IJCSMA

Shubham Sharma *et al*, International Journal of Computer Science and Mobile Applications,
Vol.6 Issue. 2, February- 2018, pg. 21-30 **ISSN: 2321-8363**
Impact Factor: 5.515

Combining Keystroke Security and Finger Print Identification for Mobile Based Secure Authentication System

Shubham Sharma[1], Rahul Sharma[2]

[1]*R.K.D.F School of Engineering, Indore (M.P), shubham.sharma883@gmail.com*

[2] *R.K.D.F School of Engineering, Indore (M.P), sharma.rahul5656@gmail.com*

Abstract

The servers are used to store the information for long term use and preservation of important data. The server secures user data from the virus and others. But these servers are not able to protect user's unauthorized access to the server files. Therefore an authentication process which is assuring the actual user data access is required. In this paper a hybrid authentication process is proposed that assures the data security by preventing unauthorized access. This method includes three parameters for secure authentication (i.e. user credential (user id and password), user behaviour credentials (typing speed and screen touch gesture) and finally biometric user identity (finger print). Before accessing confidential data and files from server user required to claim their identity through this processes. This system is developed for mobile users. In order to implement this technique, PHP technology and Android technology is used. The PHP is used for web service implementation and Android is used to provide the user interface for mobile devices. After implementation of system performance is measured in terms of time and space complexity. That is acceptable for security implementation on data access. Therefore the proposed technique is suitable to use in real world applications.

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

1. Introduction

The demand of computing is increasing exponentially; a number of new hardware and software technologies are introduced in recent years. Among them smart mobile devices is also one of the rapidly changing technologies. The mobile phones are becoming smart and involving a number of unique features i.e. touch screen, internet, and others. Due to these features and abilities a significant amount of sensitive and private data is preserved in mobile devices. But anyone can access the mobile data if mobile is lost therefore these devices are not much satisfactory for securing the private data. In this presented work 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 behaviour, device behaviour and other device centric parameters for utilizing as the credentials of the authentication. These parameters are to help identify the end mobile user by using their behaviour and activities with the mobile phones. In this context the device centric means the authentication is made for the specific mobile device. In addition of that when mobile is lost and user want to recover data user do this using other mobile too. The proposed security technique analyzed the behavioural fluctuation of user and the device for providing access to use the system. This behavioural analysis technique for securing data over server is helpful for various other applications and authentication systems. This section the overview of required system is provided in next section the detailed methodology of system design is presented.

2. PROPOSED SOLUTION

This section provides detailed explanation of proposed authentication model. Thus it includes system overview, methodology and the proposed algorithm.

2.1 System Overview

Development of technology also increases needs of computation in recent years use of mobile phone is not limited it is extended for other computational tasks. Therefore mobile phones become smart phones and able to access internet services, installation and use of new applications, text and video messaging. All these activities require computational ability as well as storage to system. Due to size of mobile devices it is not feasible to store all data in one place. In order to fulfil this need of data different internet service provides offers to host 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 unauthorized user can access the sensitive and private information. Additionally someone harm the user socially and economically. Therefore a secure authentication technique that assures the data owner before accessing confidential data from the third party hosting is required. To design such a strong authentication system proposed work includes three phases of authentication. In first the user credentials are required to identify, in next phase user behaviour is included for verification and finally biometric identity is used. The three phase authentication model assures user access and user claim.

2.2 Methodology

The figure 1 shows system architecture for designing the secure authentication model. The system includes the two basic components first the web server or actual server and second user device.

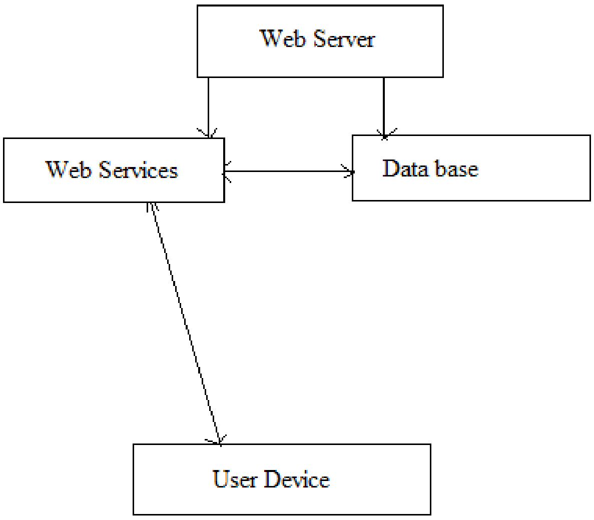

Figure 1: system architecture

Web server includes a web service repository and database. The web services are executed during user request such as new registration and authentication request. At the same time the web services utilizes database for storing data or retrieving the user information. Second component contents user interface and processes of web service call. 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. Initially the user interacts with main screen which includes login function if user is not registered with system then it is required to make registration first therefore first registration process is described. After successfully registration with the system user can access the system by authentication process.

Registration Process

In order to register user a provision is made to provide the user id and password. Both credentials are used for basic authentication of user. Now the system provides a random string for input to textbox and measuring typing speed. To measure typing speed 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.

This speed of typing is preserved with user id and password. A provision is made to compute touch gesture. Here user touches screen and system detects 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.

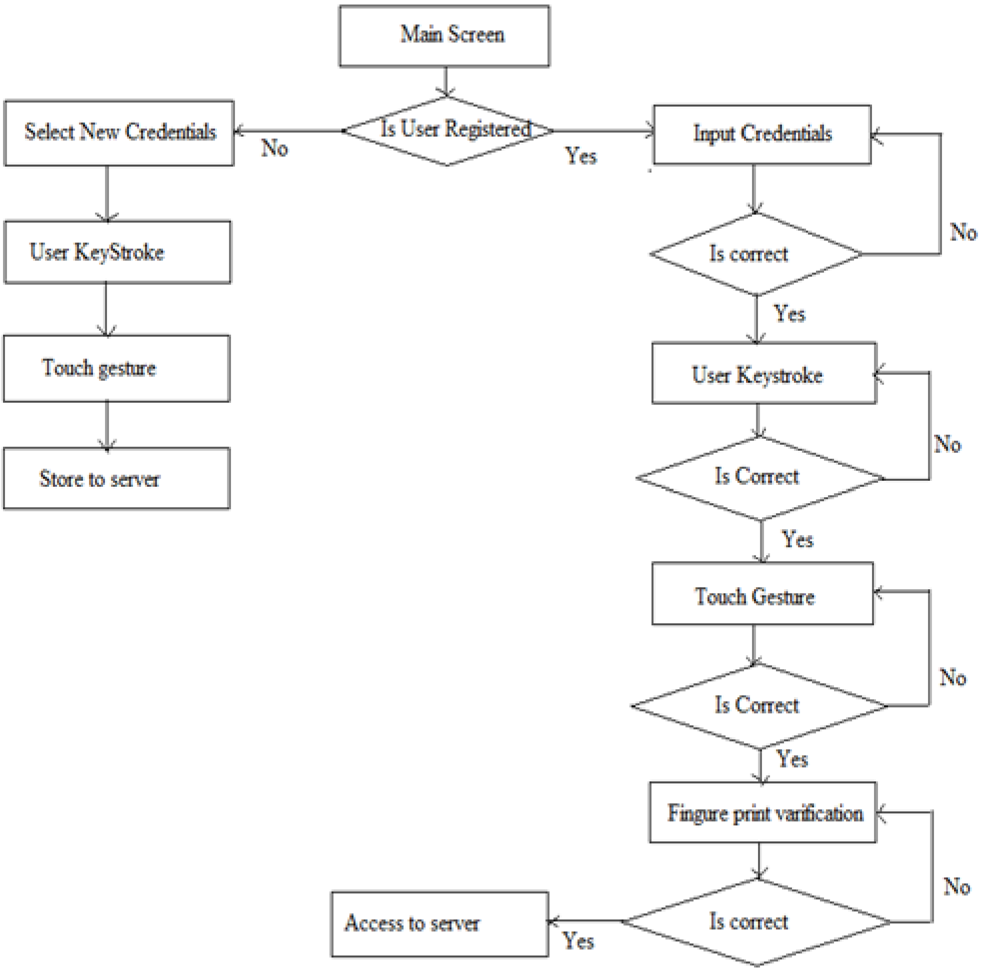

Figure 2: Registration and login process

Authentication Process

The next part of the figure 2 shows authentication process. The user provides user id and password for login. If user id and password matched with server stored user id and password then next phase is called else error message is generated. In the next keystroke of user is authenticated. 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. A threshold value for this purpose is considered, the threshold value is considered as 5 second. If current typing speed is between previous typing speed ±5 then system provide access otherwise need to retry. Afte keystroke authentication touch gesture is verified. The user select touch direction as user previously provided if direction of touch is verified then system redirect user to next phase where the finger print based authentication is take place. That is the biometric authentication is successful then user can access the files stored in server.

2.3 Proposed Algorithm

The table 1 includes the proposed algorithm for authentication that is the step procedure of the previously defined methodology.

Table 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. $if\big((S+5) \leq K_s \leq (S-5)\big)$
            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 section provides evaluation of proposed authentication system. The experimental evaluation and performance is computed and demonstrated here. Therefore some essential performance parameters are obtained and listed with obtained observations.

3.1 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 and table 2 shows amount of main memory requirements according to different variation in authentication. To represent performance X-axis contains different login session and Y-axis shows amount of main memory consumed. The outcome of developed mobile based authentication system is adaptable for accessing of user control and verification. The memory requirement of system is varies when we figure out number of experiments of similar size of data but acceptable because it is not much increasing.

Table 2: 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

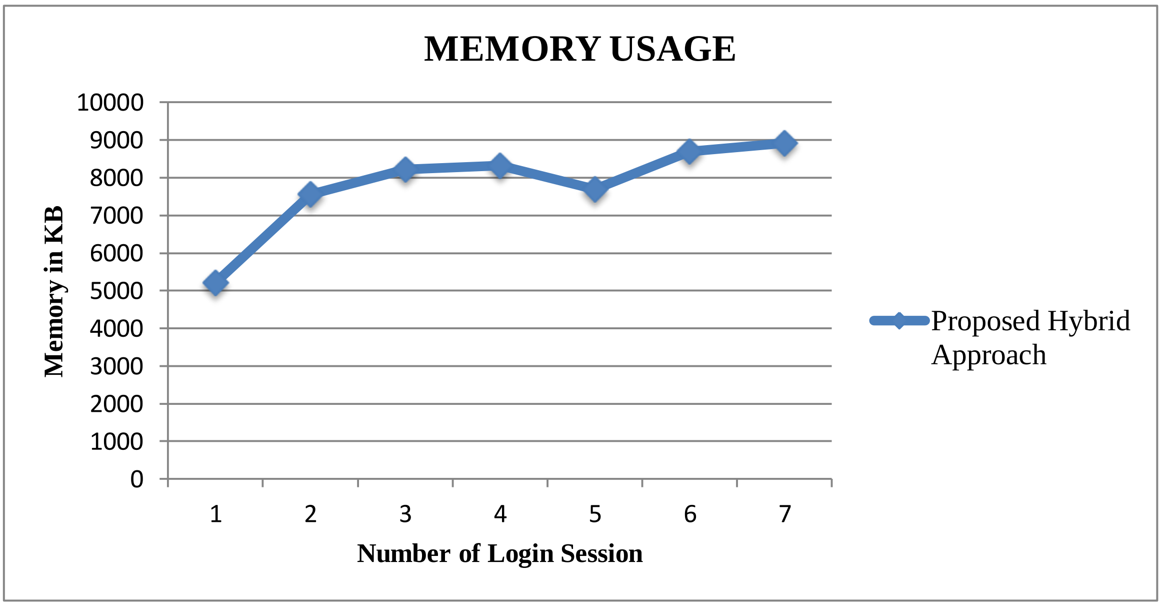

Figure 3: Memory Usage

3.2 Time Consumption

Required time for processing authentication request 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 time complexity of the system

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

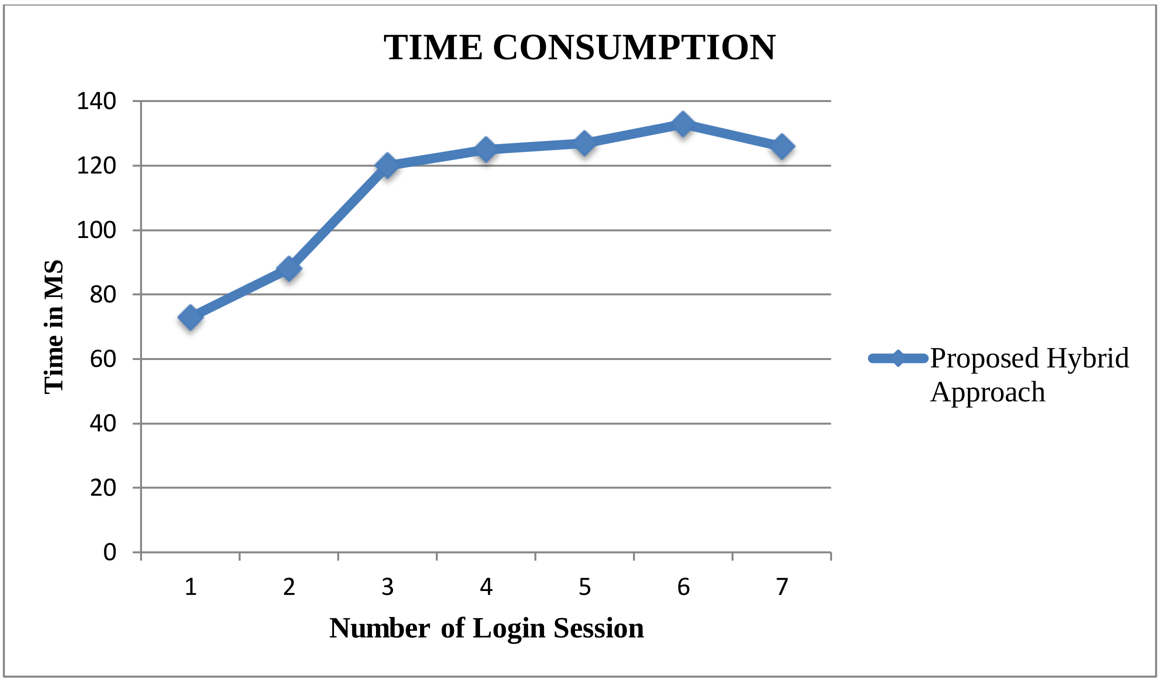

Figure 4: Time taken

Figure 4 and table 3 shows time complexity to depiction of system efficiency. In given diagram X axis contains number of different login session and Y axis shows required time for processing the authentication process. The X axis of line graph demonstrates different user login session consumed time whatever user validate or not. Additionally, blue line shows proposed approach that represents time consumption using algorithm.

Table 3: 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

After generated above two parameter result namely, time and memory now we are giving another two results with comparative analysis using FAR and FRR on the basis of input dataset. In this manner we used dataset i.e. "DSL-StrongPasswordData". Different metrics can be used to rate performance of a biometric factor, solution or application. The most common performance metrics are **False Acceptance Rate (FAR)** and (**False Rejection Rate) FRR**.

3.3 False Accept Rate (FAR)

The FAR or False Acceptance rate is likelihood that framework mistakenly approves a non-approved individual, due to inaccurately coordinating biometric contribution with a format. FAR is typically known as a rate, following the FAR definition this is the level of invalid sources of info which are inaccurately acknowledged. The False Accept Rate can be calculated using following formula:

$$\text{FAR} = \frac{\text{Wrongly Accepted Individual}}{\text{Total Number of Wrong Matching}}$$

Table 4 Numeric Values for FAR

S. No.	Number of Login Session	Proposed Hybrid Approach	Old Approach
1.	1st Login	4.3	6
2.	2nd Login	4	5.4
3.	3rd Login	4	4.3
4.	4th Login	3.2	5.4
5.	5th Login	2.9	3.4
6.	6th Login	3	3.8
7.	7th Login	3.3	4.3

In this figure 5 shows false accept rate of both proposed and old approach. Here Blue line show the proposed hybrid approach and red line depicts the old approach. Here table 4 also show numeric values in tabular format. Therefore, above graph demonstrate the FAR values for both old and proposed system on different experiments. According to proposed generated result FAR is lower than the comparable to the old approach.

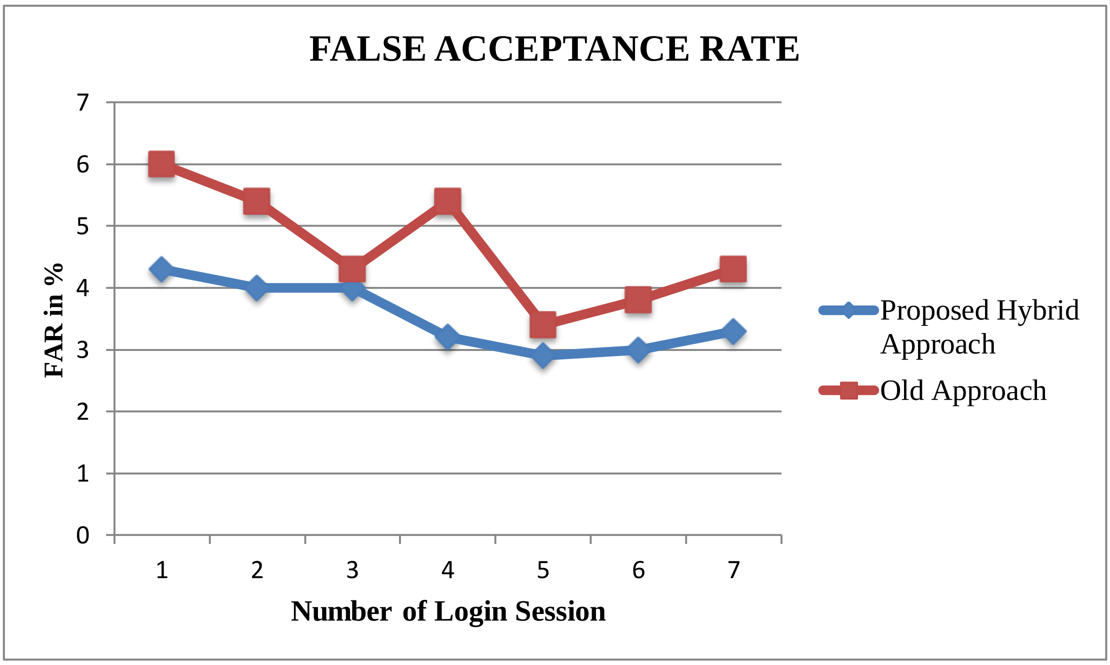

Figure 5: False Acceptance Rate

3.4 False Reject Rate (FRR)

The FRR or then again False Rejection Rate is the likelihood that the framework erroneously rejects access to an approved individual, because of neglecting to coordinate the biometric contribution with a format. The FRR is ordinarily communicated as a rate, following the FRR definition this is the level of legitimate information sources which are inaccurately dismissed. FRR can be estimated by using following formula:

$$\text{FAR} = \frac{\text{Wrongly Rejected Individual}}{\text{Total Number of Correct Matching}}$$

The multiple attempts done with the system to enrol or getting rejected is measured by false rejection rate. In figure 6, we show the false rejection rate for both approaches. Additionally, FRR is measured in amount of %. Also FRR numeric value demonstrated in tabular form in table 5. In above graph, x-axis shows number of session login where as y-axis depicts the amount of false rejection rate. There False rejection rate in proposed system is lower than the old approach.

Table 5: Numeric Values for FRR

S. No.	Number of Login Session	Proposed Hybrid Approach	Old Approach
1.	1st Login	60.3	79.5
2.	2nd Login	54.3	69.7
3.	3rd Login	45.2	58.5
4.	4th Login	40.9	54.2
5.	5th Login	50.6	65.7
6.	6th Login	35.6	62.7
7.	7th Login	40.8	51.4

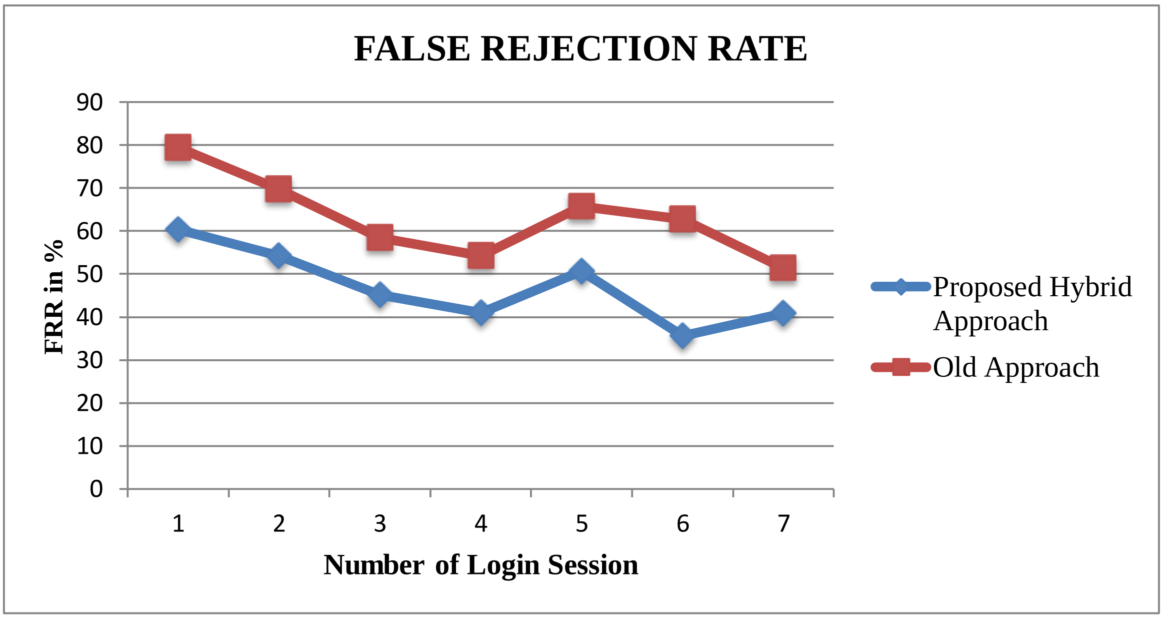

Figure 6: False Rejection Rate

4. Conclusion

The proposed work is aimed to design and develop a secure authentication system using user's behaviour and biometric attributes. The implementation and of required technique is completed successfully. This section provides summary of entire work performed and future extension of work is also included.

4.1 Conclusion

Mobile phones are mounted with the high definition camera and internet based applications therefore mobile phones contains confidential and private data on storage. But mobile phones are not much secure when the mobile phone is lost or stolen. To provide solutions for such confidential data storage a number of mobile companies are offering cryptographic storage. This cryptographic storage is a secure storage and user can put their data on servers. But to access and manage data low or weak authentication mechanism is used. In this context proposed work is aimed to design and develop a secure mobile authentication system. The proposed authentication technique is a hybrid authentication model which consumes user attributes as well as biometric attribute to secure user access. To design authentication technique two behavioural parameters namely user keystroke and gesture is used and finally user is verified by user's biometric identity namely finger print. The keystroke speed and pattern indicate user's habit of using mobile device, additionally most of time a user can represent the similar behaviour. In second parameter gesture is used which need to be recognize last pattern which is submitted to data base. Finally biometric identity of user is provided to verify user. The implementation of proposed technique is performed using PHP based web service and Android mobile. In addition of that hosting of web service Linux web server is used. After implementation the performance of proposed authentication technique is evaluated and obtained performance is concluded in table 7.

Table 7: 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

4.2 Future Work

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 behaviour parameters in near future more behavioural 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/bio metric-authentication.html

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