IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, June 2022
Impact Factor: 6.252

# Token Based Authentication for Smartphone

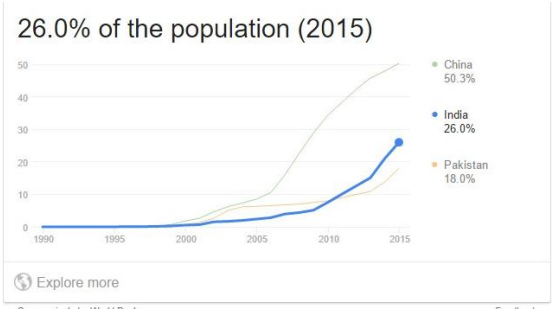
**Yagnesh V.Chudasama[1] and Vinayak D. Howale[2]**
Students, Department of MCA
Late Bhausaheb Hiray S S Trust's Hiray Institute of Computer Application, Mumbai, India

**Abstract:** *In today world user privacy is most important and every user want to be secured. To overcome this issue the current scenario is text based authentication i.e. password based authentication. Password based authentication is less secured and can easily be hacked by hacker using some hacking methods and tools. Also, user preferred to remember easy password i.e. 123456 etc. and are not using complex password such as 12@34@5Six so it is easily identified and hacked. To overcome this issue Token Based Authentication can be used to as an alternative for text based authentication but its costly and required special hardware and software setup. This paper understands the current authentication scenario and survey the smartphone based authentication architecture and password algorithm.*

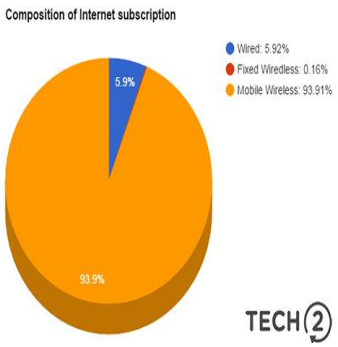
**Keywords:** Authentication, Dynamic Password, Mobile Token

## I. INTRODUCTION

Authentication is a method by which a machine authenticates the identity of a user who need to access it. Any security system protects information they stored their resources and human factor like ease of use and accessibility. Finally, security system must reflect security, reliability, usability and human factor such as easy to use, understand and highly accessible. The increase use of Internet in our day to day activities had made our life easy and provides us with business solution, online service, government portals, social network sites, information portals are replacing the traditional way of working and communication. In current scenario, the use of Internet mostly via smartphones as compared to computer and other devices such as Desktop, Laptop etc. To understand it the below graph how Indian user uses Internet has increased dramatically.




Fig(1)




Fig(2)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, June 2022
Impact Factor: 6.252

And prediction is being made number of Internet user in India could cross 450 million by June 2019. TRAI release data on internet usage and there is growth of 9.72 percentage over previous year. There are 350.48 million internet users out of which 162.06 are broadband subscriber and 188.42 are narrowband subscribers. Only 0.16% of user has fixed wireless broadband connection and 28000 users across the country have a fixed wireless narrowband connection. A mobile wireless connection is how most people in India subscribe to a broadband connection.

From above figure Internet access through smartphones is more as compared to other devices in India. Smartphone has become part of our day to day life and this paper propose cheap way to achieve token based authentication using smartphone and paper consist of architecture and algorithm which calculate dynamic password.

## II. BACKGROUND

Security is mandatory for the success of Digital Solution. The way to achieve it is to achieve higher level of security by achieving strong authentication. There is no standard definition of strong authentication. Security is necessary to maintain user information confidential and maintain the system. Security is also used to gain trust while buying, selling and exchange of good and service over network. Communication between 2 PC over network, Server, Application and Mobile Phones Security plays vital role in their interaction. The primary requirement of security is identification and authorization of user. Present scenario relies on password based authentication to identify user and established trust that the user entering the system is valid user or not. Normally, users choose password which are easy to guess and remember, relevant information or common for all authentication process. Strong password is not easy to remember and are written somewhere in diary or notes which lead to password leek. Weak authentication can cause exploitation of user private information, Corporate internal details etc. All hacking on system is unique by itself and hacker uses basic methods such as spoofing, surfing, eye dropping, brute forcing, predicting profile study etc. These studies conclude that there is a need for strong authentication process other than password authentication which is more secured than password authentication. Token based authentication is a way we can achieve more security as compared to password based authentication. It requires hardware interaction by the user to complete the authentication process. Hardware consist of custom software which may or may not be synchronized with the server application to produce dynamic password. The password is normally based on 3-digit timestamp to produce unique password. When user need to authenticate it uses password to generate token and it can be used only once also called one time password. Time limit and complex algorithm trouble hacker to crack it and unauthorized access to user. It is also difficult to predict next password which is to generate by the system. So, the algorithm and timestamp make it difficult to predict and crack it by some non-authorized means. Token based authentication require dedicated device and many device are available in the market with different algorithm. Security token depend on seed value to generate pseudorandom number and include timestamp to generate truly random password. Configuration of security is done at the application server. This way we can have connection less password for strong authentication. But there is some issue related to token based authentication. The first one is high cost of installation because of hardware and server installation. Consider a case study Bank of America, they begun to provide security token to its 14 million customers for digital identification. Where minimum investment cost for security token was $140 million when they use cheapest security token. These make the worry about to look out another security option for strong authentication. Further, The National bank of Dubai made compulsory for commercial customers and optional for personal customers to obtain tokens. Another key aspect of security token is, not only used by banking industry but also used in ERP system for employee login and digital verification (i.e. Merrill lynch). From the above study, we can say that security token is costly and millions of users requires millions of token and service provider must bear this cost. The user also must carry multiple token if they are in multiple organization and this become a tedious job for the user. Also, user must be trained for using token and training cost is incurred in it. In case of misplace or loss of token who will pay the token cost is also management issue.

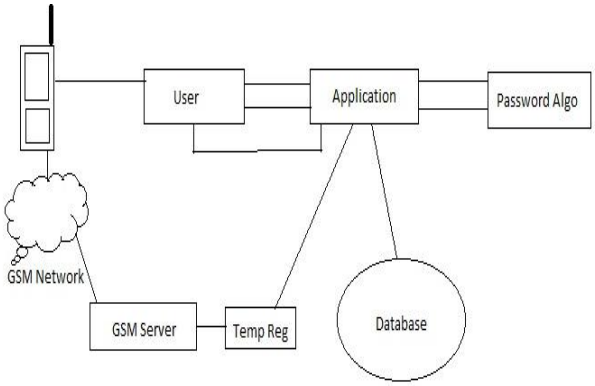
This paper take mobile phone as an emerging alternative of security token because it reduces the cost and provide with generalized solution to replace security token with smartphones. [2]

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, June 2022
Impact Factor: 6.252

## III. AUTHENTICATION ARCHITECTURE

Authentication Architecture consist of following elements.

1. User want to have access of the application and connect with application or node with network.
2. Password algorithm is applied to generate dynamic password.
3. The GSM Server or SMS Server help to send message of dynamic password
4. Temporary Registry is the registry used to store username and password for session.




Fig(3)

Through this paper, we address the overview of token based strong authentication. The sequence of events during the strong authentication is as follow:

1. User send REQUEST to the Application with its general identity i.e. Username and Password.
2. Application Server will check that the user is valid in database.
3. After that, it sends password request & static password to the password algorithm to generate dynamic password for user. By taking seed value, timestamp, date and static password, algorithm generates a 24 bit (8digit) dynamic password for digital identification.
4. Password generated is stored in temporary registry
5. Now the server send the dynamic password to the user via SMS message or GSM Modem.
6. User retrieve the password from the mobile phone.
7. User gives identification by username and dynamic password which is send by server.
8. Server validate the password stored in temporary registry.
9. If the user is identified the user get access.

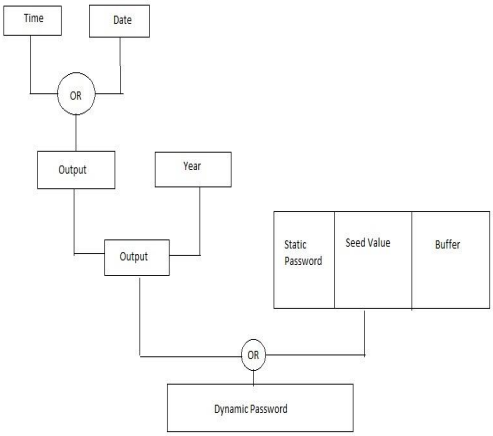
Algorithm changes password every 120 sec. Another scenario is on verification the time system must again calculate password so a temporary buffer is created which last for 2 min and store generated dynamic password the name of the buffer is temporary registry for users. Permanent storage of password may cause replay attack. After every 2 min, temporary registry is refreshed and old entries are removed.[3]

### 3.1 Password Algorithm

To secure the system, dynamic password should be hard to guess, retrieve and untraceable. Therefore, a strong password algorithm to generate dynamic password is needed. This not only help to generate password but also able to introduce variation into two consecutive outcomes. In the proposed algorithm, following factors has been chosen to generate 24-bit dynamic password.

1. Static password must be 4 digit (max. 14 Bits).
2. Date & month generate password unique for day and month.
3. Year generate unique for the year.
4. Seed value to generate randomness
5. Buffer is used to make string complete of 24 bit. Fill 0 before start bit (if required).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, June 2022
Impact Factor: 6.252




Fig(4)

The following steps would be used to generate the algorithm.

- Step 1: System will retrieve server current date (dd: mm) and time (hr: mm) and perform OR operation to generate 12-bit outcome.
- Step 2: System will concatenate this 12-bit outcome with current year (12 bit) and make 24-bit string.
- Step 3: Thereafter, System will use static password value to make password for individual user. System will concatenate this 14-bit value with 10-bit seed (pseudorandom number) and develop 24-bit string.
- Step 4: If the string size is less than 24 bit, buffer bit would be added to frame 24-bit string.
- Step 5: Now, System would again perform bit outcomes and generate 8 digits (24-bit) dynamic password

In this password algorithm, we chose time, date and year to make unique value for the instance of year. 4 digit Static passwords would help to generate a unique string for each individual request. Because Time and date is known by everyone, Seed value would help to introduce randomness for each outcome. Due to this entire factor generated password would be unique and very hard to trace and predict.

## IV. CONCLUSION

Security is the key for success of digital solution. But to achieve it require hardware and software also environment setup which is costly. This paper review how to use smartphone, architecture and algorithm which is cost efficient and user-friendly. Also, additional token management is not required and issues related to loss and misplace of token etc. Future development includes more flexible and strong mechanism without embedding hardware (i.e. Virtual token).

## REFERENCES

[1] Fadi Aloul, Syed Zahidi, Wassim El-Hajj "Two Factor Authentication Using Mobile Phones" proceeding of 978-1-4244-3806-8/0 IEEE Conference in 2009.
[2] SIMSON L. GARFINKEL "Email-Based Identification and Authentication: An Alternative to PKI?" published by The IEEE Computer Society proceeding 1540-7993/03 in 2003.
[3] Ghassan Kbar "Wireless Network Token-Based Fast Authentication" published in proceeding of 17th International Conference on Telecommunication 978-1-4244-5247-7/09 in 2010.
[4] Sharma M.K., Gawshinde S., Parekh T., "Values of Authentication in E-Business" published in proceeding of 1st International Conference in 2011.
[5] Do van Thanh, Ivar Jorstad, Tore Jenvik "Strong Authentication with mobile phone as token" Proceeding of 978-1-4244-5113-5/09 IEEE Conference in 2009.
[6] Haidong Xia, Jos´e Brustoloni "Virtual Prepaid Tokens for Wi-Fi Hotspot Access" Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04) 0742-1303-in
2004.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, June 2022
Impact Factor: 6.252

[7] Hristo Bojinov, Dan Boneh "Mobile Token-Based Authentication on a Budget" in Proceeding ACM 978-1-4503-0649-2 in 2010.
[8] L. E. Sebola and W.T. Penzhorn "A Secure Mobile Commerce System for the Vending of Prepaid Electricity Tokens".
[9] D. Ilett, "US Bank Gives Two-Factor Authentication to Millions of Customers" 2005.
[10] A. Herzberg, "Payments and Banking with Mobile Personal Device" Communications of the ACM, 46(5), 53-58, May 2003.
[11] "RSA Security Selected by National Bank of Abu Dhabi to Protect Online Banking Customers" 2005 Available at http://www.rsa.com/press reease.aspx: id=6092