; images that work in a flexible context, whether fluid perhaps controlled

through overflow mechanisms; and media queries, which optimize the design for different viewing contexts and spot-fix bugs that occur at different resolution ranges.With a fluid layout, flexible content, and web standards that can sense display capabilities—size, resolution, pixel density, and orientation—designers can finally create context-sensitive, adaptable websites. The result should be an improved experience for all users that access the site, not just those in a minimum target range.

User research is essential to help organizations surface unfamiliar user needs, perspectives, and goals to provide customers with an enriched experience. Organizations such as Human Factors International has developed training programs geared to the science of persuasion, emotion, and trust to help businesses create successful online interactions that motivate and influence users. The training program provides research based methods to help organizations understand the human factors that lead to customer conversion. Such understanding then becomes the basis for developing persuasive strategies and forging strong customer relationships. The spontaneous comments of designers themselves about designing can seem obscure, but it is possible to gain some insights byinterviewing them more care-fully, and interpreting the implications of their responses. Asking designers about what they do is perhaps the simplest and most direct form of inquiry into design ability, although this technique has not in fact been practiced extensively. Chrome and Safari fully support the max-width property. For older IE and Firefox versions, website designers must use a browser specific style sheet instead. Such legacy browsers can be quirky when rescaling certain media types. If a website must support these browsers, the designer can also incorporate a JavaScript solution to handle media scaling on the browser's behalf.

III. ARCHITECTURE

Note-Taking files Storage Cloud Architecture

The cloud architecture describes that the note-taking app is integrated with the cloud storage CloudMe. Initially the user can create their notes through the note-taking user application.
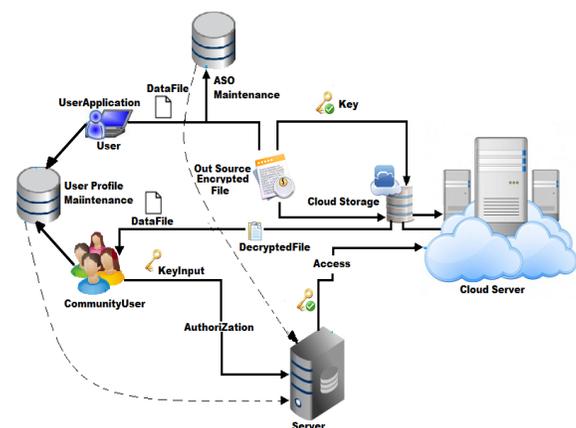

Fig. 2. Note-taking files Storage Cloud Architecture

And encrypt the notes, active storage object maintenance maintains the user notes files, and the keys are stored in specific server, then the encrypted files moved to the CloudMe account. If the user or community user requests the file, then it request key and authorize the key to provide access to the requested file by decrypting them.

1) User Application

The user Application represents the note-taking application to create, save and retrieve the notes.

2) Community User

It allows the group of users to collaborate with others to share their notes.

3) Key Store

AES algorithm[4] uses the key to encrypt and decrypt the notes. So storing and maintaining the key secretly is a challenging one. The key is stored in cloud storage, and it can be shared to the user through the secret value which is the reference to the key.

4) Cloud Storage

CloudMe[6] is used as a cloud storage to store and manage the user notes.

5) Cloud Server

The CloudMe Storage service is provided by the European Cloud server where the cloud storage is resided.

Storage In The Cloud

The data is the gold of the application. Clearly the critical aspects of the digital note-taking application are the user's digital notes themselves. The user notes contain metadata and attachments such as HTML text or photos. A variety of models can be used to store metadata plus attachments such as keeping the note metadata and index data in a database pointing to attachment files in a file system.

Sweden-based CloudMelooks like a fairly standard online backup and sync service, and it's clearly taken a lot of inspiration from the well-known Dropbox service, with similar pricing, a free option, and extra storage for referrals.

The service itself works well, and may be exactly what some users are looking for. CloudMe has a relatively standard feature set, but it's worthy of note that its WebDAV functionality does give you the ability to interface with a host of the note-taking app files.Still, CloudMe does work as a simple backup, sync and sharing service.User could find some use for it as a simple place to dump some notes files. Essentially, CloudMe doesn't offer any built in encryption. It is free toupload and download encrypted files, but the encryption process itself is down to user.

IV. IMPLEMENTATION

Application Design

Design guidelines [2] and libraries are provided for iconography, color schemes, and layouts. It is used to create uniform look and feel enterprise note-taking application. Using the design thinking guidelines and frame works for the note-taking application has a consistent look and feel and coherent experience throughout. As a note-taking app, the most important aspect is the note content. The note-taking app allows the users quickly and reliably take notes and note

necessarily to format them during the process. Lastly simple design and well thought out user flow will leave users with a good experience while accomplishing an important task.

Finally font and color play on important but subtle role in the app experience. Well-matched colors and contrast can guide the user on the flow of the application without requiring explicit help content. Consistent typeface font and scale provides users with focus on content. This is a highly user interactive application. Using native user interface (UI) and controls help make the user experience much more simple and smooth. This application is a new kind of hybrid that consists mostly of native UI in terms of layout, controls, and gestures. However there is one web view component, which is native by design but displays data that is compatible with other platform.

The simplicity of the design also lends itself to be cross platform and makes the app easy to use. With only a few key screens the user can learn to use the app through intuition. UI elements are placed by task and frequency of usage. Most commonly required functions such as writing a note appear automatically as the main focal point on the page. Some tasks are done automatically such as save and sync so that the user never has to worry about losing their data.

With the fast progression of digital data exchange in electronic way, information security is becoming much more important in data storage and transmission. Security mechanism uses some algorithms to scramble data into unreadable text which can be only being decoded or decrypted by party those possesses the associated key.Advanced Encryption Standard (AES) algorithm is not only for security but also for great speed. It can be implemented on various platforms specially in small devices. It is carefully tested for many security applications. In the proposed system to protect the user notes files are protected using this AES algorithm.

Fig. 1. Note-Taking User Interface Design

Fig.2. depicts the user interface. Using thisuser creates the notes and saves it in to the cloud storage, before storing to the

cloud storage the notes files are encrypted by the four steps in the AES algorithm. The four rounds are Substitute Bytes, Shift Rows, Mix Columns and Add Round Key. Here the input plain text is the user notes, then the plain text is transformed using the four rounds. Decryption is done while the user retrieves their notes from the cloud storage where the file is encrypted format, so these cipher text is provided as a input to the AES [4] decryption, the it will ask for the key used to decrypt the cipher text. User provides the key and the file is decrypted at the client side machine.If the users want to share the encrypted file with the other users in the community, they have to share the key by sharing the secret value. Here the secret value is a reference to the key which is stored in the cloud storage. Using this reference the community users can access the key and decrypt the encrypted file.AES algorithm consumes least encryption [5] and RSA consume longest encryption time.

Connecting application to cloud

CloudMe [6],[7],[8],[9],[10],[11] connects desktop to cloud, it reports that the cloud storage service provider CloudMe has updated its CloudMe desktop application for Linux, Mac, and Windows. It states that CloudMe aims to connect its desktop software and online service. Also mentioned are the operation and services offered by the company including storage, sharing, and synchronization. CloudMe is the European Sync / Storage provider. A full service provider of; file syncing, backup, restore, sharing and online cloud storage. All data on CloudMe is safely stored on servers that are owned, operated and maintained by CloudMe in a data center facility located in Sweden, the European Union. From this data center, CloudMe serves users worldwide in more than 200 countries. CloudMe is incorporated in Sweden, EU.

Security Implementation

With CloudMe users are able to activate client-side encryption for any folder. This will require user to enter an encryption key that will be used to encrypt user files before sending them over the encrypted communication channel to CloudMe. Since all encryption is done on the client-side. Advanced Encryption standard algorithm with 126 bit keys are used to protect the user files and notes.

V. CONCLUSION

Electronic note-taking is a common practice on laptop and mobile devices and there are a number of applications available on the consumer market today.it becomes more portable solution than traditionalarchitectures.
The purpose of using an AES algorithm is resistant against known attacks, simple, and quick to code. The solution described above differentiates itself from others by providing a secure and contained user experience needed by corporations to help protect from data leakage and data exposed in the clear. Future work will focus on developing the cloud backed note-taking application, and providing the large volume of cloud storage to the user.

REFERENCES

[1] Robert Smart, David Jaramillo, Charisse Lu, Thomas Cook," Implementing a cloud backed scalable note-taking application with encrypted offline storage and cross platform replication,"Proceedings of the IEEE SoutheastCon 2015, April 9 - 12, 2015Fort Lauderdale, Florida.

[2] Nigel Cross, "Design Thinking: Understanding how designers think and work" Apress, May 2011.

[3] Brett S Gardner, "Responsive Web Design: Enriching the UserExperience,"Noblis, Volume 11, Number 1, October 2011.

[4] Douglas Selent,"Advanced Encryption Standard," Rivier Academic Journal, Volume 6, Number 2, Fall 2010

[5] Prerna Mahajan&AbhishekSachdeva "A study of encryption algorithms AES, DES and RSA for Security," Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013

[6] CloudMe,wikipedia.org/wiki/CloudMe

[7] Yates, Darren(2014), "Cloudme connects desktop to cloud" Worldwide Databases; Vol. 26 Issue Number 4.

[8] (2014), "CloudMe goes all in with responsive design for its European sync / cloud storage service", www.cloudme.com/en/pr.

[9] (2012), "CloudMe Integrates With WinZip to Provide Secure EU Cloud Storage and File Sharing", www.cloudme.com/en/pr.

[10] (2014), "CloudMe makes the desktop experience seamlessly connected with the cloud" CloudMe press releases, www.cloudme.com/en/pr.

[11] (2013), "WD Sentinel CloudMe User Guide", CloudMe.com WD Sentinel CloudMe User Guide, www.cloudme.com/en/pr, Document.