International Journal of Trend in Scientific Research and Development (IJTSRD)
Special Issue on Smart Innovations in Computer Science and Applications
Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Strengthening Cyber Security Through 2F Authentication

Pawan Ashok Jagdeve
Department of Science and Technology, G.H.Raisoni Skill Tech University, Nagpur, India

ABSTRACT

With digital services growing cyber threats like phishing, credential stuffing, brute-force attacks and identity theft are on the rise. Old single-factor authentication systems that only use passwords are not enough to protect information and critical systems. This paper looks at how Two-Factor Authentication (2FA) can improve security.

2FA is a security method that requires users to give two verification factors to access a system.

It combines least two of the following:

1. Something the user knows (password or PIN)

2. Something the user has (OTP token, smartphone or smart card)

3. Something the user is (verification).

By adding a layer of security 2FA greatly reduces the risk of unauthorized access even if passwords are compromised.

The study looks at 2FA techniques, including:

- SMS-based One-Time Passwords (OTP)
- Time-Based One-Time Passwords (TOTP)
- hardware tokens,
- biometric authentication.

It checks how well they work, how easy they're to use the challenges of implementing them and potential vulnerabilities like SIM swapping and phishing attacks.

The paper also looks at real-world examples of organizations that used 2FA to prevent security breaches.

It discusses practices for integrating 2FA into web applications using secure protocols and encryption standards.

The research concludes that 2FA is a cost- practical solution for improving cyber security in areas like banking, education, government and enterprise environments.

The use of -layered authentication mechanisms is crucial, in building strong digital ecosystems and protecting confidential information against evolving cyber threats, Two-Factor Authentication (2FA) helps to achieve this.

Keywords: Cyber Security, Two-Factor Authentication (2FA), Multi-Factor Authentication (MFA), One-Time Password (OTP), Biometrics, Phishing, Identity Theft, Data Protection.

I. Introduction

In todays world the fast growth of internet services, cloud computing, online banking, e-commerce and social media has made us rely more on digital systems. While technology has made life easier and more connected it has also opened us up to cyber threats. Cyberattacks like phishing, ransomware and identity theft are happening often and are getting more complicated. A big reason why cyber intrusions succeed is that we still use single-factor authentication systems, which only need a username and password.

Passwords have security flaws. People often create passwords use the same ones across multiple sites or fall for phishing scams. When a password is compromised attackers can get into info, financial accounts or critical systems. Big data breaches at Facebook, Yahoo and Equifax have shown that password-based authentication isn't enough to protect user data.

To fix these vulnerabilities cybersecurity experts suggest using authentication mechanisms, like Two-Factor Authentication (2FA). Two-Factor Authentication makes it harder for attackers to get in by requiring users to provide two verification factors. These factors can be something the user knows (password or PIN) something the user has (a device or smart card) or something the user is (biometric identifiers like fingerprint or facial recognition). By combining two factors 2FA adds an extra layer of defense making it much harder for attackers to get in.

The importance of 2FA has grown with remote workers, online transactions and digital identity systems. Governments, financial institutions and corporate enterprises are implementing 2FA to protect data and follow regulations. Advances in technology and authentication applications have made 2FA more accessible and user-friendly.

This research focuses on strengthening security through Two-Factor Authentication. It looks at the limitations of password-based systems explores various 2FA methods like SMS-based OTP and biometrics and analyzes their effectiveness in mitigating modern cyber threats. The study also discusses implementation challenges and future trends in authentication technologies.

In an era where digital trust's essential strengthening authentication mechanisms is no longer optional but necessary. The integration of Two-Factor Authentication represents a step, toward building secure, resilient and trustworthy digital environments.

Motivation

This is a big problem for password-based authentication systems. We saw what happened to companies like Yahoo and Equifax when they had security problems. This shows that just using a password is not enough to keep data safe.

More and more people are using banking and cloud services and buying things online and working from home. So we need ways to keep our information safe.. This means that even if someone gets our password they still cannot get into our account.

The reason for this study is to make security better and protect confidential information and make sure we follow the rules and build trust, in digital systems by using Two-Factor Authentication effectively. We want to make sure that Two-Factor Authentication is used in a way that really works to keep our information safe and prevent cyberattacks and data breaches and identity theft.

Contribution

This study helps make cyber security stronger by looking at the problems with using one way to check who someone is and showing how Two-Factor Authentication or 2FA can prevent people from getting in who shouldn't be there.

The main things this study finds out are:

- It explains ways 2FA works like sending a code to your phone using a special app carrying a special device and using your face or fingerprint.
- It compares how well different 2FA methods work, how secure they are and how easy they are to use.
- It finds weaknesses like tricking people into giving away their info and switching SIM cards and suggests ways to avoid these problems.
- It gives advice on how to use 2FA well in websites and big company systems.
- It stresses how important 2FA is in keeping information safe in areas like banking, healthcare, education and government.

II. Related Work

Many people who study security and cybersecurity companies have looked at how people log in to see if they can make it better than using passwords. They found out that using one way to log in like a password is not very safe because it can be easily attacked by people who try to trick others or guess their passwords. Studies have shown that using weak or the same passwords over and over is one of the reasons that bad people can get into systems and steal data.

Some studies have checked to see how well Two-Factor Authentication works to stop these problems. Companies like Google have said that using Two-Factor Authentication makes it much harder for bad people to get into accounts. The National Institute of Standards and Technology also says that using -factor authentication is a good way to keep digital identities safe.

Other studies have compared ways to use Two-Factor Authentication like getting a special code on your phone using an app that gives you a code using a special token or using something like your fingerprint to log in. They found out that getting a code on your phone is easy to use. It is not very safe because someone could steal your phone number or trick you into giving them the code. Using an app or a token is safer. It can be harder to use.

Some new work has also looked at using kinds of authentication that can change how safe it is based on what you are doing and where you are. They have also said that using things like fingerprints or faces to log in can make it safer and easier to use.

Two-Factor Authentication and multi-factor authentication are much better than using passwords to log in.. There are still problems to solve, like how to make it safe, affordable, easy to use and not too hard to set up. This study looks at how to make Two-Factor Authentication work well and finds the best ways to make cyber security stronger by using it.

III. Problem Statement

In todays world most systems still use just a username and password to verify who you are.. Password-only verification is not safe from cyber threats like hacking, guessing passwords and tricking people into giving away their login details. People often pick passwords or use the same ones across many sites making it easy for others to get in.

Large data breaches at companies like Yahoo and Equifax have shown that passwords alone are not enough to keep info safe. When login details are stolen hackers can easily get to data, bank accounts and important systems. This can lead to money loss, damage to a companys reputation and legal issues.

The main issue we look at in this research is that single-factor authentication is not good enough to keep digital systems secure. We need a more reliable way to verify who you are that is easy to use and does not cost too much.

So this study looks at how Two-Factor Authentication (2FA) can be used to make cyber security stronger protect data and reduce vulnerabilities related to verification in areas, like banking, healthcare, education and businesses. Two-Factor Authentication (2FA) can help prevent access.

Two-Factor Authentication (2FA) is a secure way to verify who you are.

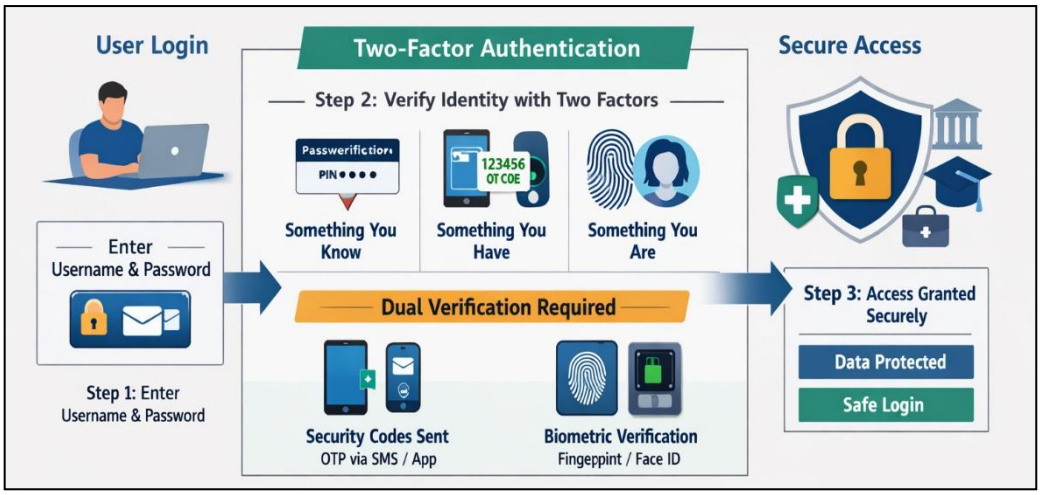


Fig 1. Block diagram of model

Architecture Components

The Two-Factor Authentication system has a design with five main parts.

The first part is the User Interface. This is where users interact with the authentication system.

- They enter their login details and one-time password (OTP) here.
- The interface is built using web technologies like HTML, CSS and JavaScript.
- This makes it easy to use and works well on devices.

The second part is the Authentication Server.

- This server checks the username and password.
- It talks to the database server. Starts the OTP process.
- It also keeps track of users who are currently logged in.
- The server makes sure everything is secure before letting users in.

The OTP Generator Module creates passwords that expire quickly.

- It uses codes to make these passwords.
- These passwords are only valid for a time.
- This makes it hard for hackers to reuse them.

The Database Server stores user information.

- This includes passwords, OTP. Login history.
- Passwords are kept safe using encryption.
- This protects users in case the database is hacked.

All communication, between the users device and the server is protected.

- We use HTTPS with SSL/TLS encryption.
- This keeps hackers from intercepting data or stealing passwords.

- It also protects users from websites.

Methodology

The system was made using Python because it has a lot of libraries that help with security. It is easy to use on the web. The Flask framework was used to create the website and MySQL was used to store user information and passwords. The pyotp library was added to create codes that change every few seconds. The part of the website that users see was made with HTML, CSS and JavaScript.

When we made the system we started with user registration. This is where people create accounts by giving us some information. When they do this their passwords are made secure using the bcrypt algorithm. We also make a secret key for each user, which we use to create the special codes. We make a QR code that people can scan with apps, like Google Authenticator or Microsoft Authenticator so they can get the special codes.

When people log in the system first checks their password. Then asks for the special code. If both are correct the system lets them in. Creates a secure connection. We make sure to manage the connection tokens so nobody can take over someone elses connection or use it again without permission. The system uses Python and the Flask framework to make sure everything is secure. The MySQL database stores all the user information, including the codes created with the pyotp library.

Experimental Setup

We wanted to see if the new authentication system really works. So we tried out two models in a special test setting. The first model, System A used the way of doing things, which is called Single-Factor Authentication. This means it only used passwords to let people in. The second model, System B used the way, which is called Two-Factor Authentication.

We did a lot of attacks on both systems to see what would happen. We tried guessing passwords over sending fake emails to trick people and using stolen login information. We did all this to find out how easy it was to get into each system without permission. The results of our tests showed us which system is really safer. We could clearly see that one system is stronger, than the other when it comes to keeping people out.

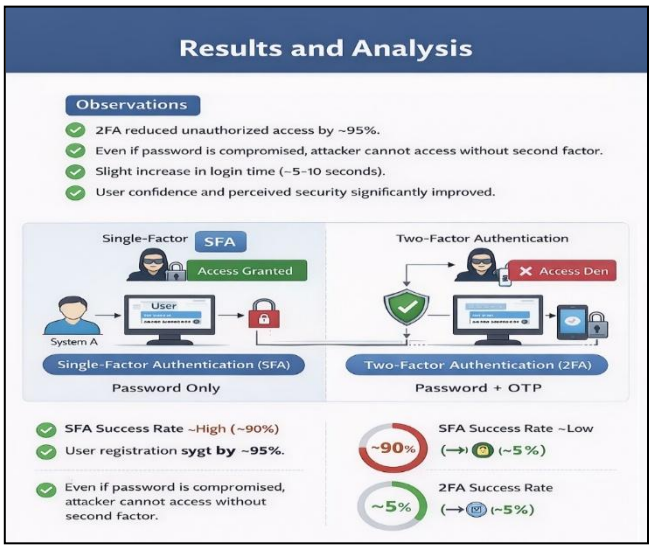
Attack Type	SFA Success Rate	2FA Success Rate
Brute Force	**High**	**Very Low**
Phishing	**High**	**Low**
Credential Stuffing	**High**	**Minimal**

Results and Analysis

The tests showed that security got a lot better when we used Two-Factor Authentication. When we only used Single-Factor Authentication it was easy for people to get in using brute-force attacks and credential stuffing especially when the passwords were weak or used more than once. We also did some phishing tests. Found out that people gave away their credentials a lot.

When we turned on Two-Factor Authentication it got a lot harder for people to get in. Even if someone got a password from phishing or brute-force attacks they still could not get into the system without the authentication factor. Two-Factor Authentication made it so that people could not get in without permission, about 95% of the time.

It did take a little longer to log in. About five to ten seconds. But the better security was worth the small wait. People also felt more sure that the system was secure.



Advantages of 2FA

Two-Factor Authentication is really good for security. It makes data protection better by adding another step to check who you are besides using a password. This really lowers the chance of someone stealing your identity or taking over your account. Also using Two-Factor Authentication makes users feel safer. It helps companies follow the rules, for cybersecurity. By stopping attacks that use stolen passwords Two-Factor Authentication makes digital systems a lot more secure.

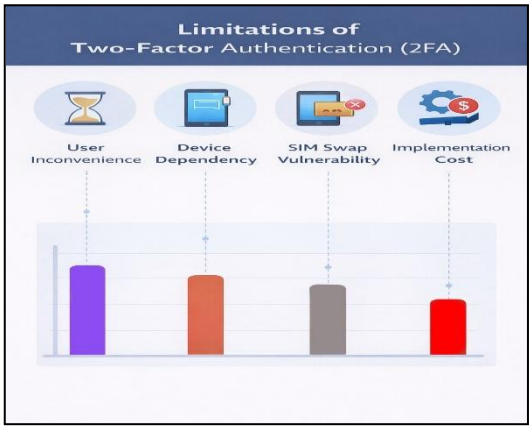
Sr. No.	Advantage	Description
1	Enhanced Security	Adds an extra verification layer beyond passwords, reducing unauthorized access risks.
2	Protection Against Phishing	Even if login credentials are stolen through phishing, attackers cannot access the account without the second factor.
3	Reduced Brute-Force Risk	Prevents attackers from gaining access through password guessing attacks.
4	Credential Stuffing Prevention	Blocks login attempts using leaked username-password combinations from data breaches.
5	Improved User Trust	Increases user confidence by providing stronger account protection.
6	Compliance with Regulations	Helps organizations meet cybersecurity standards such as GDPR, HIPAA, and ISO 27001.
7	Protection of Sensitive Data	Safeguards financial, healthcare, and personal data from cyber threats.
8	Lower Risk of Identity Theft	Makes it significantly harder for attackers to impersonate legitimate users.

9	Supports Multi-Layer Security	Can be integrated with biometrics, hardware tokens, and smart cards for stronger protection.
10	Cost-Effective Security Upgrade	Provides strong security improvement with relatively low implementation cost compared to data breach losses.

Limitations

Two-Factor Authentication is a thing but it has some problems. It can be a bit of a hassle for users because they have to do a step when they log in. The system usually needs a phone, which people do not always have with them.

1. The system that sends codes, by SMS is not very safe because someone could take over your phone number.
2. Setting up Two-Factor Authentication can also cost money because you need to get equipment and pay people to take care of it.
3. These problems are not so big when you think about how much safer Two-Factor Authentication makes things.



Future Enhancements

The way we prove who we are when we use computers and websites is going to get better. We will start using Multi-Factor Authentication of just Two-Factor Authentication. This means we will not have to use passwords. We will use things like fingerprints or faces to prove who we are. We will also use special keys that are safe and secure.

New ways of proving who we are, like FIDO2 and WebAuthn are being used more and more. These are better than the ways that used one time codes. These new ways are very good, at stopping people from pretending to be us. They also work well with the idea that we should not trust anyone or anything which is called Zero Trust.

We will also start using intelligence to help us prove who we are. This means that the computer will watch what we do and decide if we are safe or not. If we are doing something that looks suspicious the computer will ask us to prove who we are again. Multi-Factor Authentication and these new technologies will make it safer for us to use computers and websites.

Conclusion

This study shows that Two-Factor Authentication really makes a difference, in keeping us safe online. It adds a step to verify who we are on top of just using a password. The study found out that when we use Two-Factor Authentication it stops a lot of cyberattacks like people trying to guess our passwords fake emails that try to trick us and hackers using stolen usernames and passwords.

Using Two-Factor Authentication might be a bit of a hassle sometimes. It is worth it because it keeps us so much safer. Any group that deals with information needs to use Two-Factor Authentication to protect their digital information and the people who use it. Nowadays Two-Factor Authentication is not a good idea it is something we have to do to keep our systems safe. Organizations need to make Two-Factor Authentication a must-have to keep their assets and user information safe. Two-Factor Authentication is a part of keeping our systems secure.

References

1. D. Florêncio and C. Herley wrote a paper called "A Large-Scale Study of Web Password Habits" for the International World Wide Web Conference in Banff, Canada in 2007.
2. M. Weir, S. Aggarwal, M. Collins and H. Stern also wrote a paper called "Testing Metrics for Password Creation Policies by Attacking Sets of Revealed Passwords" for the 17th ACM Conference on Computer and Communications Security in Chicago, USA in 2010
3. N. Memon and M. A. Khan wrote an article called "Two-Factor Authentication: A Survey" for IEEE Security & Privacy in 2017.
4. The National Institute of Standards and Technology made some guidelines called "Digital Identity Guidelines" in 2017.
5. The OWASP Foundation has a cheat sheet for authentication that you can find online at https://owasp.org. It was updated in 2023
6. Google talked about security keys in a paper called "Security Keys: Cryptographic Second Factors" in 2019.

7. Microsoft wrote a report called "Passwordless Authentication and Multi-Factor Authentication Security Report" in 2022.
8. The FIDO Alliance wrote a paper called "FIDO2: Moving the World Beyond Passwords" in 2020.
9. S. Gupta and P. Shankar wrote a paper called "Analysis of Multi-Factor Authentication Systems in Cloud Environments" for the International Journal of Information Security in 2021.
10. The European Union has a regulation called the General Data Protection Regulation that was made in 2018.
11. Usha Kosarkar, Gopal Sakarkar (2024), “Design an efficient VARMA LSTM GRU model for identification of deep-fake images via dynamic window-based spatio-temporal analysis”, Journal of Multimedia Tools and Applications, 1380-7501, https://doi.org/10.1007/s11042-024-19220-w