International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 5 Issue 1 January 2018

A Hybrid Authentication System using Keystroke Security and Finger Print Identification for Mobile Cloud Environment

Shubham Sharma[1], Asst. Prof. Rasna Sharma [2]
RKDF School of Engineering, RGPV, Indore, MP, India[1, 2]
shubham.sharma883@gmail.com[1], rasna.sharma4@gmail.com[2]

Abstract: *The cloud servers and remote web servers are used to store the information and records for long term use and preservation of important data. These servers offer the security of the user data from the virus and others which affect the files and data normally in the personal computers or mobile devices. But these servers are not able to protect the user's unauthorized access to the server files. Therefore an authentication process which is assuring the actual user data access is required to design. In this presented work a new hybrid authentication process is proposed for design and implement that provide assure the data owner from unauthorized access. The proposed method includes the three different parameters of secure authentication namely user credential by using the user id and password. The user behavior credentials namely the typing speed and screen touch gesture and finally the biometric user identity namely the finger print. Before access the confidential data and files from the web server or cloud server the user required to verify their identity using these processes. This system is currently demonstrated for the mobile users which can be used for different other applications such as organizational confidential file access such as army and similar security agency. In order to implement the proposed technique the PHP technology and Android technology is used. Where the PHP is used for web service implementation and the Android mobile is used to provide the user interface. After the successfully implementation of the required system the performance of the system is measured which is also acceptable in terms of time and space complexity. Therefore the proposed technique is suitable to use in real world secure authentication mechanism design.***

Keywords: *Smart mobile, authentication, android mobile, biometric, keystroke.*

1. INTRODUCTION

In this generation the demand of computing is increases exponentially. Additionally a number of changes in hardware and software technologies are observed. Among them one of the frequently used device namely mobile devices are also changed in similar manner. The traditional mobile phones are become smart and mounted with a number of unique features such as touch screen, internet, sensors and others. In the similar fashion the utilization of these devices in a number of applications are performed. Due to these features a significant amount of sensitive and private data is also available in the mobile devices. Additionally the security or authentication features of these devices are not much satisfactory. Therefore, in this presented work the smart mobile devices and their unique features are studied, in addition of using these features a security or authentication application is proposed for development using android platform.

The proposed authentication technique is a multifactor device centric authentication scheme for android devices. Here the term multifactor indicates that the authentication involve the different aspects of the user behavior, device behavior and other device centric parameters for utilizing as the credentials of the authentication. In this context the device centric means the authentication is made for the specific mobile device. The proposed security technique analyzed the behavioral fluctuation of user and the device for providing access to use the system.

2. PROPOSED SOLUTION

This chapter provides the detailed explanation of the proposed multipurpose authentication model. Thus the chapter includes the system overview, the methodology of the system design and the proposed algorithm steps.

A. System Overview

Rapid development of technology also increases the need of computation. In last ten years the use of mobile phone is not limited to the normal voice communication that is enabled for various other computational tasks and other medium of communication. Now the mobile phone become smart phones and able to access internet services, installation and use of new applications, text and video messaging. All these activities require the computational ability of mobile devices as well as the storage requirements to the system. But due to size of mobile devices it is not feasible to store all the consumed data in one place. Therefore the additional storage requirements of mobile phones are increases. In order to fulfill this need to data owners the different cloud service and data hosting provides offers to host the data on their storage.

But it is not trust worthy enough to store the user's personal, confidential and sensitive information to third party hosting. Due to leakage of normal user credentials the unauthorized user can access the sensitive and private information of the user intentionally to harm someone socially and economically. Therefore there is a need to design a secure authentication technique that assure the data owner before accessing the confidential data from the third party hosting or cloud servers. In order to design such a strong authentication system the proposed work includes the three different phases of authentication. In first the user credentials are need to identify, then in next phase the user behavior is included for verification and finally the biometric identity is used for user verification. The three phase authentication model assures the user access and user claim. This section provides the basic aim of the proposed system and the overview of the proposed authentication model the next section includes the functional aspects of the proposed system.

B. Methodology

The figure 2.1 shows the system architecture for designing the secure authentication model. The system includes the two basic components first the web server or the cloud server and second user device.

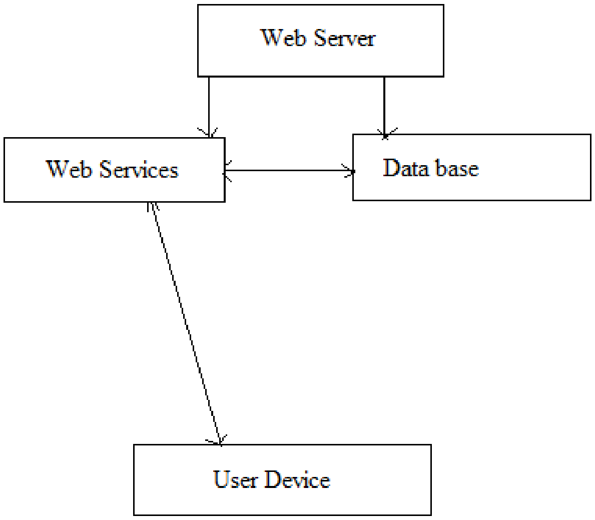

Figure 2.1 system architecture

Web server consists of a web service repository and the database. The web services are executed during the user request for new registration and authentication request. At the same time the web services utilizes the database which hosted in the web server for storing the data or retrieving the user information which is stored during the registration process. Second component contents the user interface and the processes of the web service call that executes the services remotely for verification and new user signup. After describing the basic client server architecture it is need to understand the process of user authentication. The user authentication process is described in figure 2.2.

Initially the system user interacts with the main screen which includes the login function of the system. if the user is not registered with the system then it is required to make registration first therefore first the registration process is described. After successfully registration with the system user can access the system by authentication process.

a. Registration Process

In order to register the user first a screen appears which contains the provision to provide the user id and password to the system. Both the credentials are used for basic authentication of user. Now the system provides a random string for input to the textbox and measuring the typing speed. To measure the typing speed the following formula is used:

$$Speed = \frac{T_{end} - T_{start}}{6000}$$

Where the T_{end} is the end time of the user typing and T_{Start} is the initial time of user starting the typing. The factor 6000 is used to convert the time difference into the seconds from the milliseconds.

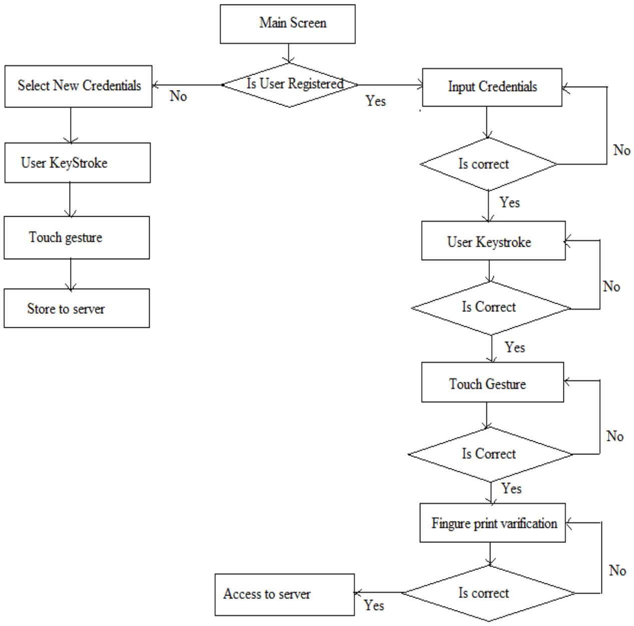

Figure 2.2 authentication flow chart

This speed of typing is preserved with the user id and password. In further a provision is made to compute the touch gesture. Here user touches the screen and the system detects the direction of screen touch. The user selected touch direction, user id, password and keystroke is stored in the database therefore a web service is called from server which carry all the information to server and make an entry to the server database. After the successfully registration user can initiate the authentication process.

b. Authentication Process

The next part of the figure 2.2 contains the authentication process of the system. Here first the user provides the user id and password for login to the system. If the user and password matched with the server stored user id and password then the next phase is called else error message is generated. In the next keystroke of the user is authenticated if the current key stroke speed and previous keystroke speed is matched then the system provide access to the next step. But practically no one can write the different text in same speed all the time. Thus a margin for typing speed is needed to implement. Thus a threshold value for this purpose is considered, in this experiment the threshold value is considered as 5 second. If the current typing speed is between the previous typing speed ± 5 then the system provide access otherwise need to retry for the same process. After the keystroke authentication the touch gesture is verified. In this context the user select the touch direction as the user previously provided during the registration if the direction of touch is verified then the system redirect the user to next phase where the finger print based authentication is take place is the biometric authentication is successful then user can access the files stored in the server.

This section provides the methodology of the authentication process and registration of new user. In next section the processes are summarized using the algorithm steps.

C. Proposed Algorithm

The table 2.1 includes the proposed algorithm for authentication that is the step procedure of the previously defined methodology.

Table 2.1 proposed algorithm

Input: user id U, password P, Keystroke speed K_s, gesture direction D, figure print P

Output: login success L

```
Process:
1. $V = CheckUserCredential(U, P)$
2. $if(V == true)$
      a. $S = Server.getUserTypingSpeed(U)$
      b. $if((S + 5) \leq K_s \leq (S - 5))$
            i. $S_D = Server.getDirecton(U)$
            ii. $if(D == S_D)$
                  1. $B = VarifyBioMatric(P)$
                  2. $if(B == true)$
                        a. L=success
                  3. Else
                        a. L = failed
                  4. End if
            iii. End if
      c. End if
3. End if
4. Return L
```

3. RESULT ANALYSIS

This chapter provides the evaluation details of the proposed multifactor authentication system based on keystroke dynamics and fingerprints. The experimental evaluation and the system performance is computed and demonstrated in this chapter. Therefore some essential performance parameters are obtained and listed with their obtained observations.

A. Memory Usage

The main memory required to process the algorithm is known as memory usages or space complexity of the system. When a user requests to the server for authentication then the process consumes some of space in system to perform task. By the following formula we can calculate memory usage of the system

$$\text{Memory Usage} = \text{Total Memory} - \text{Free Memory}$$

The figure 3.1 and table 3.1 shows the amount of main memory requirements according to different variation in authentication. To represent the performance X-axis contains the different login session for a single user authentication and Y-axis shows the amount of main memory consumed for process user authorization. The outcome of the developed mobile based authentication system is much adaptable for accessing of user control and verification of valid authenticity by fingerprint. The memory requirement of the system is varies when we figure out number of experiments of similar size of data but acceptable because it is not much increasing as if the amount of data.

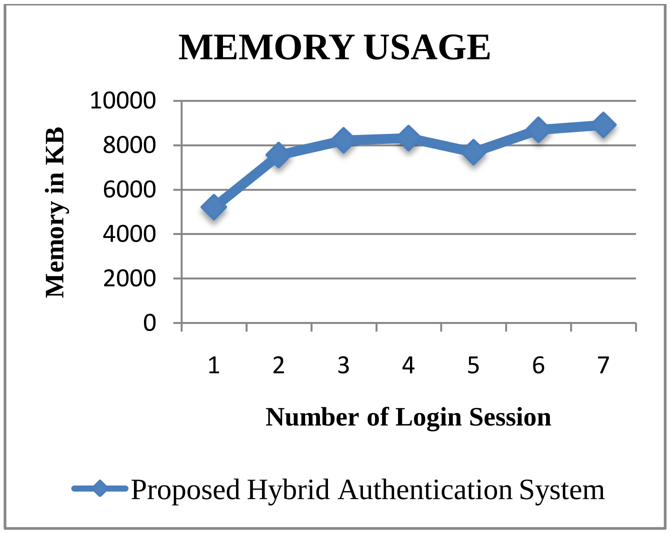

Figure 3.1 Memory Usage

Table 3.1: Numeric Values of Memory Usages

S. No.	Number of Login Session	Memory in KB
1	1st Login	5214
2	2nd Login	7556
3	3rd Login	8225
4	4th Login	8321
5	5th Login	7692
6	6th Login	8692
7	7th Login	8911

B. Time Consumption

In order to required time for processing the authentication processing using keystroke and fingerprint for designed hybrid authentication system is termed as time consumption. The time requirement of the algorithm is directly depends on the amount of data supplied for processing. This is also termed as the time complexity of the system

$$\text{Time Consumed} = \text{End Time} - \text{Start Time}$$

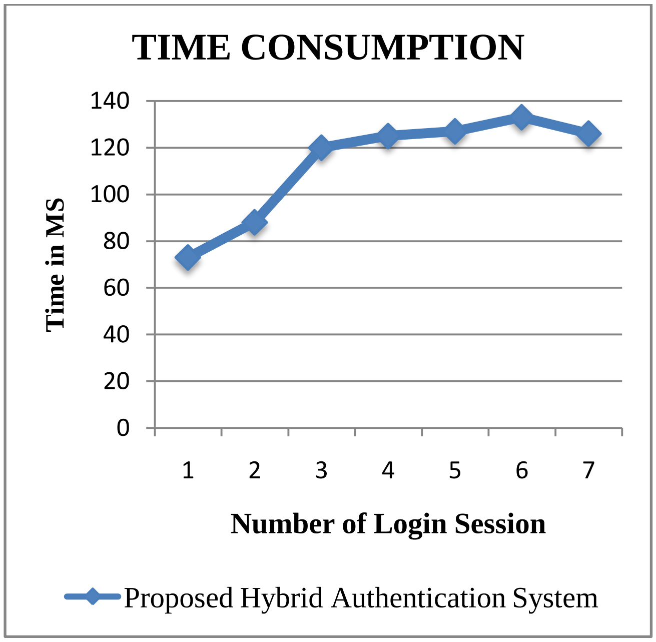

Figure 3.2 Time taken

Figure 3.2 and table 3.2 shows the time complexity or time taken to depiction of the system efficiency. In the given diagram the X axis contains the number of different login session and the Y axis shows the required time for processing the data during authentication process. The line graph demonstrates the different user login session consumed time whatever user validate or not. Additionally, blue line shows the proposed approach that represents the time consumption using designed algorithm.

Table 3.2 Numeric Values for Time taken

S. No.	Number of Login Session	Time in MS
1.	1st Login	73
2.	2nd Login	88
3.	3rd Login	120
4.	4th Login	125
5.	5th Login	127
6.	6th Login	133
7.	7th Login	126

C. Response Time

The response time is the amount of time which includes the total time required to get the response from the authentication server. Thus the response time starts with the initiation of user query, categorization single user access and getting outcomes to the user device.

Table 3.3 Numeric Values of Response Time

S. No.	Number of Login Session	Response Time in KB
1	1st Login	32
2	2nd Login	65
3	3rd Login	50
4	4th Login	82
5	5th Login	93
6	6th Login	45
7	7th Login	59

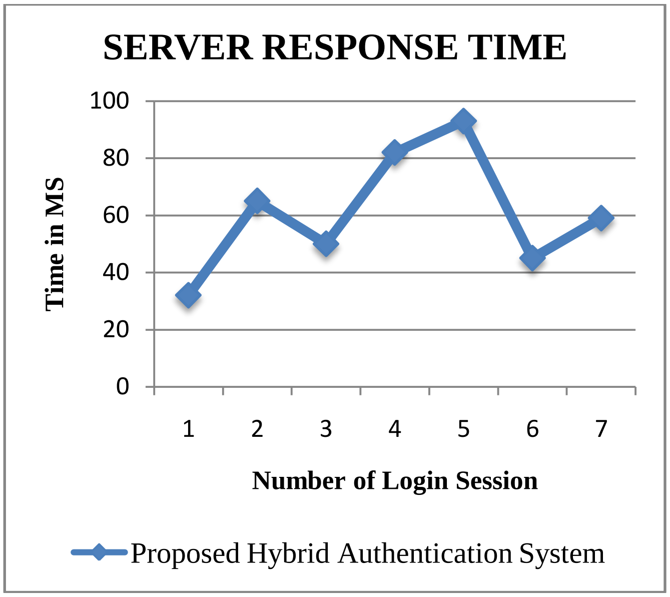

Figure 3.3 Response Time

The required server response of the proposed working model is computed and reported using figure 3.3 and the table 3.3. In order to represent the performance of the system the X axis of diagram contains number of login session and the Y axis shows the amount of time consumed during process. According to the measured outcomes the response time of the system is fluctuating and varies according to the work load on server system.

4. CONCLUSION

The proposed work is aimed to design and develop a secure authentication system using the user's behavior and biometric attributes. The implementation and design of the required technique is completed successfully. This chapter provides the summary of the entire work performed as conclusion of work and the future extension of the work is also included in this chapter.

A. Conclusion

Now in these days the usages of the computation and data storage units are increased in significant amount. Not only using the traditional computers the storage requirements of mobile devices are also increased. Mobile phones are mounted with the high definition camera and internet based applications therefore mobile phones also contains the confidential and private data on their storage. But the mobile phones are not much secure when the mobile phone is lost or stolen by someone. In order to provide solutions for such confidential data storage now in these days a number of mobile companies are offering the cryptographic cloud storage to their clients. This cryptographic cloud storage is a secure storage units and user can put their data on cloud. But to access and manage the data low or weak authentication mechanism is used which make vulnerable this cloud storage.

In this context the proposed work is aimed to design and develop a secure mobile authentication system which can be used for various applications for authorizing the user access. The proposed authentication technique a hybrid authentication model which consumes the user attributes as well as the biometric attribute to secure the user access to the server files. In order to design the authentication technique the two behavioral parameters namely user keystroke and the gesture is used and finally the user is verified by the user's biometric identity namely the finger print scan. The keystroke speed and pattern indicate the user's habit of using the mobile device, additionally most of the time a user can represent the similar behavior. In second parameter the gesture is used which need to be recognize the last pattern which is submitted to the data base. Finally the biometric identity of the user is provided to verify the user.

The implementation of the proposed technique is performed using the PHP based web service design and the Android smart mobile. In addition of that hosting the web service the Linux web server is utilized. After implementation of the proposed system the performance of the proposed authentication technique is evaluated and the obtained performance is concluded in the table 4.1.

Table 4.1 performance summary

S . No.	Parameters	Remark
1	Memory usages	The less amount of main memory required for executing the user parameter evaluation on server side scripts
2	Time complexity	The acceptable time delay is noticed for authentication process and parameter submission
3	Server response time	Low server response time observed for responding the user parameter submission

B. Future Work

The main aim of the work is accomplished successfully the designed approach is a promising approach due to high secure technique of user verification. In near future the following improvements and extension of the work is proposed for work.

1. The proposed work currently demonstrate the authentication module using web server in near future the technique is integrated with the real world application for securing the application access.
2. The proposed technique is currently usages the figure print verification method which is further extended to incorporate the face recognition based verification approach
3. The proposed system currently includes two user behavior parameters in near future more behavioral parameters are explored and implemented with the system.

REFERENCES

[1] Saini, Baljit Singh, Navdeep Kaur, and Kamaljit Singh Bhatia, "Keystroke dynamics based user authentication using numeric keypad", In Cloud Computing, Data Science & Engineering-Confluence, 2017 7th International Conference on, pp. 25-29, 2017.

[2] Venakatesan, N., and M. Rathan Kumar, "Finger print authentication for improved Cloud Security", International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), pp. 434-439, 2016.

[3] What is a smartphone? Available online at: https://www.digitalunite.com/guides/smartphones/what-is-a-smartphone

[4] "Smartphone", available online at: https://techterms.com/definition/smartphone

[5] "Introduction to Smartphones", Part 2, Tech Savvy Seniors.

[6] "Mobile Design and Development- the Evolution of Devices", https://www.safaribookson-line.com/library/view/mobile-design-and/9780596806231/ch01s02.html

[7] TechPluto Staff, "Characteristics of a SmartPhones", http://www.techpluto.com/smartphone-characteristics/

[8] T.S Sadham Hussain, Mr. M. Mohammed Sithik M.E, "An Identity based Batch Verification Scheme For Authentication Provision in VANETs", International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)Vol. 2, Issue 4, April 2016

[9] Talapa reddy Susmitha, Endela Ramesh Reddy, "Implementation of Security for Web Services Using of Trustee Based Authentications from User Friends", international journal & magazine of engineering and technology, management and research vol 2 (2015), issue no 8

[10] Gollmann, Dieter, "What is authentication?" In International Workshop on Security Protocols, pp. 65-72, Springer, Berlin, Heidelberg, 1999

[11] Tanuj Tiwari, Tanya Tiwari, and Sanjay Tiwari, "Biometrics Based User Authentication"

[12] Russell Kay, “Biometric Authentication”, available online at: https://www.computerworld.com/article/2556908/security0/biometric-authentication.html

[13] “Applications”, available online at: https://findbiometrics.com/applications/