iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VIII **Month of publication:** Aug 2023

DOI: https://doi.org/10.22214/ijraset.2023.55465

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

Alternative Method for OTP based Authentication in Areas with Weak Mobile Signal

Mr. Arin Mashta
Department of Computer Engineering, Lokmanya Tilak College of Engineering, Mumbai

Abstract: ***The rapid development of Internet-based applications and services has made websites a crucial part of our lives. More and more users are using online office services instead of desktop office software, online social services to engage in social activities, online information boards to post their business products, and online shopping to do their purchasing. To make all these online activities more secure One Time Password (OTP) are used. Due to weak mobile signal receiving this OTP becomes difficult.***
Keywords: OTP, Weak mobile signal, IVRS, Authentication, mobile phone.

I. INTRODUCTION

User authentication is very crucial for the computers as well as network system security. Most of the login strategies share a common problem that is they authenticate at user just at the initial login session and then do not re-authenticate the owners until the end user logs out. In this case virtually, anyone can use the system materials if the initial user does not effectively logout. And so, for resolving this issue, the system must continuously monitor and authenticate the end user after the original login session. To be able to do this objective, One-time password (OTP) is used for strong, dependable also as user-friendly technique for the constant user authentication.

However, the security and privacy problems have also grown along with these newer and open Internet applications. In order to use the online services and applications, users typically need to create accounts including usernames and passwords. The username-based identity and the related password problems because of online user behaviours have been a focus of research studies for quite some time.

II. OTP & ITS MECHANISM

One-time password (OTP) is the kind of password that is only valid for one transaction. Different from the traditional passwords. The OTPs can be generated in three ways: the time-synchronization OTP is calculated based on current time, the previous password-based OTP is calculated using the previous OTP, and the challenge-based OTP is calculated with a challenge from the server. The OTP can be generated respectively by the client and an authentication server with shared secret key, or it can be generated on the server side and then sent to the client through SMS or Email.

One time password (OTP) systems provide a mechanism for logging onto a network or a service using a unique password which can be used only once, as the name suggest. This prevents some forms of identity theft by making sure that captured username/password cannot be used second time.

Typically, user logon name stays same, and one time password changes with each login. One-time passwords are a form of so-called strong authentication, provides much improved protection to online banking accounts, corporate networks and other systems containing sensitive data. a one-time password (OTP) strategy, to protect network access and end user's digital identities. This adds an extra level of security and it will be extremely challenging for an attacker to access unauthorized data, networks, or online accounts.

III.FIRST PROPOSED ALTERNATIVE

One-time password (OTP) plays an indispensable role on authenticating mobile users to critical web services that demand a high level of security. As the smartphones are increasingly gaining popularity nowadays, software-based OTP generators have been developed and installed into smartphones as software apps, which bring great convenience to the users without introducing extra burden. However, software-based OTP solutions cannot guarantee the confidentiality of the generated passwords or even the seeds when the mobile OS is compromised.

Moreover, they also suffer from denial-of-service attacks when the mobile OS crashes. Hardware-based OTP tokens can solve these security problems in the software-based OTP solutions; however, it is inconvenient for the users to carry physical tokens with them, particularly, when there is more than one token to be carried.

M.Wu, S. Garfinkel, and R. Miller, proposed an authentication protocol which uses a mobile phone as a handheld authentication token, and a security proxy which allows the system to be used with unmodified third-party web services.

IV. SECOND PROPOSED ALTERNATIVE

We can propose a new design of secure OTP using mobile phones. Our design can achieve the better level of security. We can implement our proposed alternative through Interactive voice response (IVR) system.

IVR is the technology that allows phone systems to route calls based on spoken word responses and touch-tone input. Inbound callers are categorized and grouped by responding to automated menus that then help connect them to live contact centre agents.

Interactive voice response works by combining existing physical phone system setups with VoIP technology to create a call routing system. This system is then supported by IVR software to help build out automated menus that direct calls to the appropriate departments, live agents, or databases as necessary. These systems greatly improve customer experience by providing a seamless routing infrastructure to efficiently connect them with the resources they need. Phone calls are connected quickly, saving both businesses and customers precious time, and improving the relationship between the parties. We have planned to implement this IVR services using emergency call feature provided by every mobile phone. Emergency calling feature was introduced back when GSM standards were created in the 1990s. Here we can make an emergency call with no service, as long as there is a cell phone tower nearby, and you are using a local SIM. By using this feature a user having a weak network signal or no signal can use IVR services by calling on emergency call number pertaining to a particular institution whose services user want to use. With the help of IVRS relating to a particular institution, First user details will be verified and then OTP can be shared with the user to complete their task.

To use emergency call services, we do not need a paid subscription or a phone plan to make an emergency call. If user have no bars on their phone, it simply means that there are no towers nearby that support their carrier. But, when they will make an emergency call, the authentication process changes.

In emergency calls, the signal can piggyback using the infrastructure of another network provider. An interesting chain of events is triggered when we place an emergency call in such circumstances.

The internal phone software quickly analyses available signals in the region and identifies the strongest for fielding the emergency call. This emergency call is then tagged, thus giving it priority as specified by guidelines.

The priority tag is very important because if the cell phone tower is running at maximum capacity, it will simply bump a call with no priority status to allow an emergency call to connect. It does seem like a lot is happening at once, but we should know that all of this happens in a matter of a few seconds. That is why we get such a quick response when any user dials an emergency number in most cases. So, by keeping all above concepts in our mind we can solve this problem.

A. We can Implement it in following Way

1) The primary communication service connected to the server. Here, any API service provider can be used.
2) The server where the application worker is hosted on. E.g., AWS EC2, Heroku, etc.
3) Access to emergency service band by telecommunication providers, in the production phase
4) Database used to store the users, organizations, and generated OTPs details. E.g., MySQL, Redis, MongoDB, etc.

B. Use Case Details

1) It can provide better services in the field of banking, health care or basic PDS facility.
2) It will help in decreasing user complexity and user hesitation in using online services.
3) It will solve the biggest problem of getting OTP in areas of weak mobile signals in rural and urban parts of India.

V. RESEARCH GAP

Most of the research papers which have been published mostly solve the problem of generating strong OTPs or creating algorithms for strong OTP generator. None of the research papers have tried to either solve or even look upon the problem of OTP non-receival due to weak network signal. Research papers have generally considered OTP will be received only on smartphones and ignored that the rural areas of generally experiences mobile network issues. So, there is an analysis and research gap in particularly this domain.

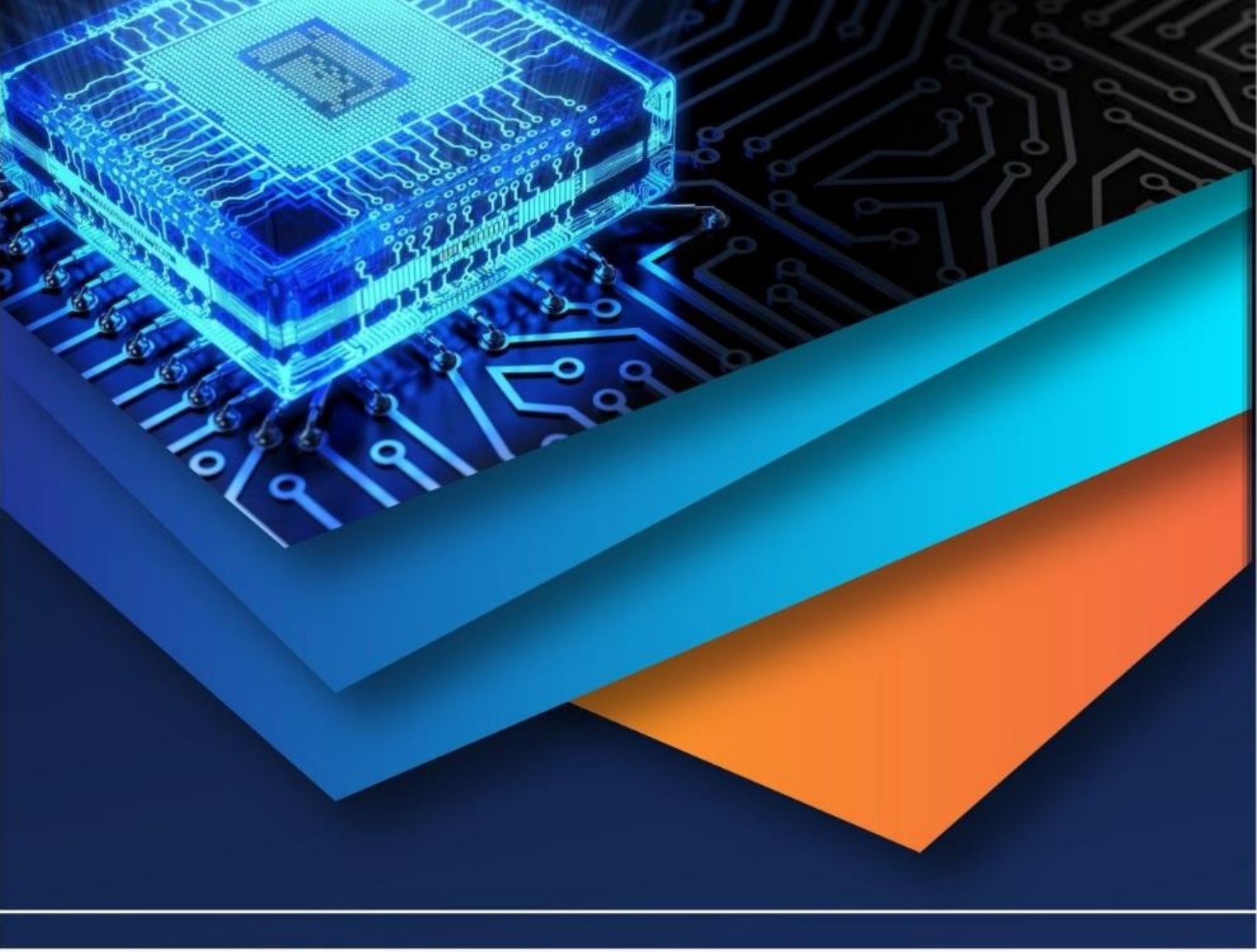
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

VI. CONCLUSIONS

Till date there has been no solution for this problem. Here we have tried developing a solution for this problem by proposing an idea to implement it with IVRS based OTP services with the help of emergency calling feature of mobile phones. We can also try to implement it on a larger scale for rural parts of India with the help of greater research facilities.

REFERENCES

[1] SolidPass. Desktop soft token. http: //www.solidpass.com/authentication-methods/onetime-password-generator-otp-token.html.
[2] McAfee. Mcafee one time password. http://www.mcafee.com/us/products/one-timepassword.aspx.
[3] Symantec. Whitepaper: Two-factor Authentication: A TCO Viewpoiont. https://www4.symantec.com/ mktginfo/whitepaper/user_authentication/ whitepaper-twofactor-authentication.pdf.
[4] EMC2 . RSA SecureID Hardware Tokens. http://www.emc.com/security/rsa-securid/rsasecurid-hardware-tokens.html
[5] Dmitrienko, C. Liebchen, C. Rossow, and A. Sadeghi. Security analysis of mobile two-factor authentication schemes. Intel Technology Journal, 18(4), 2014.
[6] TrustOTP: Transforming Smartphones into Secure One-Time Password Tokens He Sun, Kun Sun, Yuewu Wang , and Jiwu Jing
[7] A Survey on One Time Password Mirza Tanzila Maqsood , Pooja Shinde



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY