ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

OTP over SMS: Time Delay Issues and Causes

Dhanashri Ghosalkar[1], Shweta Patil[2]

MBA-IT, Symbiosis Institute of Computer Studies and Research, Shivajinagar, Pune, India

ABSTRACT: In this study, the issues and causes related to sending One Time Password (OTP) via SMS are examined and analysed. One-time password (OTP) is password that validates an authentic user for only one login to the respective system. If user is unauthorized, system will not allow further access. OTP can be generated by using different cryptographic hash functions that provides a fixed string which can be used as second level security [1]. In generation of OTP there are many factors that can make OTP unique every time it is generated. In this report, the flow of system I am developing, topics related to issues and causes, about OTP over SMS. One Time Passwords (OTP) is introduced to provide an additional layer of security. OTP is normally transmitted through SMS, but recent studies prove that OTPs over SMS are causing various issues and causes which lead time delay in transaction [6].

KEYWORDS*:* One Time Password(OTP), SMS, Security, Authentication

I.INTRODUCTION

The one-time password is a random password generated by the server send to the user via SMS for their person authentication access. In contract with the traditional approach the work addresses the concept of two factor authentication for accessing and approving the one-time password by the legitimate user. This works on all platforms and applications that are either may be online processed transaction done via system or electronic gadgets. This work will add additional secure measure despite the security poised by the one-time password.

The concepts of OTP using two factor semiautomatic authentications messaging via secure channels are used widely in network mechanism. These methods are used in online secure transaction especially in the case of payment and other validation and verification process. OTP can be achieved either via SMS or any digital messaging service for providing consistent service.

The problem with two factor authentication also has few pitfalls arises in the form of following outcomes
(i) Sending SMS to users
(ii) Delay messaging in sending/receiving

Sending SMS to users:

While sending the OTP to the user, the concern authority or the providers will send SMS in the form of OTP to the user electronic medium or gadgets for getting their instant approval for all the transaction. This involves two way communications for sending the SMS and receiving the acknowledgment. The receiving SMS will be charges depending on the provider’s constraint. If sending the SMS falls within the scope of the provider’s constraint, then it will also be considering as the criteria for either sending or receiving the SMS.

Delay messaging in sending/receiving:

The receiving and sending SMS will be left unnoticed when the charge is taken by the provider and the message is not delivered. This is because of the huge network traffic and that leads to delay. Generally, the delay arises in both ends (sending/receiving). In order to avoid such factor affecting the transaction the delay is measured and the alternative way has been chosen to resend the code that expire the previous message send via the same portal [6].

II. METHODOLOGY

1. Approaches for generation of OTP:

The various approaches for the generation of OTPs are listed below:

- Based on time-synchronization between the authentication server and the client providing the password (OTPs are valid only for a short period of time).
- Using a mathematical algorithm to generate a new password based on the previous password (OTPs are effectively a chain and must be used in a predefined order).
- Using a mathematical algorithm where the new password is based on a challenge (e.g., a random number chosen by the authentication server or transaction details) and/or a counter. The following Figure-1 shows how OTP is generated and used for the transactions. [7]

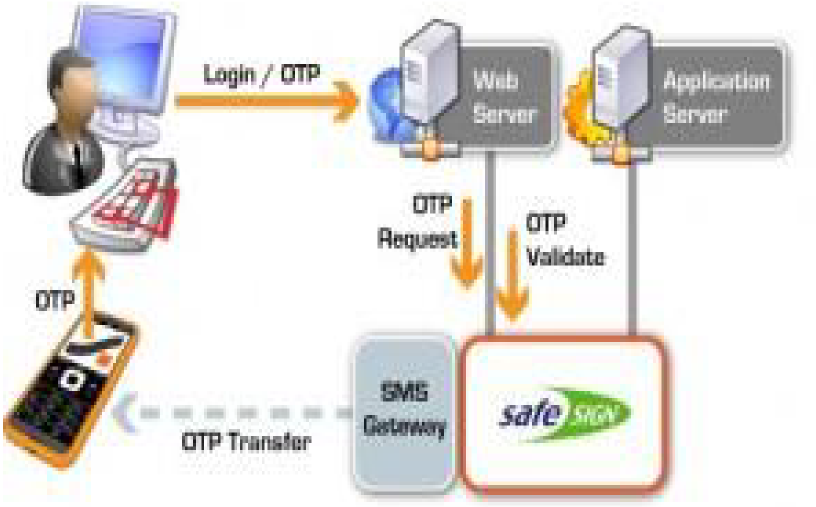


Figure-1-Genation of OTP and usage [7]

2.One-Time Passwords via SMS:

One-Time Passwords (OTP) are utilized as an important factor in multi-factor authorization/authentication applications. They are only valid for exactly one authorization or authentication request. To avoid password lists, a convenient way to provide the user with an OTP is to send it via SMS. The phone number of the user must be registered for the service that provides SMS OTPs for authentication or authorization. OTPs are quite popular as an additional authorization or authentication factor in web-based services. These passwords can be utilized to authenticate a user, i.e., the user needs a valid OTP to prove his identity to log into a web application or to access the company's private network .SMS OTPs are also used for account verification, e.g., Google Mail. The OTP is bound to a certain request or transaction in order to confirm it. Additionally, the OTP can be restricted to a very short time window. In online banking web applications for example, the user has to authenticate himself via a valid username and password to initiate a transaction. Directly after this transaction request, the user gets an SMS message containing the OTP that must be additionally entered to authorize the transaction. In this application area the OTP is called a mobile Transaction Authorization Number

The basic principle for SMS-based OTPs is always the same, no matter what application is considered. The online service sends the OTP to the user's mobile phone via the cellular network, and the user enters the OTP to authenticate or authorize a transaction. [9]

3.Problem in OTP generation:

Use of one time passwords as a second step to logging in seems to be getting more popular recently. There are two main approaches to OTPs, the first being delivery of the OTP over a channel like SMS, and the other being a code that changes every time you use one to log in or on a predefined time schedule, based on a predefined algorithm. To use the first type, one must have a device with network connectivity and a phone number to receive SMS. With devices like RSA Secure ID tokens or Google Authenticator, a person can generate the second type of OTP manually generate the OTP on your mobile handset instead of receiving it through SMS. OTP application is available to Apple, Android, Windows and blackberry mobile users. OTP can be generated through an application without internet connection/Mobile network. Activation of this application will involve two steps as under: Downloading of Mobile OTP application "CA MOBILE OTP" on handsets. Users are required to download the application from respective app stores [7].

4.Causes for Delay in Delivering OTP over SMS:

Location Issues:

The location of the sender or recipient can create a delay in text message delivery. What causes this varies from handset to handset, but common reasons are being on the border of two cell coverage areas or travelling at speeds above about 50km/h. This is most likely happening if messages arrive all at once. If a mobile device is located outside a network's coverage area or in a spot where the network signal is blocked such as in a mountainous region, a delay in transmission may occur. In urban areas, tall buildings can also cause transmission issues. Being in an old building with poor cell reception is another possible culprit.

Mobile Device Issues

Problems with a mobile device may cause delays in text message transmission. The most obvious cause is a device that has been turned off, but a weak or uncharged battery may also negatively impact message delivery. Devices that have an adjustable antenna may experience transmission difficulties if the antenna has sustained damage or has not been fully raised.

Different Networks

A text sender and receiver using different networks may have a greater chance of experiencing texting delays than those using the same network, because of communication between networks or the carrier prioritizing their own traffic.

Network Traffic

Texting during periods of heavy network use impacts text delivery speed. Periods of increased traffic may create congestion on the local network and delay arrival of messages to the handset.

Message Length

You may know that, typically, an SMS is 160 characters in length (if you were thinking 140, that's Twitter). If you've read examples through three however, you'll know that nothing is as simple as it seems. Countries like Brazil only support messages of up to 157 characters of length. If your message length is over this limit, it will be rejected if your SMS provider doesn't automatically split it into multiple messages. One of the main things to look out for is a link being split into two, rendering it unclick able. [3]

Encoding

At a basic level, encoding determines the possible combination of characters for which characters can be sent. Typically, messages are sent using either Unicode, which allows for 70 characters, or using the global standard GSM

3.38 which allows 160 characters. It's important to know that different carriers and countries require different encoding. Some carriers simply will not deliver messages that are sent in Unicode while others will deliver the message incorrectly.

Using Cheap Routes

The bulks SMS industry has long been plagued by shady characters and tactics used to maximize margins. Techniques such as SIM boxes and "grey" routes are illegitimate ways for businesses to connect to the telecom network for a very low cost. With sending bulk SMS, the general rule is that you get what you pay for. SIM boxes, due to their illegality, are shut down by carriers and lead to extremely unpredictable and unreliable message delivery.

Filtered Content

Some countries are banned or filtered content, it would probably be easy to come up with a few like China or Saudi Arabia, where the government controls what information citizens are allowed to receive. Aside from the government filtering certain types of content, there is also the issue of what the carriers will allow. In Japan, for example, if there is a URL in the body of the message then the message delivery will fail. Those messages are classified as illegal, and are either discarded completely or the part of the text that is illegal will be removed. [4]

5.Some other Issues with SMS-OTP

The main problems with the SMS-OTP design under overloaded situations are:

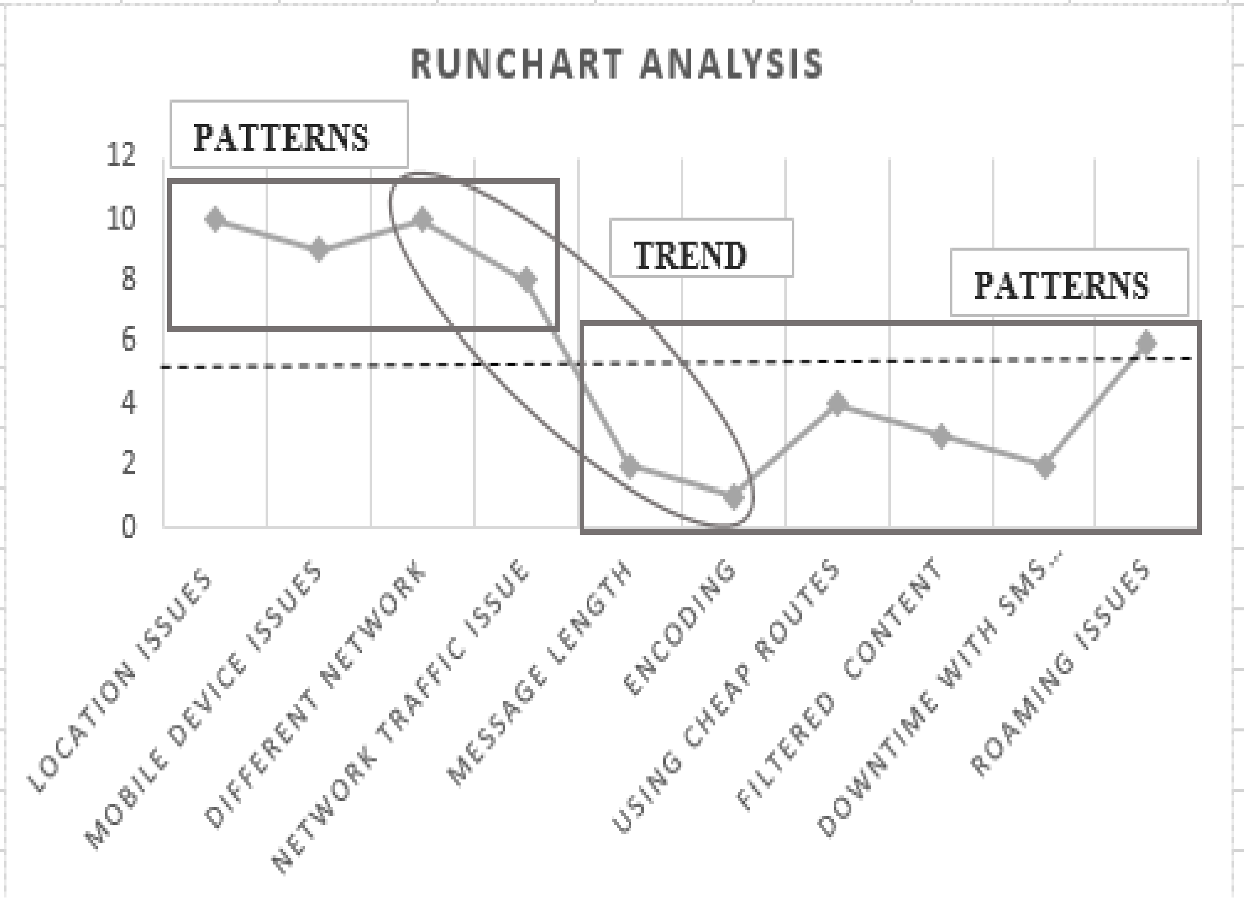
- Delay in delivery of SMS. The MNOs cannot guarantee SMS text message delivery within an acceptable timeframe for 100 percent of all SMS messages delivered. That is because SMS traffic is not sent point to point, it is queued and then sent on to the required network cell where it is again queued and finally sent to the end user's phone. There are times when the mobile network is overloaded, e.g. peak times at events and natural disasters.
- Low coverage areas.
- Downtime with SMS gateway.
- Non-availability of service for roaming user.
- High cost for roaming user.

Late delivery of an OTP contained in an SMS text message can be problematic for a time critical login that can mean no access to critical enterprise resources, and there is a possibility that a user at Payment stage (Web page for making payment) in the Ecommerce application may suffer from:

- Service outage of mobile network which means transaction termination due to timeout of transaction (valid OTP not provided to bank).
- Delayed receipt of SMS-OTP that may in turn delay the response time (increase user frustration) [8].

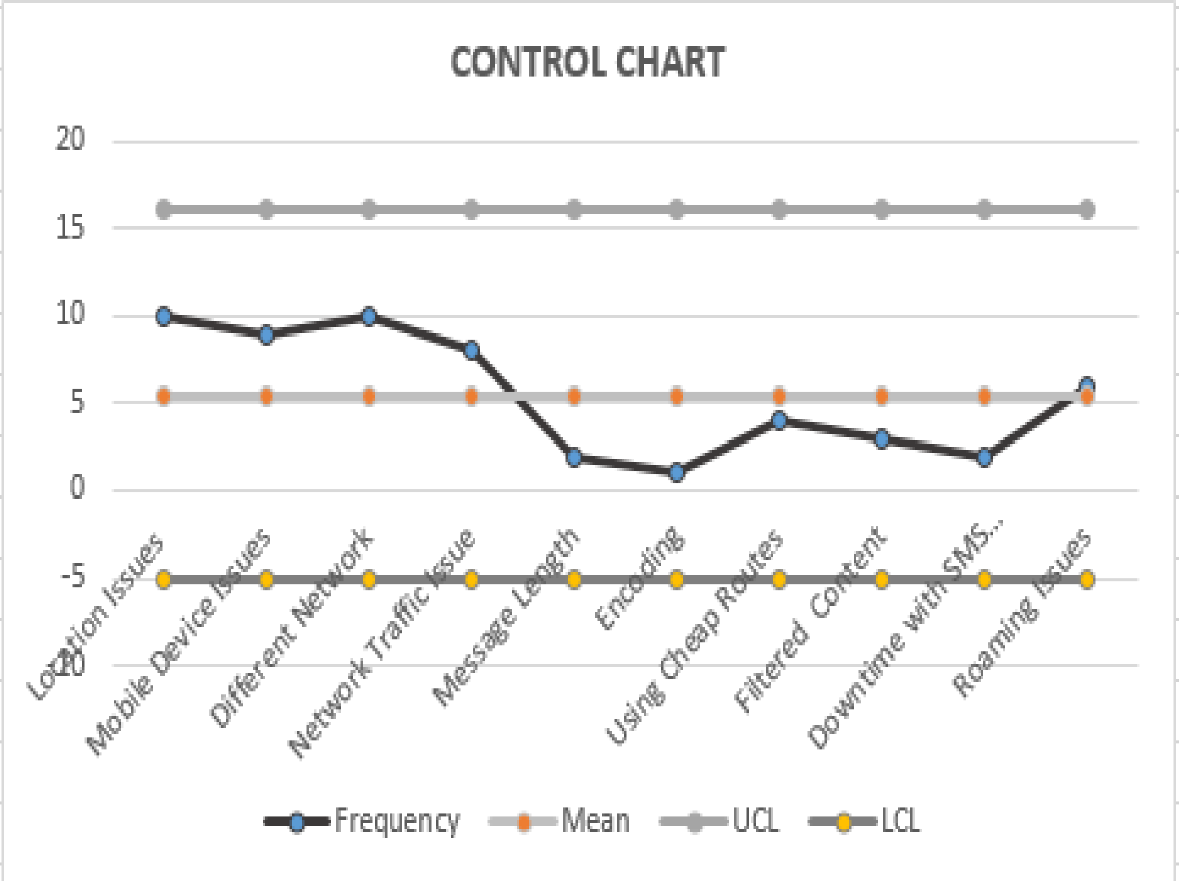
6.Analysis:

A. RUNCHART ANALYSIS:



- Issues like Different Network, Network Traffic Issue, Message Length and encoding forms a Trend which is caused due to High Response Time.
- High Response Time indicates these are major issues and need to focused with priority.

B. CONTROL CHART ANALYSIS:



- All the points are within the control limit therefore the frequency of causes can be easily predicted and controlled.
- Control Limits will provide information about process behaviour, therefore the considered state is ideal.

III. CONCLUSION

OTP is considered to provide two-factor authentication which was delivered to the intended user through text messages i.e. SMS. This paper thus focusses on time delay issues and causes of One Time Password (OTP) via SMS.Services adopting SMS OTPs are not limited to banking and other financial services, but include email providers and popular applications and games. The major issues and causes of One Time Password are described in the content which cause time delay while authenticating banking and other transactions.

IV. ACKNOWLEDGEMENT

We thank Mr. SupratikGhatak who provided insight and expertise that greatly assisted the research. We would also like to thank Symbiosis International (Deemed University) for providing the platform for doing the same.

REFERENCES

[1] 1429768516.pdf_Securing ATM with OTP and Biometric
[2] IJERT.pdf _SMS Based One Time Password Vulnerabilities and Safeguarding OTP over Network.
[3]https://help.nexmo.com/hc/en-us/articles/204014893-What-Causes-a-Delay-in-Delivering-SMS-Messages
[4]https://www.nexmo.com/blog/2015/01/13/top-5-reasons-sms-isnt-delivered/
[5]http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.678.114&rep=rep1&type=pdf
[6] Two Factor Authentications Using One Time Random Password for Secure Online Transaction-pdf
[7] Comparative Study On One Time Password Algorithms-pdf(https://ijcsmc.com/docs/papers/August2018/V7I8201811.pdf)
[8]http://shodhganga.inflibnet.ac.in/bitstream/10603/90827/15/15_chapter%207.pdf
[9]SMS-based One-Time Passwords: Attacks and Defence

BOIGRAPHY

1. Dhanashri Ghosalkar (BSc-IT)-Currently Pursuing Master of Business Administration from Symbiosis International (Deemed University), Pune.

2. Shweta Patil (BE-E&TC) 1.5 Years' Experience as Business Analyst - Currently Pursuing Master of Business Administration from Symbiosis International (Deemed University), Pune.