International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9, Issue-7, May 2020

Secured data management using face detection and Video mode

B.Kalpana, A.K.Manaswini, K.Gayathri, Kotamreddy Srilekha

Abstract : ***Data security is protecting digital data, from the unwanted actions of unauthorized users, like cyberattack or data breach. Data is no longer said to be secure if it falls into the hands of hackers or those that would misuse it. Data is well secured and guarded within an organization. But, when its employees sell their access specifiers to their competitors, data is no longer protected. This could be avoided by advanced technology. The Identity-based approach is an approach to regulate access to a digital product or service based on the identity of an individual. This allows organizations to grant access to a variety of digital services using the same credentials, ensuring the accurate match between what users are entitled to and what they really receive, while also permitting other access constraints like company, device, location and application type(attributes) In our application, data is uploaded by an encryption format attached with the video mode and it is downloadable by the user only through the unique face detection mode. When a user tries to download the encrypted file, a notification is sent to four admins for better privacy reasons. Only upon acceptance from four of these admins, the file could be downloaded. The admins can authenticate the user using his face captured through face detection. This could be used at any level in an organization but is much efficient when no of users trying to access a file is limited. This provides high security and rejects unauthorized users. Breach of data leads to a decline in profits and incline in losses. This could be reduced if the data security could be ensured using face detection of a person who is trying to access the data.***

Keywords – Identity-based approach, Encryption, Face detection.

I. INTRODUCTION

In today's digital world, data security has become a big problem. Data is no longer said to be secure if it is attacked by hackrs or by some man-in-the-middle. Authenticated people may lose their login credentials which might benefit others who are trying to get access to the data. Besides, these credentials could be sold to some influential people who will use it for their personal uses. The issues in the current system are:

- Vulnerability to fake data collected from various sources
- Existence of untrusted mappers.
- Troubles of cryptographic protection.
- sensitive information mining.
- Data provenance difficulties.

A.User Friendly: The app which developed is user friendly because its user interface is quite simple and easy to understand. One doesn't need any guidance or complex instructions to handle or to use the application.

B.Application Control Management: The mobile-based control is maintained by representatives and an administration that updates and controls the entire system. So, there is no scope for errors. Moreover, storing and retrieving information is easy.

In this paper, we explained the literature survey in subsection II. Subsection III and IV will be describing the design and development of the application and its architecture. The final subsection concludes the paper.

II. LITERATURE SURVEY

The Vision of this paper is to ensure that data is stored securely in an organization. This not only stores data securely but also monitors about who and when has accessed the data. This allows employees or administrators to allow only legitimate users to get access to the data. It faces the challenges in the establishment of data security in organizations and other places. It avoids complex processes and makes the entire process safe and secure. It does not require more no of the staff and can be used as an online application. This paper addresses those data security challenges in an organization through a website. Thus, data security is no longer a complex issue and this can lead to incline in profits rate for an organization.

DEVELOPMENT OF DATA MANAGEMENT APPLICATION

We have developed a graphical tool based on data flow diagram to analyze and describe the movement of data in the system. From this central tool, the other components will be developed. The transformation of data from input to output, their processing will be described independently and logically with the physical components associated with the system. These are known as logical data flow diagrams. The actual implementation and movement of data between people, departments and, workstations will be shown in this Physical data flow diagram. The full description of the system comprises a set of data flow diagrams.

Revised Manuscript Received on May 30, 2020.

***** Correspondence Author

Dr.B.Kalapana*, Assistant Professor, Department of Information Technology,R.M.D Engineering College,Thiruvallur,, Tamilnadu, India. Mail: cgkkalpana@gmail.com

A.K.Manaswini*, Currently pursuing bachelor's degree in the stream Information Technology at R.M.D Engineering College,Thiruvallur, Tamilnadu, India. Mail: keziamanaswini@gmail.com

K.Gayathri, Currently pursuing bachelor's degree in the stream Information Technology at R.M.D Engineering College, Thiruvallur,Tamilnadu,India. Mail: gayathrikrishanan33l@gmail.com

Kotamreddy Srilekha, Currently pursuing bachelor's degree in the stream Information Technology at R.M.D Engineering College, Thiruvallur,Tamilnadu,India. Mail: lekha.kotamreddy@gmail.com

Each component is labeled with a descriptive name. The DFD's will be developed at several levels. Each process in low-level diagrams will be further drilled down into more detailed DFD in the next level. The top-level diagram is called a context diagram, and it consists of a single process bit. In first level DFD, the process in this diagram is exploded into other processes.

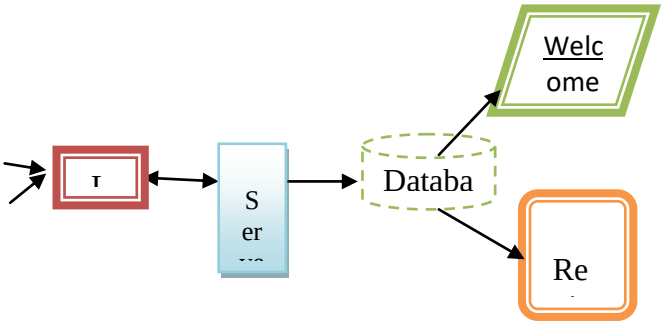

Figure: Level 0 DFD

Data flow will move in only one direction between the symbols. Before an update, it may flow in both the directions between a data store and a process In DFD, If the same data comes from two or more different processes the data will be pooled or sink in a common location known as join. It requires a huge database, as it stores huge Volumes of data about all those who tried to access the data.

A. Algorithm Behind website (Application):

This application uses the AES encryption algorithm to encrypt and store the uploaded data. It is highly secured and efficient in various ways.

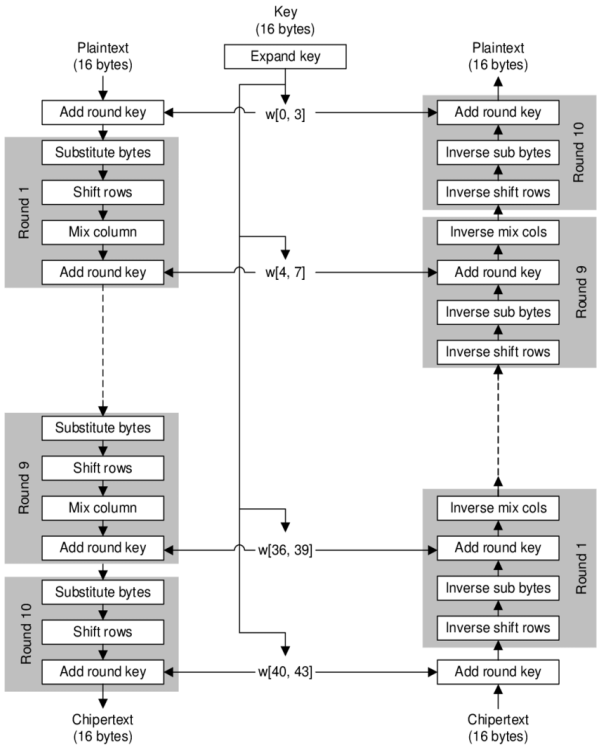

Figure: Algorithm working

III. EXISTING SYSTEM:

In an existing system, data is corrupted by the unauthenticated user with the help of employees. Even though the data is securely managed by an organization, a few employees still sell their credentials and access specifiers to hackers for money.

Currently, the data signing algorithm is being used to store data safely. Using this, the user can only sign documents on that particular computer. The security of the private key depends completely on the security of the computer.

This platform has some demerits. First, the user can only sign documents on that particular computer. Second, the security of the private key depends entirely on the security of the computer. Thus, it fails to manage the data securely in an organization.

IV. PROPOSED SYSTEM:

In this technique, the data is uploaded by the encryption format with video mode. Here, the data is shared in an encryption algorithm so that unauthorized users cannot access the data.

It uses the AES encryption technique. Through the use of this algorithm, data is actually broken down into some meaningless text that is not understandable unless broken down to its original form.

AES encryption algorithm scrambles the message and it can only be unscrambled with a key created at the same time. Cipher algorithms are either symmetric or asymmetric in nature. For example, Symmetric -The exact key is used to encrypt and decrypt data.

V. RESULT AND DISCUSSION

Login page

File download page

Video Notification Page

VI. ARCHITECTURE OF APPLICATION:

The main functionality of this application is to allow only legitimate users to get access to data. It provides a platform for the administrators to get a notification when someone is trying to access the data. It also allows them to accept or reject the person's request to access the data. Besides, it allows a person to upload and store a file securely. It records the session of a person trying to get access the data.

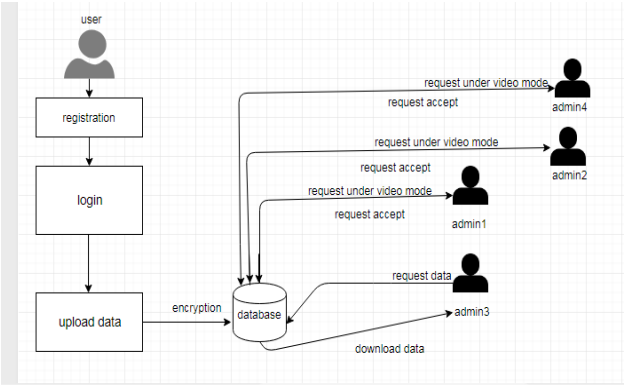

Figure: Architecture of Application

VII. FUTURE ENHANCEMENT:

The website designed will be made as an android app such as it'll get more reach and will be easily accessible. Live tracking feature and professional monitoring feature will continuously monitor the professional This service can be further extended to serve other areas of interest.

VIII. CONCLUSION:

Data security thus plays a vital role in the organization. Storage and access to data should be highly secured which else would result in incurring high losses to a company. Therefore, data must be securely stored and face detection mode contributes a high contribution to this part. Face detection provides high security and allows only authenticated persons to get access to the data. It allows a person to access the data not based on his credentials but by personal lookup by an administrator or a legitimate person. His/her session could be recorded for future use. This makes this more advantageous and secure.

REFERENCE*:*

1. Qingchen Zhang, Laurence T. Yang,,"PPHOPCM: Privacy-preserving High-order Possibilistic c-Means Algorithm for Big Data Clustering with Cloud Computing "
2. Joseph K. Liu, Kaitai Liang, Willy Susilo, Jianghua Liu, and Yang Xiang, Senior Member, IEEE "Two-Factor Data Security Protection Mechanism for Cloud Storage System", IEEE TRANSACTIONS ON COMPUTERS, VOL. 65, NO. 6, JUNE 2016
3. Qingji Zheng, Shouhuai Xu, Giuseppe Ateniese , University of Texas at San Antonio, USA, Sapienza University of Rome, Italy and Johns Hopkins University, USA, " VABKS: Verifiable Attribute-based Keyword Search over Outsourced Encrypted Data"
4. Victor Chang, Muthu Ramachandran, Member, IEEE, " Towards achieving Data Security with the Cloud Computing Adoption Framework "

AUTHORS PROFILE

Dr.B.Kalpana, B.E,M.E, Ph.D is an Assistant Professor in the Department of Information Technology, since May 2006. She obtained her B.E (CSE) from Sri Ram Engineering College and M.E (Embedded Systems) from Anna University, Chennai. She has obtained her Ph.D in Information and Communication Engineering from Anna University, Chennai, in 2019. She has been in the teaching profession for the past 15 years .Her areas of interest include Graphics and Multimedia, Network Programming, Operating Systems.

A.K.Manaswini, currently pursuing a bachelor's degree in the stream of Information Technology at R.M.D Engineering College, Thiruvallur, TamilNadu, India. She is interested in the fields of Cloud technology, App development and website development. She has done several projects related to application development.

K.Gayathri, currently pursuing a bachelor's degree in the stream of Information Technology at R.M.D Engineering College, Thiruvallur, TamilNadu, India. She is interested in Front end development and website designing. She has done many projects related to website development.

Kotamreddy Srilekha, currently pursuing bachelor's degree in R.M.D Engineering College, Thiruvallur, TamilNadu. She has keen interest in app development, cloud technology . She did many projects related to application development.