International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 5, May 2020||

Desktop Security Provider by using Fingerprint Authentication, Image Capture and Screen Recording

Dhanashri R. Zope[1], Prashansa N. Kankariya[2], Priyanka S. Patil[3], Prof.Leena R. Waghulde[4]

BE Scholar , Department of Computer Engineering, KCES's. COEIT, Jalgaon, India[1, 2,3]

Assistant Professor, Department of Computer Engineering, KCES's. COEIT, Jalgaon, India[4]

ABSTRACT: In Institute or Colleges some demos of the practical give to the student on PC or on projector. But sometimes student may be absent or not understand practical demo then teachers can show recordingof practical demo. In this situation teacher give demo repeatedly to the student. Desktop Security Provider is project to record desktop activity in media file and stored on hard-disk. User can play this media file in media player to see which activity will perform on desktop.Screen Recording also useful when system give the demo of critical settings on computer. System record this setting and make media file. This media file system give to user rather than explain manual daily life many user send message from one pc to another PC in network. In this process data are more important. In many cases hackers hack the message which travelling between the networks and change this data.

KEYWORDS:JMF Player , JDK tools , Java 1.6.0_16,Mantra MFS100 biometric fingerprint scanner.

I. INTRODUCTION

The system deals with recording activities happening on monitor. Desktop Security Provider is project to record desktop activity in media file and stored on hard disk. User can play this media file in media player to see which activity will perform on desktop. In Institute or Colleges, some demos of the practical give to the student on PC or on projector. However, But sometimes student may be absent or not understand practical demo then teachers can show recording of practical demo.In this situation teacher, give demo repeatedly to the student.

This system deals with recording screen using our Desktop Security Provider. In today's computer age all the vital areas are become computerized. With the increase in the dependence of the computer, system should have the provision in order to keep record of all audio video activities happening on the computer. With the help of this project, security systemcan do this in way that is more convenient and can save the recorded activities on hard disk or other storage devices. This project includes the video as well as audio recording of the screen in any colour depth and with any quality sound. Since it is the visual age for computers, system have made our application visually appealing, to attract even non-professionals.

II. RELATED WORK

Ashwini R. Patil, Mukesh A. Zaveri in, "A Novel Approach for Fingerprint Matching using Minutiae" have proposed effective fingerprint matching algorithm based on feature extraction.For minutia marking they considered one special false minutiae removal method.[1]

Chandra Bhan Pal, Amit Kumar Singh, Nitin, Amrit Kumar Agrawal in "An Efficient Multi Fingerprint Verification System Using Minutiae Extraction Technique" has combined many methods to build a minutia extractor and a minutia matcher. [2]

H B Kekre and V A Bharadi in "Fingerprint Core Point Detection Algorithm Using Orientation Field Based Multiple Features" have used Correlation based Fingerprint Recognition rather than detecting minutiae.[3]

Mary Lourde R and Dushyant Khosla in "Fingerprint Identification in Biometric Security Systems" proposed the issue of selection of an optimal algorithm for fingerprint matching in order to design a system that matches required specifications in performance and accuracy. [4]

Chomtip Pornpanomchai Apiradee Phaisitkulwiwat in, "Fingerprint recognition by Euclidean Distance" proposed the fingerprint recognition by Euclidean distance method. [5]

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 5, May 2020||

System analysis is the process of gathering and interpreting facts, diagnosing problem and using the fact to improve the system.
The existing system concentrates only on the security provided by the client and fragments data based on it. But the enhanced performance is achieved if the sensitivity of the data is also considered before storing the fragments. If suppose a non-sensitive data occupies the full storage space of the Level 1 client (highly secured client), then the sensitive data will not find space for itself. So we propose a simple quantitative metric termed as Fragmentation Factor which accounts both the security of the client and the sensitivity of the data. The highly secured data must be fragmented and placed in highly secured clients. The less secured data can be placed in Level 3 (less secured) clients in [1].The fragmentation Factor for each file is determined by the level of security of client required and the level of security necessary for data. Here we assure the bit wise values for the parameters to reduce the complexity.[2]

Very little research has been done to study the difficulty of cracking graphical passwords. Because graphical passwords are not widely used in practice, there is no report on real cases of breaking graphical passwords. Here we briefly exam some of the possible techniques for breaking graphical passwords and try to do a comparison with text-based passwords. The attack programs need to automatically generate accurate mouse motion to imitate human input, which is particularly difficult for recall based graphical passwords. Overall, we believe a graphical password is less vulnerable to brute force attacks than a text-based password. [3]

Fingerprint Scanners is a biometric device for authentication and identification through fingerprint recognition module which has superior execution, precision, toughness based on the fingerprint reader. Fingerprint Reader or Scanner is very safe and easy to use device for security compared to remembering the password that is vulnerable to fraud and difficult to keep in mind. [4]
The system deals with recording activities happening on monitor. Desktop Security Provider is project to record desktop activity in media file and stored on hard disk. User can play this media file in media player to see which activity will perform on desktop.
This system deals with recording screen using our Desktop Security Provider. In Institute or Colleges, some demos of the practical give to the student on PC or on projector. However, sometimes student may be absent or not understand practical demo when teacher display this practical demo. In this situation teacher, give demo repeatedly to the student.Fingerprints are the tiny ridges, whorls and valley patterns on the tip of each finger. They form from pressure on a baby's tiny, developing fingers in the womb. No two people have been found to have the same fingerprints -- they are totally unique. There's a one in 64 billion chance that your fingerprint will match up exactly with someone else's.[5]

Robot Fingerprint Matching Method ability to discriminate among different textures comes partly from our fingerprints, new research shows. Scientists say this study could influence the development of prosthetic hands for amputees, as well as for robotic systems.

As the finger passes over a surface, nerve endings in the skin detect vibrations that arise when the finger touches something, the study demonstrates. These nerve endings, called Parisian corpuscles, are connected to sensory neurons, which signal the brain. [6]

III. PROPOSED METHODOLOGY

Important phase in system development is the successful implementation of the new system design. Implementation includes all those activities that take place to convert from the old system to the new system. Two type of authentication is provided in our system, one is password login and the other is fingerprint authentication.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 5, May 2020||

- **Block Diagram**

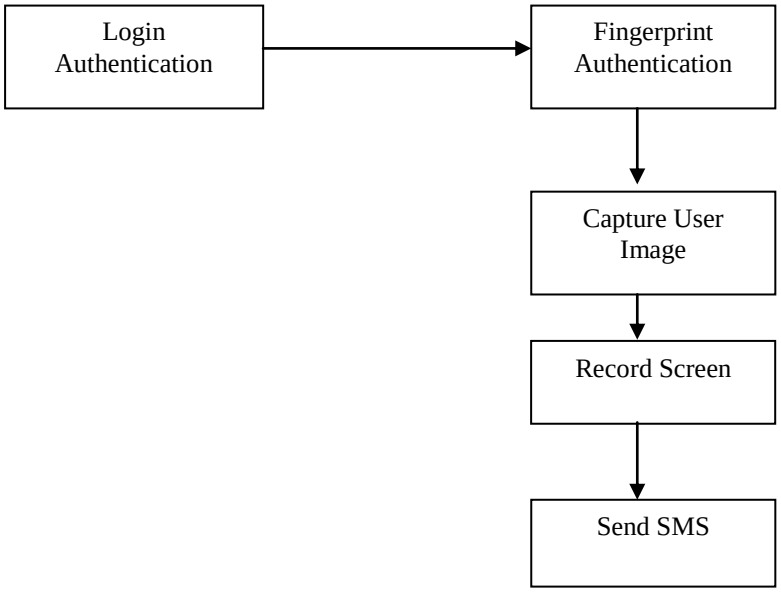

Figure 1 : Block Diagram of Desktop Security

1. Login Authentication

If unauthorized user trying to access the system forcibly through password and after many attempts he was not able to access the system then software will access through fingerprint authentication if the password showing incorrectly.

2. Fingerprint Authentication

For finger authentication we used Mantra MFS100 biometric fingerprint scanner. Mantra MFS100 biometric fingerprint scanner is high quality USB fingerprint biometric device for fingerprint authentication. MFS100 is based on optical sensing technology which efficiently recognizes poor quality fingerprints easily. System also used Robust Fingerprint Matching algorithm. Robust fingerprint matching algorithm is robust to rotation and translation alignment in which the best alignment of two fingerprints is achieved by maximizing the correlation between their extracted orientation fields. It utilizes the orientation field (OF) features for evaluating the similarity between test and trainee fingerprint images. Fingerprint Scanners is a biometric device for authentication and identification through fingerprint recognition module which has superior execution, precision, toughness based on the fingerprint reader.[7]

3. Capture User Image

If unauthorized user trying to access the system forcibly through fingerprint authentication and after mightily attempts he access to the system or many attempts he was not access the system the software capture the user image through simply web camera and send SMS .

4. Record Screen

When the user enters unauthorisedly , the screen will record through JMF player.

(a) JMF

Java Media Framework (JMF), which deals with media functions, were also helpful to us in implementing audio video effects. It supports recording, streaming, playing, and converting between multiple media formats.
JMF Players performs following activities :

- Record Screen : Select this option for screen recording.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 5, May 2020||

- Pause : It pauses the screen recording.
- Resume : By clicking on this button, recording will resume.
- Stop : Use his button to stop the recording.
- Area : By using this menu, we can select the area for recording.
- FPS Setting : This button will display a dialogue box to do setting for FPS.

(b) Displaying Menus

The task of this module is to display the menus of a Desktop Security Provider to navigate through the application. Giving reliable shortcuts and tool menus Is the main purpose keep in mind.

(c) Perform Various Functions (Record/Stop/Snap)

The task of this module is to allow the user to record, stop, snap the screen according to his needs. He should be able to choose the specific file where he want to save his recorded file. Then, recording, saving according to the requirement can be performed. Data validation should be performed before accessing the database.

(d) Browsing storage

The task of this module is to allow the user to allow to browse the destination storage for the recorded screen or captured screen shot.The proposed system is robust to rotation and translation alignment in which the best
alignment of two fingerprints is achieved by maximizing the correlation between their extracted orientation fields. The proposed approach utilizes the orientation field (OF) features for evaluating the similarity between test and trainee fingerprint images This approach requires very few pre-processing steps as compared to other approaches in the literature, which require very complex and computationally expensive steps.

5. Send SMS

When the user enters unauthorisedly , the screen will record the activity which perform by unauthorized user and Send SMS through email or text.

Robot Fingerprint Matching Method ability to discriminate among different textures comes partly from our fingerprints, new research shows. Scientists say this study could influence the development of prosthetic hands for amputees, as well as for robotic systems.

As the finger passes over a surface, nerve endings in the skin detect vibrations that arise when the finger touches something, the study demonstrates. These nerve endings, called Pacinian corpuscles, are connected to sensory neurons, which signal the brain.[8]

Algorithm for Normal Profile Generation And Attack Detection

In this algorithm the normal profile Pro is built through the density estimation of the MDs between individual legitimate training traffic records (TAM normal, i, lower) and the expectation (TAM normal, lower) of the legitimate training traffic records.
Step 1: Input network traffic records.
Step 2: Extract original features of individualrecords.
Step 3: Apply the concept of triangle area to extractthe geometrical correlation between the J^{th} and k^{th}features in the vector xi.
Step 4: Normal profile generation
i. Generate triangle area map of each record.
ii. Generate covariance matrix.
iii. Calculate MD between legitimate record's TAM and input records TAM
iv. Calculate mean
v. Calculate standard deviation.
vi. Return pro.
Step 5: Attack Detection.
i. Input: observed traffic, normal profile and alpha.
ii. Generate TAM for i/p traffic

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 5, May 2020||

iii. Calculate MD between normal profile and i/p traffic
iv. If MD < threshold
Detect Normal
Else
Detect attack.

In the training phase, we employ only the normal records. Normal profiles are built with respect to the various types of appropriate traffic using the algorithm describe below. Clearly, normal profiles and threshold points have the direct power on the performance of the threshold based detector. An underlying quality usual shape origins a mistaken characterization to correct traffic of network.

This algorithm is used for classification purpose.
Step1: Task is to classify new packets as they arrive, i.e.,decide to which class label they belong, based on the currently existing traffic record.
Step2: Formulated our prior probability, so ready to classifya new Packet.
Step 3: Then we calculate the number of points in the packetbelonging to each traffic record.
Step 4: Final classification is produced by combining bothsources of information, i.e., the prior and to form a posterior probability.

IV. EXPERIMENTAL RESULTS

- **Result For Successfully Login (Fingerprint Match)**

If unauthorized user trying to access the system to forcibly through fingerprint authentication or password and after mightily attempts he access to system. When he login to the system, the software capture image of unauthorized user and send SMS to the system owner and also records the activity which perform by unauthorized user.

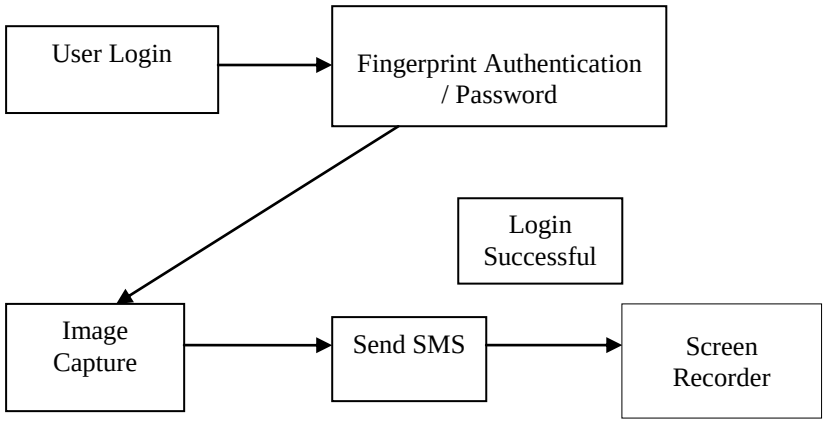

Figure 2 : Fingerprint Match

- **Result For Unsuccessful Login (Fingerprint Not Match)**

If unauthorized user trying to access the system forcibly through fingerprint authentication or password and after many attempts he was not able to access the system (Fingerprint not match) then software capture image of that user send SMS to the system owner and shut down or exit the system.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 5, May 2020||

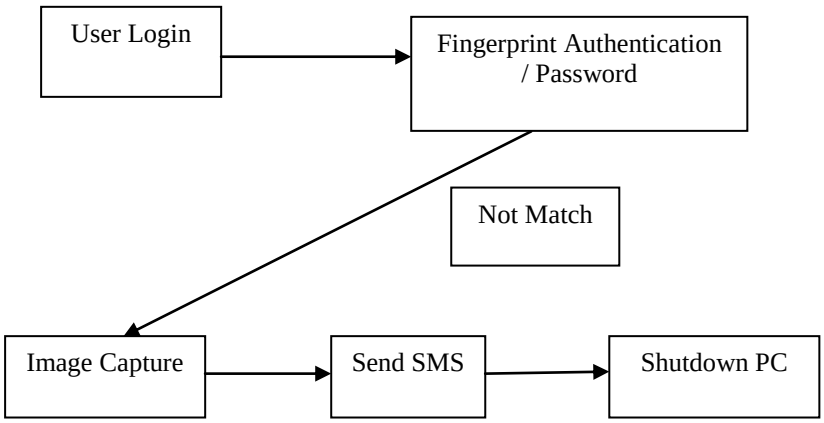

Figure 3 : Fingerprint Not Match

V. CONCLUSION

With the help of this desktop security provider can be said that project is a sincere effort to design and implement a digital diary that can be somewhat considered different from the run of the mill applications of similar nature.With the help of this system have learned a lot, especially about bit operations and bit masking, something that system never understood before. Desktop security provider was fun from the start and only got more interesting as system went on developing it. Desktop security became more interested in the subject the more we researched it. System have learned that while implementing screen recording is important, thinking of how to take screen shots and merge them into the video file with audio.There is a lot of research that is beginning to discover new ways to screen recording, most of which involves some variation of statistical analysis. Improvements to software are always possible. Similarly further improvements to this software can also be made. Providing the application's own website so that "Desktop Security Provider" can be accessed with ease on the Internet can also be tried out

REFERENCES

[1] Ashwini R. Patil, Mukesh A. Zaveri in, "A Novel Approach for Fingerprint Matching using Minutiae" have proposed effective fingerprint matching algorithm based on feature extraction.For minutia marking they considered one special false minutiae removal method.

[2] Chandra Bhan Pal, Amit Kumar Singh, Nitin, Amrit Kumar Agrawal in "An Efficient Multi Fingerprint Verification System Using Minutiae Extraction Technique" has combined many methods to build a minutia extractor and a minutia matcher.

[3] H B Kekre and V A Bharadi in "Fingerprint Core Point Detection Algorithm Using Orientation Field Based Multiple Features" have used Correlation based Fingerprint Recognition rather than detecting minutiae.

[4] Mary Lourde R and Dushyant Khosla in "Fingerprint Identification in Biometric Security Systems" proposed the issue of selection of an optimal algorithm for fingerprint matching in order to design a system that matches required specifications in performance and accuracy.

[5] Chomtip Pornpanomchai Apiradee Phaisitkulwiwat in,"Fingerprint recognition by Euclidean Distance" proposed the fingerprint recognition by Euclidean distance method.

[6] R. Vaishnavi , Jose Anand,R.Janarthanan, "Efficient Security for Desktop Data Grid using cryptographic protocol. International conference on "Control Automation, communication and energy conservation "-2009.

[7] Jayashree Baidya,Trina Saha, Ryad Moyashir, Rajesh Pali, "Design and implementation of a fingerprint based lock system for shared access",IEEE International Conference Annual Computing and Communications, January, 2017.

[8] Brown, Michael K., Stephen C. Glinski, Bernard P.Goldman, and Brian C. Schmult. "PhoneBrowser: A Web-Content-Programmable Speech Processing Platform." Position Paper for The W3C Workshop on Voice Browsers, Cambridge, MA (October 1998),Http://www.w3.org/Voice/1998/Workshop/Michael- Brown.html

[9] Cassell, J. "Embodied conversational interface agents"; Communications of the ACM 43, 4 (Apr. 2000), 70783. Danis, C. and Karat, J. "Technology-Driven Design of Speech Information Systems", Symposium on Designing Interactive Systems. ACM: New York (1995), 17-24.

[11] Ajinkya Kawale,"Fingerprint based locking system", International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013.

[12] Shivprasad Tavagad, Shivani Bhosale, Ajit Prakash Singh, Deepak Kumar ," Smart Surveillance System" , International Research Journal of Engineering and Technology, Volume: 03 Issue: 02 | Feb-2016.