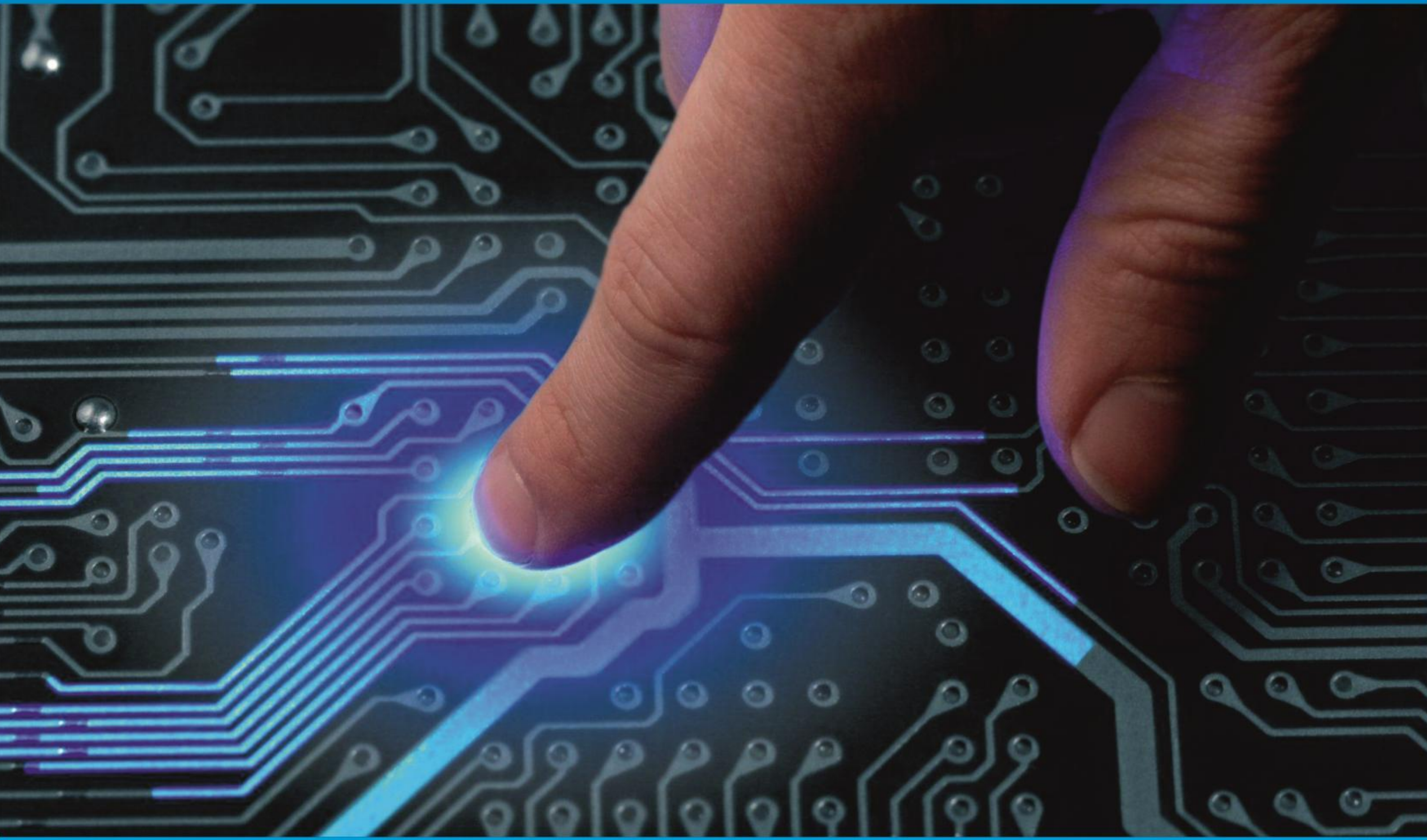
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905034 |

Two-Factor Authentication Using Malware

Parikshit Taksande[1], Pravin Choudhry[2], Prof. Rajeshwari Gundla[3]

Student, School of Computer Science and Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra, India [1]

Student, School of Computer Science and Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra, India [2]

Assistant Professor, School of Computer Science and Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra, India [3]

ABSTRACT: In today life people like to use online banking or mobile backing for payments. Tow -factor guarantees that authentication to services, such as online or mobile banking. The one-time password involves the single SMS, that SMS not gives information about transactions, Cause lot of peoples are not a wear of fords any one can stole their information, purpose of this paper is to introduce the two step Authentication, Two Step authentication asks for permission to do transitions.

KEYWORDS: Online banking, Mobile backing, One-time password ,Two step authentication.

I. INTRODUCTION

Now a day lot of peoples gives preference to use online or mobile banking, So that numbers scams happening around us and count of scammers are increased day by day. For that Two steps authentication is the way to secure our account from scammers. It provides a detail of transaction and ask user about that transaction, in case of one-time password it only gives a code number and a message to do not share code with other guys, but for two step authentication it will notify all details of transaction. And because ofthat user can protect their accounts from scammers. The Internet is that the fastest growing banking channel today, both within the fields of corporate and retail banking. The development is no longer just driven by the banks' desire to reduce costs: first and foremost, it is a manifestation of customers' demand to access bank services online at any time and from any location. The importance of Internet banking is clear for several reasons. Firstly, it offers a cost-efficient alternative to telephone and branch banking due to the relatively low capital and maintenance costs, and its fully-automated processing of most transactions. Secondly, it offers unparalleled customer convenience by enabling 24-hour access to a wide range of services.

II. RELATED WORK

1.Threats and Countermeasures

- **Attacks on Internet Banking-**

The first 'phishing' emails targeting on-line financial systems were seen in 2001, as a 'Post 911 ID check' following the September 11 attacks on the World Trade Centre1 . From 2004 onwards, the industry has seen a dramatic rise in attacks against both large and little financial institutions worldwide. In parallel with this growth in attack volume, there has been a parallel rise within the variability and complexity of attacks. Banking security experts must now be conversant in a bewildering array of techniques and terminology: phishing, pharming, spear phishing, session hijack, man-in-the-middle, man-in-the-browser, Trojans, Rock Phish…the list goes on. Despite the range in attack methods, most aim to achieve an equivalent objective: to get confidential user information, like usernames, passwords, Mastercard numbers and Social Security numbers.
These are all static credentials they don't change and therein lies the problem.
Once obtained, they will be employed by the attacker to impersonate the customer to perpetrate fraud.

| DOI: 10.15680/IJIRCCE.2021.0905034 |

1.2 Two-Factor Authentication

Whilst it's useful to undertake to counter specific attacks (and as a part of a layered security strategy, we might always recommend this), the sole long-term, strategic solution is to maneuverfaraway from the present dependence on static credentials. Traditionally, all authentication mechanisms are often placed into one among the subsequent three categories:

· Something you know—a secret, like a password.
· Something you are—a biometric, like a fingerprint.
· Something you have—a device or object or some kind, like a MasterCard .

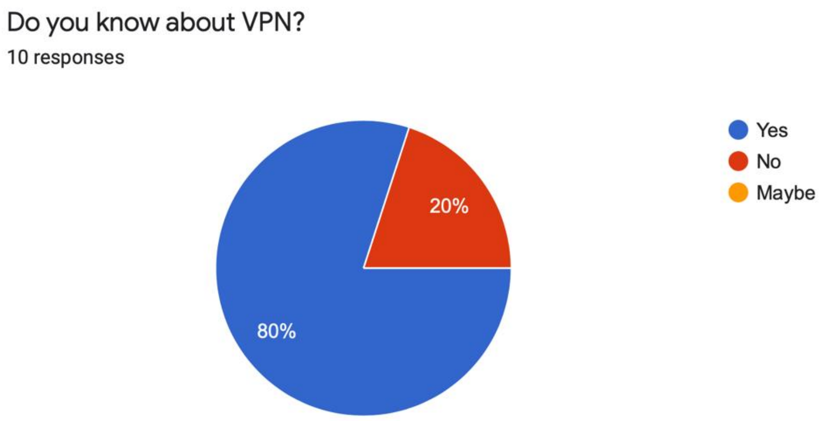
With this approach, it can readily be seen that the issues with phishing arise from an overreliance on the primary category. Strong authentication are often achieved by employing two different authentication credentials in parallel, from different categories this is often often mentioned as Two-Factor Authentication (2FA)For reasons of cost, complexity, reliabilityand privacy, biometrics aren't widely utilized in banking. There are however a good sort of low-cost, dependable security devices available. Typically, such devices generate and display a One-Time Password (or OTP)because the name suggests, an OTP is valid for one use only, and lots of also are time-limited. instead of being static, OTPs are dynamic—new OTPs are often generated on demand, from an inexhaustible sequence that's unique to every device. The OTP is copied from the device to the online terminal by the customer. To the bank, knowledge of a legitimate OTP demonstrates proof of possession of the device, which when including a standard static password offers a particularly effective defence against online attacks.

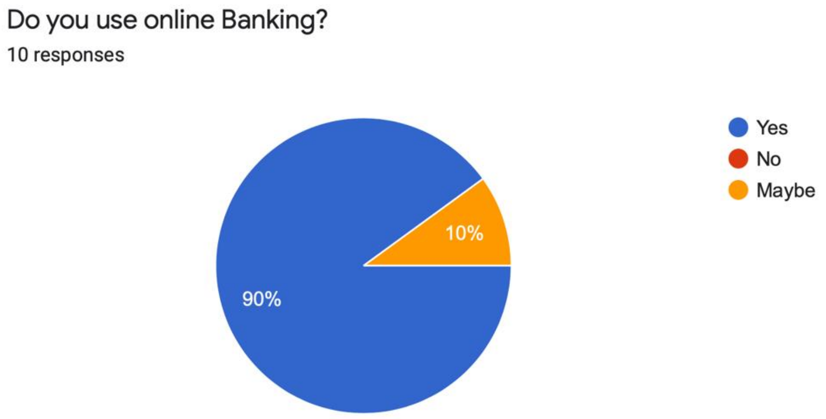
1.3 Attacks Against 2FA

Few fruitful assaults against 2FA-empowered Web banking frameworks have prompted press reports that 2FA as an overall methodology has been 'broken'. the truth is quite more complex, as we shall discuss below. An attacker may obtain a legitimate OTP from a customer using an equivalent methods as those wont to obtain a static password.If the bank has deployed an easy systemwith 2FA utilized for login just, this assault may succeed. To understand the way to mitigate or eliminate this risk, it's first necessary to know how attackers operate. instead of one individual or organisation being responsible, attacks are administered by loose associations of people or groups, each with their own specialist role. Different parties cooperate, each providing a service: creating a fake internet site , sending spam email, collecting passwords, and eventually using those passwords to get cash.Passwords and different accreditations are purchased and sold between groups, this requires some serious energy. Since most OTPs include an expiry mechanism, the attacker’s standard operating model is no longer effective, and a considerably more complicated model of real-time attacks is being adopted. This clarifies the proceeding with techonology advances in on-line assaults which we examined before. is that this a never-ending race , or will there eventually be an outright winner? Cheerfully, the most grounded kinds of 2FA accessible today offer a long haul, provably secure arrangement. The way’s to move from validating the client, to verifying the exchange which the client wishes to perform. The client experience stays straightformple: the user simply enters the beneficiary account number and transaction amount into their authentication device, by means of an integral keyboard. The OTP thus created acts as a digital signature on those transaction details—even if obtained by an attacker, the OTP can't be used for the other purpose. Whilst this step might not be necessary today, many banks are deploying 2FA solutions with the choice to upgrade to transaction authentication within the future. By this route, their customers first gain familiarity with the only sort of the technology, and therefore the bank is strategically placed to reply to future threats.

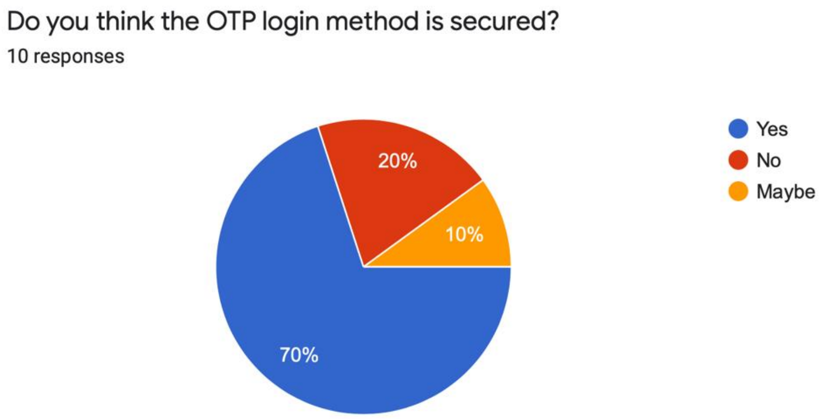
III. LITERATURE SURVEY

We did a survey on how many people are aware about scam happen on internet and after survey we got some data.
So out of 10 people 8 peoples know about VPN, VPN is a virtual private network this Add another level of security.

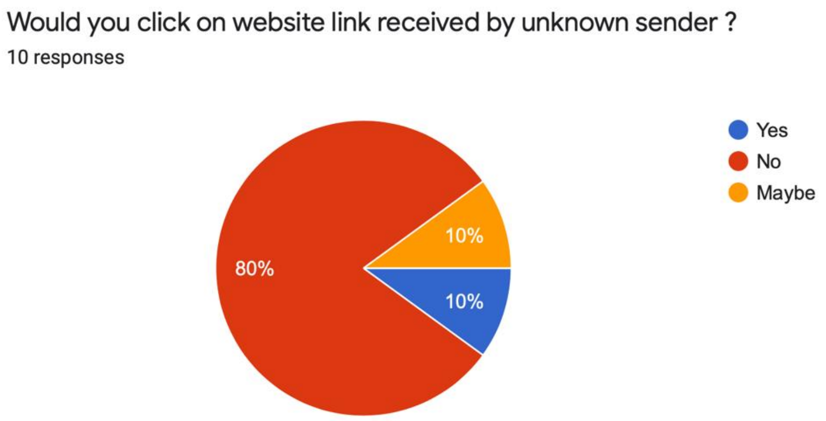

Do you know about VPN?
10 responses


Do you use online Banking?
10 responses

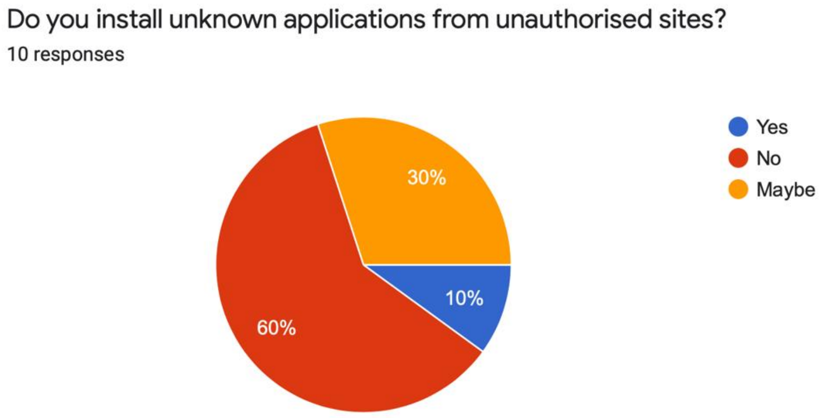
90% of peoples are using online banking as we can see it’s important to be aware about 2FA.


Do you think the OTP login method is secured?
10 responses

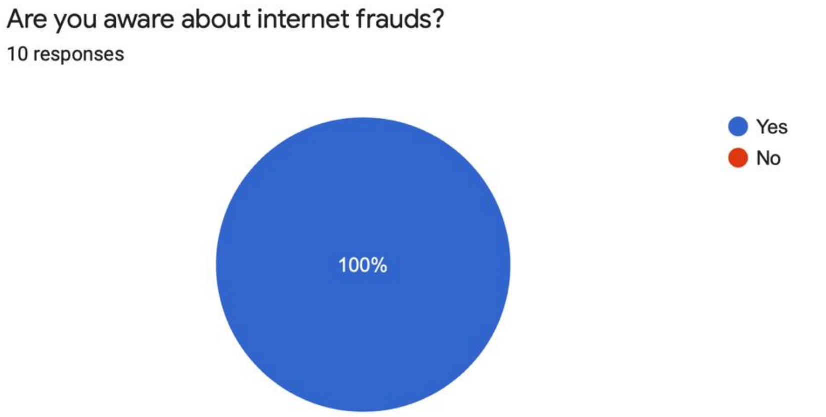
70% of peoples think that one time password login is a secured method and 20% of peoples think its not completely secured.



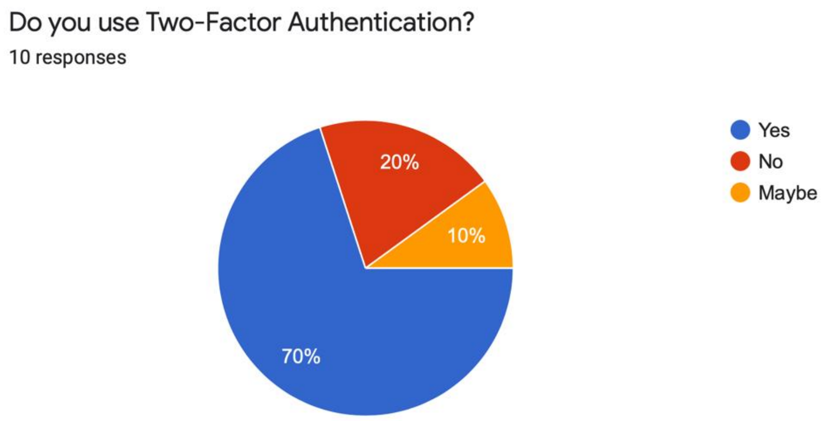
80% people are strongly saying that they are not opeaning website link link from unknown sender and 10% people open that link and 10% of people are not sure.



10% of the people are installing app's from unauthorised site and they are taking risk on security of their device and 30% of peoples are not sure they might sometimes install app's from unauthorised sites**.**



100% of peoples are strongly agreed they are aware about scam's on internet.



70% of people are using Two-Factor Authentication on their account and 20% of peoples are not using and 10% of people are not aware about this And this survey says that lot of people are about 2FA and they are using this security layer on their accounts but they are not aware about how 2FA can also compromise.

IV. PROPOSED ANALYSIS APPROACH

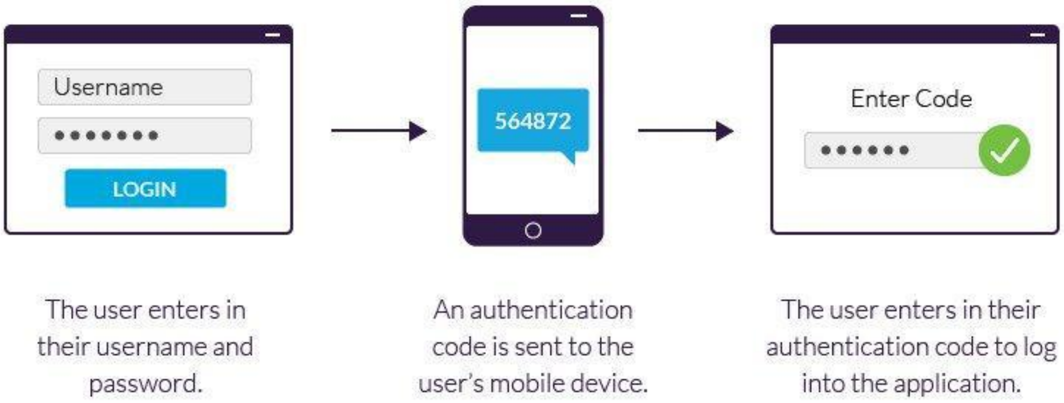
Spear-Phishing:

Activity Emmental assaults start with spear phishing messages, sent in a client's neighborhood language, that have malware connected. On the off chance that clients execute the malware, which might be veiled as a Windows update device, the malware changes their framework's settings to highlight an assailant controlled Area Name Framework, along these lines permitting aggressors to listen in and control all HTTP traffic. The malware additionally introduces its own Protected Attachments Layer endorsement.

The malware additionally introduces its own Protected Attachments Layer authentication. "This permits the assailants to show content from secure phishing destinations without setting off a notice from the program, To make the assault hard to recognize, the malware then erasesitself, leaving only the altered configuration settings. At the point when clients with contaminated PCs attempt to get to the bank's site, they are rather highlighted a Malwaresite that resembles that of their bank.

So starts stage two of the assault: When clients sign into the phony - yet genuine looking - banking site, they're told to download and introduce an Android application to produce one-time tokens for signing into their bank. "Actually, it will capture SMS messages from the bank and forward them to an order and-control worker or to another cell phone number. This implies that the cybercriminal not just gets the casualties' web based financial qualifications through the phishing site, yet additionally the meeting tokens expected to bank online too.The criminals end up with full control of the victims' bank accounts all would likely appear normal to their bank. ""By taking the capabilities and compromising the approved gathering of the customer, it looks like a customer is just dealing with a common financial trade This, joined with the truth that the PC malware isn't constant, takes into account these programmers to limit their profile and simultaneously direct bank heists across 34 distinctive monetary foundations in Europe and Asia.

Authentication Methods


Username
•••••••
LOGIN
564872
Enter Code
••••••
The user enters in their username and password.
An authentication code is sent to the user's mobile device.
The user enters in their authentication code to log into the application.

Any bank considering deploying 2FA must choose between a wide range of possible authentication devices. The following list, whilst not exhaustive, gives a representative sample.

3.1 EMV Card and Reader
MasterCard has contrived a plan dependent on existing retail banking keen cards and PINs. Dubbed the Chip Authentication Program (CAP), it has also been adopted by Visa, under the Dynamic Passcode Authentication (DPA) banner. The client is provided with a little, hand-held card peruser, into which their current EMV 'Chip and PIN' card is embedded. On entering the card PIN, the chip on the card is utilized to produce an OTP, which is shown on the peruser's screen. Extra capacities on the peruse additionally support exchange confirmation. The benefits incorporate a high security, while by utilizing existing cards and issuance measures arrangement and the board costs are decreased. In any case, the client experience, while natural, is more confounded than with different tokens.
3.2 Hardware & Software OTP Tokens
Many vendors give OTP-generating tokens. they are gettable throughout a giant choice of shapes and sizes, and lots of give custom disapproval selections. solely|the best tokens ar applicable for user authentication solely. plenty of advanced tokens incorporate a keyboard, making them applicable for dealing authentication. Most vendors use proprietary algorithms to come back up with the OTPs. However, the Initiative for Open Authentication (OATH, see www.openauthentication.org) is Associate in Nursing business pool promoting standardisation and talent.

3.3 Hardware-based PKI Tokens.
A PKI system employs a personal key, wont to create digital signatures that area unit valid employing a public key. the general public secret is control by the bank, and also the personal key by the client. Chip-card or USB devices area unit unremarkably wont to secure the customer’s personal key. Since PKI tokens cannot generate OTPs, they have to instead be connected to the customer’s laptop. Devices and keys area unit typically managed employing a Certificate Authority. they provide a high security level, though PC-based attacks might use the token illicitly. By as well as the power to sign transactions and alternative directions, they provide nice flexibility to banking applications. As a result, they're a lot of common in business banking than shopper banking.

3.4 SMS-based OTPs
An appealing different to deploying tokens is to use one thing the client already has—their portable. during this case, the bank generates the OTP associate degreed sends it to the client as an SMS message. The client returns the OTP to the bank through their applications programme. Naturally, this approach depends on the bank maintaining current details of the client’s sign and therefore the customer having the ability to receive messages at the actual moment of login. in addition, a dealing outline could also be enclosed within the SMS. this allows the user to discover fraudulently changed transactions.

| DOI: 10.15680/IJIRCCE.2021.0905034 |

3.5 TAN Lists

TAN (Transaction Authentication Number) lists square measure paper-based lists of one-time passwords. they're firmly generated by the bank and issued to every client. The client provides associate degree OTP anytime login or submits a dealing. The OTPs square measure either employed in sequence, or the bank requests a selected OTP mistreatment associate degree index. while providing a lower security level, this low technology approach offers a mixture of simplicity, responsibility and low price.

3.6 Matrix Cards

Also referred to as grid card, this can be a random grid of numbers or letters generally written on a credit-card sized piece of plastic issued by the bank. The client is prompted to produce the contents of two or three cells throughout login or once submitting a dealing. for instance, the prompt "A4, C7" would offer the log-in response "5, 8" exploitation the cardboard shown. With similar blessings to TAN lists, the cardboard format is convenient and sturdy. while re-use of cells create the safety analysis less clear, it additionally permits for a additional versatile termination policy.

V. CONCLUSION

This paper focuses on the implementation of two-factor authentication methods using mobile phones. It provides the reader with an overview of the various parts of the system and the capabilities of the system. This paper gives overview who Two step authentication can be bypass using malware and technique called spear-phishing, this proposed system has two option of running, either using a free and fast connection-less method or a slightly more expensive SMS based method. Both methods have been successfully implemented and tested, and shown to be robust and secure. The system has several factors that makes it difficult to hack. Future developments include a more user-friendly GUI and extending the algorithm to work on Blackberry, Palm, and Windows-based mobile phones.

REFERENCES

[1]. Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011, October). A survey of mobile malware in the wild. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*.

[2]. Aloul, Fadi, Syed Zahidi, and Wassim El-Hajj. "Two factor authentication using mobile phones." In *2009 IEEE/ACS International Conference on Computer Systems and Applications*, pp. 641-644. IEEE, 2009.

[3]. Dmitrienko, Alexandra, Christopher Liebchen, Christian Rossow, and Ahmad-Reza Sadeghi. "On the (in) security of mobile two-factor authentication." In *International Conference on Financial Cryptography and Data Security*, pp. 365-383. Springer, Berlin, Heidelberg, 2014.

[4]. Order, USEUCOM Task. "Two-factor authentication." (2008).

[5]. Jin, Andrew Teoh Beng, David Ngo Chek Ling, and Alwyn Goh. "Biohashing: two factor authentication featuring fingerprint data and tokenised random number." *Pattern recognition* 37, no. 11 (2004): 2245-2255.

[6]. Wang, Ding, and Ping Wang. "Two birds with one stone: Two-factor authentication with security beyond conventional bound." *IEEE transactions on dependable and secure computing* 15, no. 4 (2016): 708-722.

[7]. Mail, A. O. L., and Drop Box. "Two factor authentication." (2017).

[8]. Wang, Ding, Debiao He, Ping Wang, and Chao-Hsien Chu. "Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment." *IEEE Transactions on Dependable and Secure Computing* 12, no. 4 (2014): 428-442.

[9]. Karapanos, Nikolaos, Claudio Marforio, Claudio Soriente, and SrdjanCapkun. "Sound-proof: Usable two-factor authentication based on ambient sound." In *24th {USENIX} Security Symposium ({USENIX} Security 15)*, pp. 483-498. 2015

[10]. https://www.cryptomathic.com/hubfs/docs/cryptomathic_white_paper-2fa_for_banking.pdf Accessed on 7 march 2021

[11]. https://lifars.com/2020/02/mobile-banking-users-are-targeted-by-sms-based-phishing-attacks/ Accessed on 7 march 2021

[12]. https://duo.com/blog/bypassing-googles-two-factor-authentication Accessed on 7 march 2021 addition to the use of Bluetooth and WLAN features on mobile phones for better security and cheaper OTP generation