International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 07 | -2016 www.irjet.net p-ISSN: 2395-0072

Implementation and Performance Analysis of a Strong Bi-Factor Re-Authentication Technique in Cloud Environment

Jyotika Chhetiza[1], Nagendra Kumar[2]

[1]*Jyotika Chhetiza, CSE Department, Shri Ram Institute of Science and Technology, Jabalpur, India*
[2]*Nagendra Kumar, CSE Department, Shri Ram Institute of Science and Technology, Jabalpur, India*

Abstract - *There has been continuously inclination towards the practice of multi-factor authentication (MFA) mechanisms due to the security infringements episodes happening lately with the use of single factor authentication services. As contemporary hand held computing apparatus such as smart phones are widely available, used and share a big chunk of the computational devices market, these MFA mechanisms should be available on such smart devices. Moreover, ubiquitous nature and high social acceptability has drawn the attention of the businesses to offer their services on such smart devices. In this aspect, the biggest challenge for these firms is to assure the privacy and security of the users. For accosting this concern, we deploy and perform analysis of a verification system named Bi-Factor Re-Authentication (BFRA) paradigm that league human possession factor (OTP and Login Key) with staple knowledge factor (user specific names, passwords and answer to secret questions) along with implementation of a technique to prevent bots from logging in, to attain an advanced security feature. The major reckoning payload of the precedent work is Trans located on a cloud-based application server so that this verification becomes unconstrained of platform and is accessed pervasively. Custom application is built for the Android based devices which are linked with the cloud based two factor authentication (TFA) server.*

Key Words: **Multi-factor authentication (MFA), Security, Privacy, Bi-Factor Re-Authentication (BFRA), Human possession factor, Staple knowledge factor, two factor authentication (TFA)**

1. INTRODUCTION

Now-a-days, with the growing momentum towards internet technology and ubiquitous computing, distant or remote access to private networks and services is becoming a distinctive trait of enterprises. These advances in technology have facilitated both the firms and their consumers or targeted client groups. Gartner, in a recent report, assessed that the user authentication services used by the firms will contribute to be around 50% when compared to 10% as of today [1]. However, the correlated security challenges akin to use authentication and safety of personal data have opened new gates for malignant activities. The rising requirement is to present improved security solutions that could efficiently cater for the probable risks and potholes threatening security of smartphone users.

It is risky idea to use fixed passwords for user authentication. There have been several instances where the passwords and conventional security measures have been compromised. Hence, the latest trend is to shift towards Multifactor Authentication, which is highly rugged to security rift and identity frauds. US Federal Financial Institutions Examination Council (FFIEC) acclaims the banks to custom Two-factor Authentication, to direct and supervise fiscal proceedings [2]. The user details existent for remote validation as factors considers one time keys, biometric features, hardware authenticators and digital certificates. In our proposed work, we propose to use knowledge factor and possession factor as our authentication aspect in combination with mobile cloud computing concepts for high-level security.

Any type of authentication may authorize access, but using two types and multiple combinations of factors works to fulfill the concept of stronger security, authentication and non-repudiation, not only we can validate the identity and gain access to a resource, but we cannot contravene doing it sometimes later.

2. RELATED WORK

Use of fixed passwords for user authentication is now an unreliable task. This is very well verified from the recent episodes of security breaches faced by large enterprises. In June 2012, around 6.5 million SHA1 hashed LinkedIn passwords were disclosed [4]. Since October 2012, Dropbox started using two factor authentication after it was attacked by hackers in July 2012 [5]. In 2014, all large enterprises such as Twitter, Skype, New York Times and Wall Street Journal faced security breaches [6]. Finally, complete content and organizational editing before formatting.

In order to make safer access for cloud, numerous researches have been completed over authentication and its various mechanisms. The security breaches have become more imaginative than before due to the ever growing internet data. S.H Khan et al. devised an authentication mechanism connecting human inherence factor with standard knowledge factor [7]. Algorithms used were feature extraction, signature matching system and distant measurement. Wenyi Liu et al. carried out a privacy

preserving multifactor authentication technique based on multiple accesses with collision avoidance algorithm [8]. Jiangshan Yu et al. upgraded the two factor mechanism into developing a three factor mechanism in which a fingerprint based fuzzy vault system [9]. Couple of other techniques such as graphical authentication, single sign on, usage of smart cards, key stroke analysis and biometric features have been previously implemented so as to provide secure assess.

Our Proposed system - Cloud based Bi-Factor Re-Authentication Paradigm

While logging in for cloud we take into consideration, three phases as the core of the system. They are Registration phase, Authentication phase and key generation phase, as described in the figure 2 below.

The three phases are explained below:

1. BFRA Registration phase: This is a mandatory step for further logins in cloud and saving required files as well. This step requires the filling of a sign up form through which the details and necessary credentials for further login are collected.

- The information and data to be collected is desired username, password, phone number and IMEI number.
- On successful sign-up, an anonymous id/OTP will be generated verifying the user's identity which will be delivered on user's registered mobile number.
- This one time pass-code is necessary for the next login; hence it is not meant to be deleted and kept safe as a message.
- Once the user registers he/she enters into the main page where one can add personal data and view the profile's information.

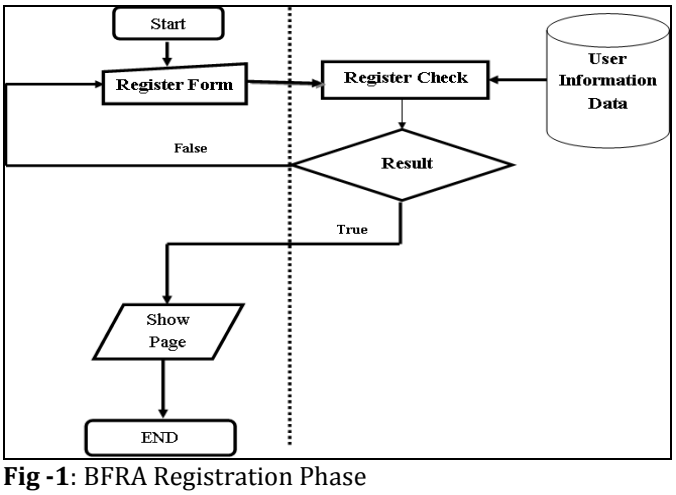

Fig -1: BFRA Registration Phase

Algorithm_Register
Request user registration;
If user-registration is true
Input user's information into Database;
Initialize first seed;
Implement MD5;
Activate userID;
Else
Return user-registration;

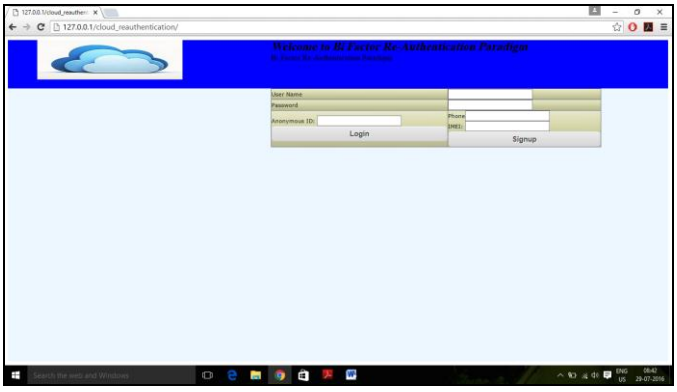

Fig -2: Registration Phase

2. Authentication phase: In this step, we ensure re-authentication each time a user logs in.

- This includes the OTP to be entered (OTP generation is explained in Key generation phase), which takes SIM as a parameter and will be delivered to user's phone as a message.
- This one time pass-code is already given to user during the previous login and is kept safe as message.
- Once the user logs in using password and an OTP, the main page displays a dialog box appearing periodically at random time values asking to perform certain mathematical calculations or answer to secret question or code to be entered from phone.
- This code is generated by an android SMS API service and is based on phone's IMEI number. This periodic entrance of code fetched from phone typically ensures an account's security if a person breaks from a session without logging out.

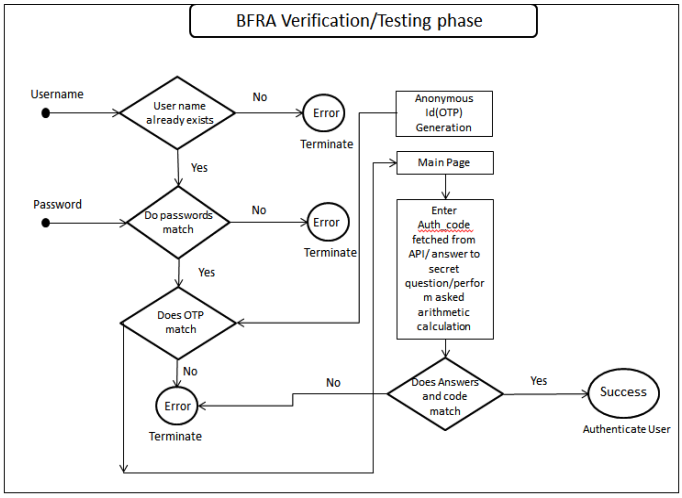

Fig -3: BFRA Authentication Phase

Request login authentication;
If login authentication is true
get session user time;
get session user phone;
get session user's initial seed;
initialize Gold_code algorithm;
generate OTP;
store OTP in database;
initialize sms service;
Goto mainpage;
Enter Auth_code;
Add User information;
Access Data;
else
return login authentication;

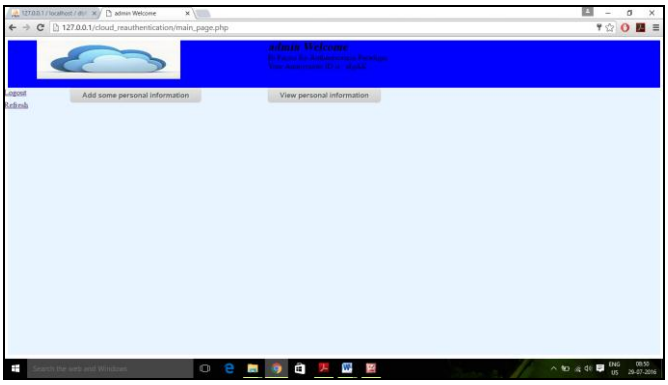

Fig -4: Main Page displaying Anonymous ID

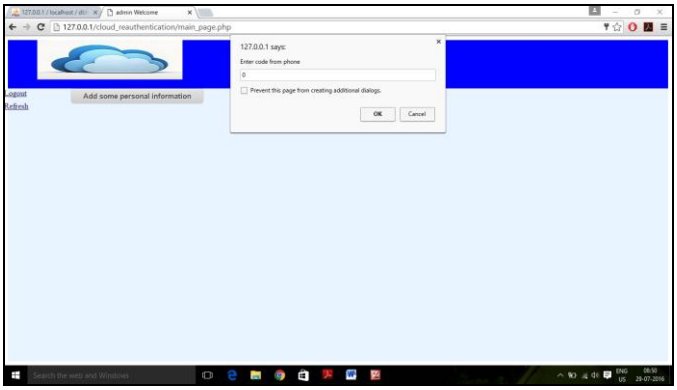

Fig -5: Dialog box to enter code fetched from API

3. Key generation phase: The anonymous ID (OTP) and Authentication Code (Auth_code) are the most essential aspect of our bi-factor scheme. For OTP to be received on the registered phone number, we need to develop an SMS-API which will interact with cloud to send it as a message. Also, when the user registers his/her phone's IMEI number, the secret Auth_code will be fetched from the same android service to be entered on the cloud interface. Key generation phase is a sub-realm of authentication in mobile cloud computing framework [3].

- **Implementation of Gold Code Sequences**: For the generation of our anonymous id each time for next login and the Auth_code, we implemented the concepts of gold codes [10]. Gold codes are an array of specific arrangements found in systems applying spread spectrum or code-division multiple access (CDMA) mechanisms. These systems are generally used in communications devices such as global positioning systems (GPS), cellular telephones and Very Small Aperture Satellite Terminals (VSATS). Gold codes have cross-correlation properties indispensable in a multi-user environment, where one code must be distinguished from many other codes prevalent in the same spectrum.

- **Pseudorandom Noise (PN) Sequences**: PN sequences are a streak of 0's and 1's which short come any palpable pattern and look statistically autonomous and consistently scattered. The arrays are deterministic, but display noise properties akin to randomness. The PN sequence generator is usually comprised of shift rosters with feedback. By linearly connecting aspects from taps of the shift register and supplying them back to the start of the generator, one could collect the arrangement of much deeper repetitive breadth using the equal number of lag elements in the shift register. Hence, these sections are also referred to as linear feedback shift registers (LFSR). The length of the shift register, the number of taps and their locations in the LFSR are critical to generate PN sequences with enticing auto correlation and cross correlation properties.

- **Scrambling Codes in CDMA**: Amid the spreading process, CDMA disburses the signal across the integrated frequency spectrum by connecting the data signal with a scrambling code which is sovereign of the transmitted signal. In a multi-path surrounding, each addressee is accredited an exclusive scrambling code. The correlation property of these codes makes it achievable to develop a division between the signals, which permits the varied paths to be interpreted by the recipient.

The scrambling codes adopted in 3G CDMA wireless systems are based on "Gold" codes. Gold codes are achieved by connecting two PN sequences and modulo-2 adding or ZORing, the output together. These codes have precise cross-correlation properties, to grant as many users as achievable, with least possible obstruction.

Working with a set of polynomials, you can create the PN sequences (also known as m-sequences). This reference design makes use of definitive primeval polynomials over Galois Filed 2 (GF[2]) as characterized in the 3rd Generation Partnership Project (3GPP) Technical Specification 25.213.

The x-arrangement uses the following polynomial:
X25 + X3 + 1

The y-arrangement uses the following polynomial:
X25 + X3 + X2 + X + 1

The specifications require the use of 25-stage LFSRs.

The concluding outcome is a lengthy scrambling code, Clong, 1n and Clong, 2n, developed by adding (using modulo-two addition) the outputs of two PN code sequence generators.

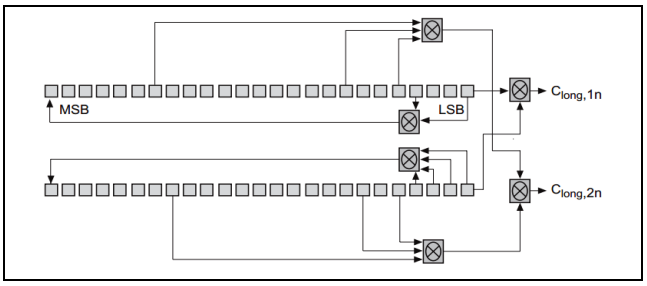

Fig -6: Long scrambling codes

Fig -7: SMS API for IMEI Display and Auth_code fetching

3. PERFORMANCE ANALYSIS AND RESULTS

In our proposed work, the main test cases are used in order to validate the user who wants to access the system. For accessing the proposed system the user needs to register and then login through the site. If the given details are valid then the user can access our proposed system.

There are three main test cases in our system mentioned below:

1. Validating the static user id and password - If the given user id and password of the user doesn't match with user id and password stored in the database then the user cannot login. So the user should provide the correct user id and password in order to login.
2. Validating the OTP - If the user successfully logs in our proposed system, an OTP for next login session is sent to user's phone as an SMS from the SMS API after checking mark the send SMS text. In this case, if the user cannot login with valid OTP, the login session will be terminated.

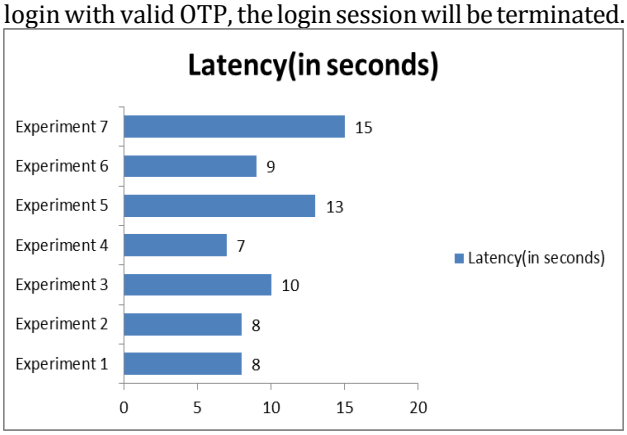

Fig – 8: Latency in OTP receipt

3. Validating Auth_code – User needs to enter the code fetched from the phone; entering wrong code will terminate the session, immediately.

Testing Scenario:

Table -1: System Specifications

System Configuration	
Processor	AMD A8-6410 APU, 2.00 GHz
RAM	4 GB
System Type	64 GB Operating System, x64 based processor
Operating System	Windows 10 Home Single Language
Software Package	Wamp (Windows, Apache, MySQL, PHP)
Android Development	Eclipse SDK, 3.5.2
Browser	Google Chrome

Table -2: Device Specifications

Device Specifications	
Brand	HTC Desire 816
CPU Speed	1.7 GHz
CPU Type	Octa-core
OS	Android OS, v4.4.2 (KitKat)

Touch Screen	HTC Sense UI 6.0
Screen Size	5.5 inches
Sampling Rate	60 Hz Maximum
Technology	GSM/HSPA

Table -3: Resource Utilization

Resource Utilization	
Resources	Consumption
Number of instances hours in test	2 hours
Number of registration request	5 users
Number of verification requests	40
Number of successful logins	34
Number of failed login	6
Average time for OTP receipt	8 seconds
API Name	AndroidCloudAuthentication.apk
Phone Storage	40.00 KB

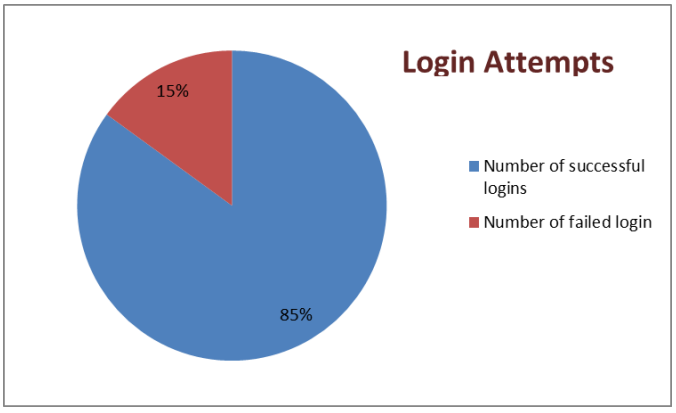

Fig - 9: Successful login attempts

4. CONCLUSION AND FUTURE SCOPE

We introduce a cloud based two factor authentication arrangement that associates possession factor and knowledge factor to improve security. The suggested arrangement is comfortably scalable and is readily accessible for the usage on mobile devices such as PDA's and smart phones. The price and resource requisites of the suggested SaaS are low and independent of the end user's platform. We display that the implemented system solutions well for a rather limited association of users. In future, we will access our authentication framework on a bigger scale, with extra clients and users enrolled on the cloud based services. The solution show cases a horizontal level of service, available for all involved bodies, that recognizes a security web through federations, within which crucial trust is maintained.

REFERENCES

[1] A. Allan, "Magic quadrant for user authentication," 2012.

[2] FFIEC. (2005, Feb.) Ffiec releases guidance on authentication in internet banking environment. [Online]. Available: http://www.ffiec.gov/press/pr101205.htm

[3] M. Alizadeh, W. H. Hassan and T. Khodadadi, "Feasibility of Implementing Multi-factor Authentication Schemes in Mobile Cloud Computing," 2014 5th International Conference on Intelligent Systems, Modelling and Simulation, Langkawi, 2014, pp. 615-618.

[4] P. Kamp, P. Godefroid, M. Levin, D. Molnar, P. McKenzie,R. Stapleton-Gray, B. Woodcock, and G. Neville-Neil, "Linkedin password leak: Salt their hide," Queue, vol. 10, no. 6, p. 20, 2012.

[5] J. Brodkin, "Dropbox confirms it got hacked, will offer two-factor authentication, "http://arstechnica.com/security/2012/07/, 2012, [Online; accessed 07-June-2016].

[6] B. Lord, "Keeping our users secure, "https://blog.twitter.com/2013/keeping-our-userssecure, 2013, [Online; accessed 06-June-2016]

[7] S. H. Khan and M. A. Akbar, "Multi-Factor Authentication on Cloud," Digital Image Computing: Techniques and Applications (DICTA), 2015 International Conference, pp. 1-7, 2015.

[8] W. Liu, A. S. Uluagac and R. Beyah, "MACA: A privacy-preserving multi-factor cloud authentication system utilizing big data," Computer Communications Workshops (INFOCOM WKSHPS), pp. 518-523, 2014.

[9] J. Yu, G. Wang, Y. Mu and W. Gao, "An Efficient Generic Framework for Three-Factor Authentication With Provably Secure Instantiation," IEEE Transactions on Information Forensics and Security, vol. 9, no. 12, pp. 2302-2313, December 2014.

[10] Altera Gold Code Generator Reference Design, March 2003, ver 1.0, Application Note 295 http://www.cs.cmu.edu/~sensing-sensors/readings/Gold_Code_Generator-an295.pdf

BIOGRAPHY

Jyotika Chhetiza is an M.Tech student in CSE department of Shri Ram Institute of Science and Technology, Jabalpur, India, affliated to Rajiv Gandhi Proudyogiki Vishwavidyalaya (State Technical Unviersity of Madhya Pradesh, India). This paper is being published in the partial fulfilment of completion of her Master's thesis.