AN INNOVATIVE APPROACH FOR USER VALIDATION SYSTEM USING
KEYLOG AND SUDOKU ALGORITHM

D. Gopika*, P J Kumar
School of Information Technology and Engineering(SITE), VIT University, Vellore, Tamilnadu, India.
Assistant Prof. [Sel.Grade], School of Information Technology and Engineering (SITE),
VIT University, Vellore, Tamilnadu, India.
Email: Gopikablue18@gmail.com

Received on 20-04-2016
Accepted on 24-05-2016

Abstract

Brute force and word reference assaults on secret key are currently across the board and perpetually expanding. Enabling suitable login for legitimate clients while averting such assaults is a troublesome issue. If such assaults happens, bonafide client is ignorant of their verification data is being uncovered. We propose a framework that validates a client in two levels. The main level uses neighbourly key logging instrument for confirmation and second level uses Sudoku based secret key for accepting the proper client where the client PIN is never uncovered.

Keywords: Keylog, Sudoku Based secret word, Assaults, PIN.

1. Introduction

Web is a spot where the vast majority of our lives have been contributed. Our privileged insights, learning and everything are in one huge innovation called Internet. From advanced science to basic undertakings, the web is assuming its significant part. Very nearly everybody needs to utilize this innovation and actually it turns into a key fixing in our lives.

So there is a essential requirement for securing and controlling this innovation in current trend. In Internet all our data is secured by an element called Secret word. Secret words can be anything until it approves substantial clients. There are a few types of secret key existing, for example, content, design, movement, biometrics and so on., and normal qualities among them is their level of security.

Every single secret key has own security calculations for approval. These calculations are developed in a manner that it avoids the vast majority of the security assaults. Currently security in websites are very essential because issues of shoulder surfing are increasing day by day affecting the clients and making them insecure about their secret word usage over the internet [1].
2. Recent Work

The Existing framework concentrates on cryptography and secret word quality instrument for shielding client's data. Existing recommendations additionally focuses on number of login trials produced using known and illegitimate clients[1]. Constant verification methodology is grounded on straightforward securing of biometric information and on versatile timeout administration for confirmation of trusted clients[2]. Utilization of Biometrics for validation can't be exceptionally helpful for ordinary clients since it requires extraordinary Biometric gadget[3]. The outline guideline of oPass is to dispose of the negative impact of human elements however much as could reasonably be expected. Through oPass, every client just needs to recall a longterm secret word which has been utilized to ensure their phone. Clients are free from writing any secret words into untrusted PCs for login on all sites[4]. The 3-D secret key is a multifaceted validation plan. The grouping of activities and cooperations of the client tends to the 3-D environment in developing the client's 3-D secret key[5].

3. System Architecture

In our framework we utilized two calculations that are built to anticipate Brute Force Attacks, Dictionary Attacks, Secret word Guessing and Shoulder Sniffing. Sometimes our calculations make these assaults more mind boggling to the Hackers. The complete construction modelling of our framework is appeared as Level 1 and Level 2. The Architecture includes two levels of acceptance. At first every client experiences enlistment process where they select username and secret key. A secret word determination, the Keylog Secret word is acquired. After effective enrollment, a 3 digits PIN number is given to each client. The principal level accepts client character by method for routine username and secret key alongside the Keylog Secret word. The Keylog Secret word is obtained from each keystrokes made by the client. These Keystrokes are obtained as a bunch of particular ASCII values and maintained in the database. In spite of the fact that the Keylog Secret word is acquired at first, it is accepted after the second level approval. This later acceptance gives an extra security and perplexity to the illegal access. The second level accepts client personality utilizing 3x3 Sudoku. This 3x3 Sudoku is produced alongside 3 digits Sequence Location number is generated. The client needs to outline number in the PIN with 3x3Sudoku at suitable Sequence Location. A mid mapping, the relating line and section area of every number is entered as Sequence Number. Here the PIN number is not uncovered as we just enter the Sequence Number. Fitting PIN is decoded from Sequence Number. This decoded PIN is accepted against the PIN in the database.
At last the Keylog Secret word is accepted to confirm the client. Subsequently the client picks up their client session after two levels of security that involves the acceptance process.

4. Methodology

The proposed framework validates a client in two layers. The principal layer uses amicable key logging component for verification which eliminates the secret key speculating assaults and the second layer uses 3X3 Sudoku to get indirect secret word from the client by mapping the Sudoku showed and the pin is approved with the client pin in the database.

System utilizes inviting key logging system for validation where key strokes by client are found during secret key entering time. System abstains from utilizing outside gadgets and assets, for example, SMS, Mobile Phone, Biometric
gadgets. System improves security by not tolerating client PIN specifically but rather through Sudoku designs. 3x3 Sudoku and Sequence Location are created uniquely each time a user login the system.

4.1 Implementation of Algorithm

4.1.1 Keylog Based Secret word

The client need to purposely enter the wrong secret key (Keylog secret word) trailed by the right secret word by deleting every character. A script will indirectly track the user keyboard strokes and the correct secret word which is entered. Hence the script will track both Keylog secret word and correct secret word the right secret key is accepted in first level and the Keylog secret word is approved after second level.

```
function myKeyPress(e)
{
  if(window.event) // IE
    keynum = e.keyCode;
  if(keynum != '0')
    {
      words[i]=keynum;
      i++;
    }
  }
else if(e.which) // Netscape/Firefox/Opera
  keynum = e.which;
  if(keynum != '0')
    {
      words[i]=keynum;
      i++;
    }
result = words.join(".");
}
```

Subroutine for keylog based secret word

4.1.2 Sudoku Based Secret word

In Sudoku based secret word client will need to enter a succession number from a Sudoku taking into account the produced grouping area. The clients need to effectively outline PIN on the 3x3 Sudoku and enter the relating line and section number. This line and section number is called Sequence number which unravels the client pin. The decoded pin is approved with the client pin put away in the database.

Given :Sequence Location k

3-digit value as (k0,k1,k2)

Sudoku as 9 (3*3)matrix is generated for the client to enter the secret word . Sudoku is generated randomly each time a client tries to a operate in the authentication system.
The above depicted 3X3 sample matrix involves randomly generated numbers from 1 to 9 without the usage of 0. The main reason for avoiding 0 in our project is because none of the PIN codes includes the value 0.

**Fig 2.** Sample 3X3 matrix.

5. **Survey Analysis**

As per the survey analysis for the trend of shoulder surfing it is reported to be mostly used by the criminals (40%). Most of the crimes of these days that happened in the ATM s followed the strategy of shoulder surfing where the cameras of ATM s are being watched by the criminals to identify the secret PIN of the legitimate user. Hackers (38%) so called wifi freaks are users who wantedly perform such activities for checking their ability on hacking skills. There are possibility that they also are also involved in such activities of crimes.

**Fig 3.** Graphical representation survey analysis.
Normal users (22%) who just as perform it for fun and time pass. They just do it so as to show they can do anything in excitement.

5.1 Performance Analysis

The keylog and Sudoku based secret word seemed to provide the result with time complexity to be Constant. Similarly the space complexity is also constant with the N elements. In our Sudoku algorithm time complexity for searching element is O(n²).

6. Results

![Fig 4: User Login Webpage.](image)

![Fig 5: User Login Page.](image)
7. Conclusion and Future Enhancements

In the proposed framework that approves the appropriate enrolled clients to enter the client session for authentication. There are two levels of security in particular key log based and Sudoku based secret key which stays away from security attacks for example, Brute Force assault, Dictionary assault, Password Guessing assault and Shoulder Sniffing assaults. This security calculation has numerous applications, for example, Bank, Education, E-Booking and others because of its adaptable nature. Later on, framework can be improved by enhancing safety by sending the client pin which is created during client registration time and sent to their Email or mobile number. Framework can progressively change the secret word in the database which makes the client extremely secure subsequent to the secret word changes in general interval of time.

References

1. Revisiting Defenses against Large-Scale Online password Guessing Attacks by Mansour Alsaleh, Mohammad Mannan, and P.C. van Oorschot, IEEE transactions on dependable and secure computing, vol. 9, no. 1, january/february 2012.


5. Three-Dimensional password for More Secure Authentication Fawaz A. Alsulaiman and Abdulkotaleb El Saddik, Senior Member, IEEE transactions on instrumentation and measurement, vol. 57, no. 9, september 2008.


**Corresponding Author:**

D.Gopika,*

**Email:** Gopikablue18@gmail.com