Implementation of Two-factor Authentication in Nepal

Anamol Maharjan
Computer and Electronics Engineering Department
Kantipur Engineering College,
Tribhuvan University
Lalitpur, Nepal
anamol.maharjan@gmail.com

Chirag Shrestha
Computer and Electronics Engineering Department
Kantipur Engineering College,
Tribhuvan University
Lalitpur, Nepal
shrestha.chiraggamerz@gmail.com

Kabin Devkota
Computer and Electronics Engineering Department
Kantipur Engineering College,
Tribhuvan University
Lalitpur, Nepal
devkotakabin@gmail.com

Nishan Khanal
Computer and Electronics Engineering Department
Kantipur Engineering College,
Tribhuvan University
Lalitpur, Nepal
nishan.khanal98@gmail.com

Nischal Khadka
Computer and Electronics Engineering Department
Kantipur Engineering College,
Tribhuvan University
Lalitpur, Nepal
nischalkhadka@kec.edu.np

***Abstract*—The purpose of this research is to study Two Factor Authentication od 2FA and its adoption to enhance system security in context of Nepal. Today's world is in ever need of high security means to protect vulnerable data from cyber-attacks. Many systems currently depend on single layer authentication which are prone to simple attacks . This is further supported by various news of cyber-attacks globally. 2FA is developed to minimize such security breaches, as it adds a second layer of authentication. The increasing demand for high security mechanisms today is drawing more people to 2FA. Many banks, companies in Nepal have started using 2FA to secure their systems from malicious attacks. However, it still has some loopholes during synchronization and recovery stages. This research paper discusses a new way to solve synchronization issue. And also, suggests ideas to counter possible attacks that arises in recovery stages. This paper discusses about implementing 2FA system and prepare a cost analysis to see the feasibility of implementing 2FA in context of Nepal.**

***Index Terms*—cyber-attcks, security, 2FA, synchronization, recovery**

I. Introduction

Password is the most popular and easiest method of end-user authentication. However, passwords lack entropy and are prone to be compromised by easy offline-dictionary attacks, by simply guessing or even by phishing. Many company and banks implement constraints to the criteria of password, that a user can choose, to enforce the strength of the password, but it is clearly not enough in any ways. A multi-factor authentication is an improvisation and provides better security by adding two more factors along with password that user needs to provide to confirm to his/her identity. But, Nepal, a least developed country cannot afford the cost of implementing multi-factor authentication in every possible sector. So, a better and minimalistic approach would be Two-Factor Authentication(2FA). Two Factor Authentication is a security purpose two-step verification process in which the user provides two different factors to confirm his/her identity which protects users credentials and the resources that the user can access. Factors that can be used to authenticate a persons identity are:

1) *Knowledge* : something that the user knows. Like password, username, date of birth etc.
2) *Possession* : something that the user has. Like phone, smart watches etc.
3) *Inherence* : something that is the user (bio metrics). Like fingerprints, iris etc.

Nepali sites have been facing frequent attacks and defacements by various hacker groups and most sites that are facing this problem belong to financial organizations, government bodies and other software companies. [1] The common types of cyber-attack are related to the ATM frauds, E-banking frauds, system hack and phishing. It is also a bitter truth that few Nepali banks have become latest to fall victim to hackers siphoning off 400 million of dollars by targeting SWIFT. Such breaches only highlight the fact that Nepali Cyber Security is far lacking. Few

banks and company like NIC ASIA, Siddhartha Bank, NMB, World Link have implemented 2FA as a step towards preventing breaches. However, most of these 2FA systems are based on Google Authenticator and are not updated or monitored up to its potential. A lot of flaws can be seen time and again that can be a big window for any hacker to get his job done. Similarly, implementation of 2FA can be seen in web-based application sectors but the use of 2FA for non-web-based application security can barely be seen, which is a good example of not using 2FA up to its potential. Therefore, this research paper focuses on highlighting the necessity of implementing 2FA system in Nepal, provides suggestions for improvement in 2FA system and prepares a cost analysis for implementing the system.

II. Methodology

The objective of this research is to implement 2FA system in an authentication system and to present a cost analysis for the system. A 2FA system is based on TOTP (Time Based One-Time Password) which is an extension of HOTP (HMAC One Time Password), which requires generation of a One-time password on an offline user possessed device. The parameters that are required for the generation of OTP are:

1) *Counter* : A counter basically is an integer counting the number of durations
2) *K(Secret Key)* : It is a secret message that is used to generate the OTP.

Following are the equations that are involved in the generation of OTP of the 2F.

1) $OTPvalue = TOTP(K, C_t)$
   where, $TOTP(K, C_t)$ is a function, C_t is the counter, K is the secret key
2) $TOTP(K, C_t) = HOTP(K, C) mod 10^d$
   where, d is the no. of digits wanted for OTP to be, $HOTP(K, C)$ is a function for HMAC One Time Password
3) $HOTP(K, C) = truncate(HMAC_H(K, C))$
   where, HOTP value is the truncation of the hash of counter under key K, $HMAC(K, C)$ is the cryptographic hash function

Similarly, the counter plays an important role in generation of OTP as well as in synchronizing the OTP generated in offline device and the online server. The equation of counter is as follows:

$$C_T = (T - T_0)/T_x$$

where, C_T is the time counter, T_x is the difference between the current Unix time T and some epoch (T_0; Unix epoch).

Using the following algorithm, an offline OTP can be generated in a device and same OTP in the online server. Now, as for the part of synchronizing these two different OTP,three level of synchronization has been created. Each are described as follows:

Level of synchronization implemented in our system:

- *1st level:*
  When the server detects the entered OTP is from the previous time-step it decreases its time adjust value by some constant (15% of the time interval used to calculate the counter value) or if it detects the entered OTP is from the next time step it increases its time adjust value by the same constant.
- *2nd level:*
  Whenever the mobile application is opened and if the internet connection is available then the time adjust value is updated using the Network Time Protocol.
- *3rd level:*
  If the mobile application is not opened for a long time and the clock is de-synchronized beyond the 1 time step then the user can scan the QR-code generated from the web app which changes every 5 seconds to compensate for slow speed mobile phones to synchronize the clock in the mobile application before entering the OTP. Also, the time adjust value in the server is reset.

III. Feasibility Study

Security is the protection of systems, information (data), resources and services from accidental and deliberate threats to confidentiality, integrity and availability.80% of security breaches occurring over the Internet can be easily prevented with 2FA security solution. Around 65% of people use a single password for multiple websites and accounts, so if your login credentials get stolen, you are leaving the doors wide open for the hackers to hack all your sensitive data and accounts.According to a study, security breaches rose by 48 percent in the year 2015 to 42.8 million. Thats the equivalent of 117,339 attacks per day. Since 2009, the growth rate of detected security breaches annually has grown a whopping 66% year over year.

A. User Data

Over 2.5 Billion User Accounts(that include email accounts, gaming accounts, social accounts) Have Been Hacked This Year Alone. There is a hacker attack every 39 seconds.By the time the average person takes a selfie and uploads it to Instagram, the next hacker attack has already taken place*(Source: Security Magazine)*. Cybercrime is more profitable than the global illegal drug trade.The profit from the illegal drug industry amounts to around $400 billion annually. For comparison, cybercriminals have earned a total of around $600 billion in 2018*(Source: Cybersecurity Ventures)*. Hackers steal 75 records every second. Cyber security facts show us the average number of record stolen per second. Breaches are actually a lot rarer than that its just that each breach allows for a lot of records to be stolen*(Source: Breach Level Index)*. [3] All these hacks and breaches are possible only due to insufficient security. With these risks at hand, users data and valuable assets cannot be declared safe.

B. Banking and Finance

For banks and finance organizations like Trading Houses, Credit Card Providers, Investment Funds, etc., protecting the sensitive data and money of the customers is of the utmost importance. A security survey report reveals that in the year 2015, there were nearly 2 Million attempts to steal customers money via online access to bank accounts. There are several links that make it quite easier for the hackers or attackers to get into customers bank accounts online and steal money. But, one of the weakest links that simplifies this task is compromising password-alone verification. The primary focus of banks and the financial services organizations must be to prevent all sorts of breaches by implementing better security on client account information. If any sort of cyber-attack ever happens in any organization, then at that time it may face serious liability issues. The lack of adequate safeguards or security solution in place can result in severe damage. It reflects that survival of banks and financial services organizations without implementing a system to increase security is not possible in the future. For better customer satisfaction and peace of mind, safeguarding clients banking information against threats must be the primary focus of these organizations. A recent survey of 200+ corporate directors reveals that more than 40% of respondents feel like CEOs should face the brunch of breach-related backlash. Financial services organizations and banks need to put securing client information and protecting accounts on the top priority. If proper security solution like 2FA is enabled, then you will be able to confidently claim that you have put every possible effort from your end to protect sensitive client information. [4]

C. Government Sectors

Government organizations are a likely target for cyberattacks due to the vast amount of information; including financial data, they gather and share about the market or businesses. An analysis by Rapid7, security risk intelligence solutions provider, has reported that more than 94 million records have been breached over a 3-year period(2009-2012) due to government sector data breaches. These records were containing PII (Personally Identifiable Information). Unintended disclosure, portable devices loss/theft, physical loss, hacking, etc., were some of the leading causes of data breaches in the government sector. Majority of these records; i.e. 86 percent, were breached due to the loss or discarding of endpoint devices. As per IBM X-Force data, 200 million government records around the world were compromised by July month of the year 2016. This is 60 million more than all the records breached from 2013 to 2015 combined. It shows that the percentage of hacking incidents of the government records is increasing rapidly.

Security Incidents Percentage by Attack Type [5]

- Physical, 5.71%
- Phishing, 8.57%
- Malware, 14.29%
- Heart bleed, 2.86%
- SQL Injection, 42.86%
- Misconfiguration, 25.71%

The best approach to solve all these problems is to implement Two Factor Authentication as it is highly secure and cost effective as well. 2FA solution not only dual checks identity, but also restricts an unauthorized user even if he knows your password.

IV. Cost Analysis for Implementation

Cost of implementing 2fa varies according to the customer needs and the company requirements. Implementing the cost of 2fa according to one cybersecurity company cost about USD 30-50 per year per node in Nepal. The average cost of lost/stolen records in $141 in the world. Managerial naivety in regards to security of firms is one of the prominent reasons for the difficulties to implement security. However, few banks and IT sectors are now open to implement security measures such as 2FA, Authentication log, SSH log, IP tracking. The implementation basically requires a system and engineers for monitoring purpose. Hence, the cost analysis in this research is presented based on nature of the company and motive of the company. Therefore, the cost analysis in this research is done for two sectors:

1) Government Sector
2) Private Sector

The difference between a governmental organization and private organization is that private organization works on the concept of profit whereas the governmental organization works on the concept of welfare or minimalistic profit. So, implementing a system for these organization varies in such sense:

A. Governmental Organization

In order to implement 2FA in governmental organizations or companies, firstly, a MOU (Memorandum of Understanding) should be maintained between the government and the person who is given the contract for the implementation. MOU is basically required to create a mutual understanding in case the system is breached or create any type of discomfort in services. Since governmental security has high priority and has huge coverage for population, the cost for establishing servers and hiring engineers increases due to increase in the number of servers and engineers. Maintenance and upgrading 2FA will also cost more compared to private sectors. Therefore, the cost of implementing 2FA increases and the increment highly depends on the quantity in case of governmental organization. Also, the factors for authentications can be compromised. For example, knowledge and inherence are expensive factors to implement compared to knowledge and possession. So, the range of security is directly

proportional to the cost of implementation. The implementation of 2FA has no case of loss in money and results profit due to enhancement of security in a long term.

B. Private Organization

Private Organizations works for profit. Therefore, customers are everything to them. Poor services and insecurity results to a huge negative impact on both goodwill and trust of the company. Therefore, a private organization must immensely think through while implementing 2FA. The concept of giving high quality services results on expensive assets (server). Also, the engineers that are needed for maintenance are also expensive. The absolute necessity of providing better security increases the cost of implementation in private organization. Therefore, the cost of implementation of 2FA increases and the increment depends on the quality in case of private organization. Also, for a private organization security breach and hack attacks can be fatal and may result in a huge loss. So, the 2FA system are also designed using inherence and knowledge as two factors. This case automatically increases the cost for its implementation. The implementation of 2FA in case of private organization also has no case of loss in money and results profit due to enhancement of security in a long term. Hence, in overall it is a good investment.
Hence, in overall, it is a good investment.

V. Suggestions for Improvement

In this day and age, there is high need and demand for a powerful but feasible security method. This is not only true for developed cities but also for developing countries as a whole where rapid digitalization is taking over. ”Security measures in developing countries are not as robust as they are in other parts of the world. This has made them attractive targets. [6] Our study focuses on highlighting the importance and viability of two factor authentication used with smartphones to improve cyber security. This model Is based on a smartphone environment because around 97.65 % of Nepalese people have access to smartphones. [7] In comparison to other authenticators on the market, we have proposed new ideas for synchronization in our model. However, this study can be further improved if following points are adopted into ours model.

A. Hand Gesture For Recovery

Recovery is the weakest link of two factor authentication. [8] Regardless, of how secure the system is with any model of 2FA, if the users smartphone is stolen, the system will be vulnerable to attacks. Thus, in such case the system needs a mechanism to stop login of any sort of that user until he recovers his old smartphone or configures a new smartphone. In case of a new smartphone, a viable recovery option must be provided. As such, the use of users hand gesture has been suggested for recovery, which the user saves during his Sign Up. Only after this gesture is identified and verified, the user is allowed to change his credentials and recover his Key.

B. Biometrics/PIN/Pattern to access OTP

Unless encrypted, its not that hard to bypass mobile phone security if someone has access to forensic equipment. Also, if someone is able to acquire the users phone for a moment, he can change time manually to acquire the OTP for another specific time. This creates a loophole that can be exploited. [9] Thus, the model has to use some other form of authentication to access the OTP, this can be prevented given its authentication data is stored as a highly encrypted data. We can use Biometrics, PIN or a Pattern, whichever the user feels comfortable with. The Biometrics is the most secure among the three but user is allowed to choose in regards to his convenience and technology available.

C. 2FA for Server Login

Different computer system OS still are dependent on the traditional authentication method i.e. Username and Password. If a hacker somehow gets over the firewall protection, the systems password can be easily cracked. A number of Nepali servers and government websites are being hacked, and critical information are being leaked. [11] If Two Factor Authentication is inbuilt into the servers itself, it will be very exhausting for unauthorized users to get into the system. On top of that, systems supporting to 2FA such as Authentication log which creates a log file of any user who has logged into the system can recognize and identify the security breach. Session log, Authentication Access can be developed into the server to prevent outside users from login. 2FA system needs to be implemented in servers, firewalls not just web based or app-based applications.

VI. Conclusion

2FA systems are cheap and efficient method to increase security of the system. With wide areas of scope such as web apps, servers,firewalls, proxy servers,2FA is a great tool. The current 2FA can be further upgraded in terms of synchronization and optimization for much better security. Deciding on the factors for authentication also plays a major role determining the security of a system. 2FA is a hot topic in cyber security and has gained attention and millions of dollars of investment in recent years. This proves that 2FA is the best economical and financial solution for data security in this current state. Depending on ready made 2FA system like Google Authenticator is a temporary approach since the contents cannot be changed according to necessity and bugs. Hence, this research paper is all about implementing an independent 2FA system in Nepal, providing a feasibility analysis and suggestion for increasing the effectiveness of 2FA in context of Nepal.

ACKNOWLEDGMENT

We would like to express our heartfelt gratitude to Kantipur Engineering College for providing us a platform and all the resources we needed to achieve this research contents. We also thank our professors and lecturers from KEC who provided insights and expertise that greatly assisted the research. Finally, we would like to thank all our friends, colleagues and well wishers for all the support they have extended towards us to make this research a reality.

REFERENCES

[1] Ashma Nepal, "Vulnerable Cyber Security" Internet: https://thehimalayantimes.com/science-technology/vulnerable-cyber-security/, Jan. 08, 2018 [Aug. 13, 2019]

[2] "NRB effortful to retrieve Rs 400 million of NIC Asia Bank transferred by hackers" Internet: https://thehimalayantimes.com/business/nrb-effortful-retrieve-rs-400-million-nic-asia-bank-transferred-hackers/, Rastriya Samachar Samiti, Oct. 24, 2017 [Aug. 13, 2019]

[3] "40 Astonishing Hacking Statistics" Internet: https://hostingtribunal.com/blog/hacking-statistics/, [Aug. 13, 2019]

[4] "7 Reasons Why Banking and Finance Need 2FA Solution" Internet: https://revesecure.com/blog/7-reasons-why-banking-and-finance-need-2fa-solution/, [Aug. 19, 2019]

[5] "Why Two Factor Authentication is Utmost Priority for Government Institutions?" Internet: https://revesecure.com/blog/two-factor-authentication-utmost-priority-government-institutions/, [Aug. 13, 2019]

[6] Ulla Gjeset Schjlberg, "Poor countries are more vulnerable to cyber attacs" Internet: http://sciencenordic.com/poor-countries-are-more-vulnerable-cyber-attacs, Jan. 30, 2018 [Aug. 13, 2019]

[7] "Telecommunications in Nepal" Internet: https://en.wikipedia.org/wiki/Telecommunications_in_Nepal [Aug. 13, 2019]

[8] O. Persson, and E. Wermelin, "A Theoretical Proposal of Two-Factor Authentication in Smartphones" Bachelor Thesis in Computer Science, Blekinge Institute of Technology,SE371 79 Karlskrona, Sweden, May 2017 [Aug. 13, 2019]

[9] Brandon Jones, "How Hard is it to Hack an Android Passcode?" Internet: https://www.psafe.com/en/blog/hard-hack-android-passcode/, Jun. 21, 2017 [Aug. 13, 2019]

[10] "Estimating Password-Cracking Times" Internet: https://www.betterbuys.com/estimating-password-cracking-times/ [Aug. 13, 2019]

[11] ,"Four Nepal Government Websites Hacked with Critical Information dumped by malicious actors" Internet: https://kathmandutribune.com/four-nepal-government-websites-hacked-with-critical-information-dumped-by-malicious-actors/, Kathmandu Tribune Sept. 22, 2018 [Aug. 13, 2019]