HKIE THE HONG KONG INSTITUTION OF ENGINEERS 香港工程師學會

# Adaptive multi-factor authentication system for detecting the irregularities for sensitive application

**Vidhyasagar BS, Vustepalley Mani Manjunath, Soma Prathibha, Dasari Vasu and Innamuri Sairam**
Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India

## ABSTRACT

MFA Multi-Factor Authentication has become one of the crucial security methods to fight against cyber threats. This paper discusses the MFA techniques and draws inspiration from the previous existing papers, reports, and cyber security frameworks which focus on the various methods of authentication like biometrics, security keys, etc. The traditional methods are based on the static authentic layers, which are vulnerable to threats. This paper proposes a Dynamic Threat Level Detection System to continuously monitor user behaviour and change the authentication levels based on the irregularities detected. The threat level ranges from 0 to 5. The level increases in the response to suspicious activities. A Split One-Time Password (OTP) Mechanism is integrated into the proposed work where the six-digit OTP is divided into two and is sent separately to the mail and the user's phone number which prevents the attackers from intercepting the OTP. At higher levels, a fake password interface is designed where the user must enter the hidden original window to enter the password; this process is only known to the user. An extra security method, i.e., the Song-Based Authentication method is introduced at the highest level where the users select a particular segment of a preloaded song. If the user passes all the levels, a biometric verification is performed, and if any wrong input is detected, the system shuts down immediately to prevent access to unauthorised people. This method enhances the resistance to phishing and brute force methods. The research has further integrated AI for anomaly detection and blockchain-based process authentication which provide a defensive mechanism against fast-improving cyber threats.

**KEYWORDS** multi-factor authentication (MFA), cyber threats, dynamic threat level detection, split OTP Mechanism, song-based authentication, AI-based anomaly detection, blockchain, phishing, brute force.

**CONTACT** Vidhyasagar BS vidhyasagar_bs@hotmail.com
Received 9 March 2026

## 1. Introduction

### *1.1. Background*

The fast-paced moving world is increasing its dependence on digital services and hence the need for a secure authentication process is growing significantly. MFA is a security mechanism that requires user verification through some independent factors like passwords, PINS, OTP, security tokens, biometric data, etc.

MFA has greatly evolved through the years, but is still static and implements the same level of security checks irrespective of user behaviour. The lack of adopting different security measures is leading to vulnerabilities in the modern era of cyber threats and attacks.

### *1.2. Existing evidence*

There are many studies related to MFA systems whose primary aim is to improve security. Perara et al. (2025) proposed a biometric-based MFA that integrates fingerprint and heart rate detection which improves the authentication by 20%, but the system was very prone to biometric spoofing and the lack of a behavioural adaptive nature. Patel and Shah in the year 2025 introduced an MFA framework for the Internet of Things security which has a dynamic feature of adjusting the authentication complexity based on the device power capacity, but it also failed to be appropriate for real-time user behaviour.

Some recent advancements in MFA focus on the adaptive method of authentication where the system can dynamically adjust the authentication layers based on the context information like the location of the device, time of the login, and patterns of the user. Still, the existing type of authentication method has no indicators for risks and does not integrate deceptive security techniques.

### *1.3. Research gap*

Even after the great evolution of MFA, there still exist some voids like

i. Static Layers – Many lack the adaptive nature during times of behaviour anomaly.

ii. Lack of Deceptive Mechanism – Current models have failed to develop the fake window of password entry and the split OTP method.

iii. Biometric interaction – Only a few systems have real-time facial recognition for the authentication to verify at the highest level of threat.

© 2026 The Hong Kong Institution of Engineers

### *1.4. Objective*

This research paper proposes a Dynamic Threat Level Detection Mechanism which is adaptive. It increases the complexity of authentication based on the security threat detected. The main objectives of this paper are:

i. Development of a Threat level score that ranges from 1 to 5, whose value increases with the increase in the irregular behaviour of the user.

ii. Integration of the Split OTP where half of the 6-digit number is sent to the e-mail address and the other half is sent to the phone number(message) of the user.

iii. Development of a Fake window that appears to be like the original, but it is not the original window. Only the genuine user would know the process of verification later.

iv. Integration of Song-based authentication which is at the highest level where the user must select a particular segment from the whole song; this method is used to prevent brute force attacks.

v. Integration of biometric image verification, which is at the last level, and only allows the genuine user to gain complete access.

### *1.5. Scope*

This research paper mainly focuses on authentication methods to improve security.

It explores adaptive authentication models, deceptive methods, and biometric verification processes to attack cyber threats.

The constraints of this research paper are:

i. Hardware-Based Authentication Tokens: The hardware tokens provide a strong security code which is hardware-based technology, but this paper focuses on software-based technology.

ii. Cloud-based: This paper is limited to only the local device of the user rather than a distributed cloud security model.

iii. Network-Level Threat detection: The user behavior is noted but the network intrusion detection is not within the scope of this research paper.

## 2. Literature review

The authentication methods have significantly evolved over the years starting from simple password to multi-factor authentication (MFA) techniques. It is evolving rapidly due to the increase in the number of cyber threats. The growing need for improved security has led to the emergence of MFA. Table 1 compares single-factor and multi-factor authentication:

Table 1. Comparison of SFA vs MFA.

| Single-factor authentication | Multi-factor authentication |
|---|---|
| Single-factor authentication solely depends on the password. | Multi-factor authentication depends on multiple verification factors. |
| It is highly vulnerable to attacks. | It is less vulnerable to attacks. |
| It has a user-convenient process. | It requires a few additional authentication steps. |
| It is widely adopted by most users. | The demand and usage is increasing rapidly. |

### *2.1. Studies related to the adoption of MFA*

i. MFA adoption trends

The 2023 study by Verizon showed that organisations saw a 90% reduction in account takeover incidents. The study also found that organisations which only use a single-factor password are prone to phishing attacks (Verizon, 2023).

ii. Effective MFA

Google conducted research in the year 2022 and concluded that the usage of MFA blocked 99% of automated bot attacks, 96% of phishing attacks, and 76% of targeted account takeover attempts. It demonstrates the benefits of MFA (Google Security Blog, 2022).

iii. User perception and challenges

Microsoft conducted a study in the year 2021 which concluded that MFA improves security, but the user interaction is not up to the mark. Thirty per cent of the users encounter inconvenience during the authentication process (Marques & Campos, 2022).

## 3. Proposed methodology

The paper proposes an adaptive authentication system which is state based in nature. The system moves through five security tiers based on the threat level of the user behaviour. The paper introduces a layered authentication framework. The system moves through the levels when any anomalies related to user behaviour occur. Level 3 of the system lets the user enter a split OTP which is divided into half between the SMS and the Email. At level 4, a fake user interface will test the authentication, where the user must click on a particular object on the UI leading to the original window. Level 5 is an audio check where the user has to select a particular song from among many songs for verification. At the next level, the biometric face should be verified. There is a defence mechanism which shuts down the system immediately when any irregularities occur at any level, thereby creating an environment which gives priority to the data integrity for the user.

### *3.1. Flow chart of the proposed methodology*

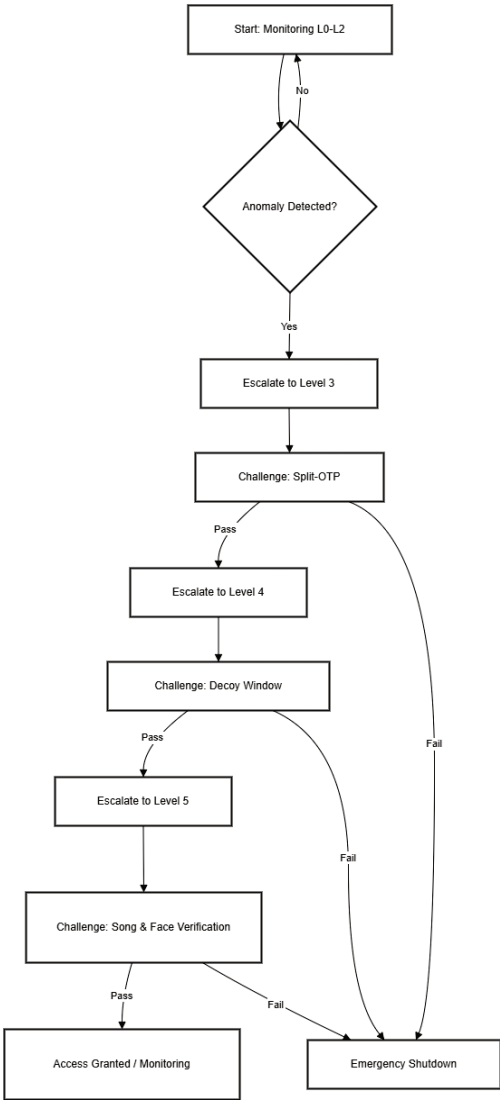



Figure 1. Flow chart.

## 4. Proposed framework for MFA

Figure 1 shows that the threat level mechanism is dynamic and monitors the user and system behaviour, allocating a threat level accordingly. This is to enhance the security of the system. The threat level ranges from 0 to 5. Every threat level provides an extra security setup for the mechanism. This is to ensure a robust authentication process throughout. The details of all the threat levels are mentioned below:

- Threat level 0 – The system is under normal conditions and undergoes a normal authentication process.
- Threat levels 1 & 2 – The system increases monitoring of behaviour; it checks for any anomalies.
- Threat level 3 – The system verifies using a split OTP where half of the 6-digit number is sent to the registered email address, and the other half is sent to the registered mobile number through SMS.
- Threat level 4 – The system presents a fake password entry window that is only known to genuine users, and it misguides unauthorised users, hackers, and attackers.
- Threat level 5 – The system requests the user to identify a specific part of a selected or preloaded song from a huge database which acts like a password.

If the verification process fails at any of the given levels, the system will shut down and remove all the changes made in it that were not saved.

Therefore, the whole process of authentication and verification is made more secure and robust.

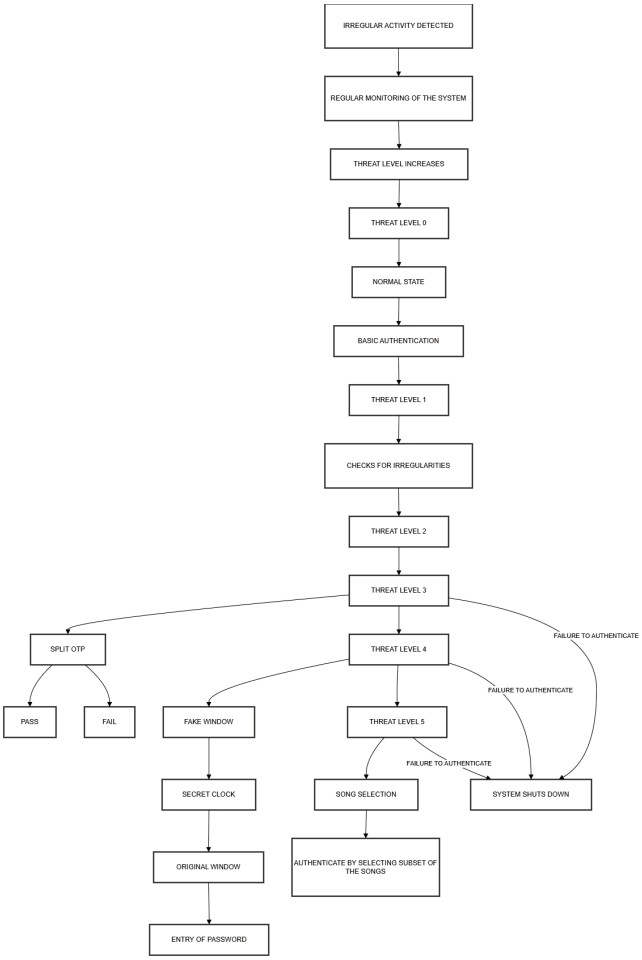



Figure 2. Threat level mechanism.

### *4.1. Authentication steps*

#### *4.1.1. Initial processes*

The user attempts to log into the system with his/her credentials. At this step, if the system detects any irregularities in the activity performed, the system itself increases its threat level to level 1. If the irregularities are normalised over a period of time, then the threat level is decreased to level 0. Concerning the threat level, extra security measures are taken to ensure extreme security of the device.

#### *4.1.2. Threat levels at a higher extent*

At threat level 3, an OTP authentication is performed. Here the OTP is split into two halves, that is, the 6-digit OTP is split into two 3-digit numbers. The first half is sent to the registered mobile number via SMS. The other half is received by the user through the email ID that is being registered by the user. The user should be able to enter both halves of the split OTP through the SMS and email ID accurately to log into the system. Attackers and non-genuine users cannot log into the system since they can receive the OTP, and they will not have access to the two halves of the OTP.

At threat level 4, a fake window appears for the user who is trying to log into the system. This level is to misguide non-genuine users. Only genuine users would know that the display is a fake window. The original window is hidden behind the fake window. The original window can be accessed using a secret button which would only be known to genuine users. When the user enters the original window, the user is supposed to enter the password, and if the user either fails to do so or enters the correct password in the fake window, the system considers both as wrong passwords and denies access to the system.

At threat level 5, the system displays a list of songs from the large database provided; the user is then requested to select one song from the list and then he/she should choose a segment from the particular song. If the segment matches the registered segment, then the authentication is successful; otherwise the system shuts down and deletes all the unsaved changes made to the system.

#### *4.1.3. Final security verification*

At a particular stage where all five levels are verified, the system requires an additional verification where the user must verify using facial biometrics. The image is compared with the registered image. If there is a mismatch between the two images the system then shuts down immediately as usual.

### *4.2. Algorithm of the system*

Step 1: Start the system by initially setting the threat level to 0.

Step 2: Regularly monitor the system and the user's activities to check for abnormalities.

Step 3: If any irregularities occur then the threat level would be increased to level 1.

Step 4: If the threat level reaches threat level 3, then the system asks for a security verification question and if the user answers the question with the registered answer, the threat level will decrease to threat level 1. If the user answers the verification question with a different answer compared with the registered answer, the system will continue the monitoring of the user activity.

Step 5: If the threat level is at threat level 4, then a fake window is shown to the user to misguide him/her. If the user enters the registered password on the original window, then the threat decreases to threat level 2. If the user does not enter the correct registered password at the original window accessed through the fake window, then the user/s activity would be monitored by the system as usual.

Step 6: If the threat level is at threat level 5, then the user is shown a list of songs from a huge database and is verified by selecting a particular segment of a particular song from the list of songs provided. This acts like a verification process for the user. If the segment is correctly selected in regard to the registered song by the user then the threat level decreases to threat level 3, but if the user is unable to select the registered song and the particular registered segment then the system shuts down then and there and all the changes made to the system during the verification session which were not saved by the system are deleted forever.

### *4.3. Implementation strategy*

#### *4.3.1. Behavioural analysis module*

The behavioural analysis module is used to monitor user patterns during the login, device identification, history of IP addresses, and other daily general usage routines. It is employed by AI technology anomaly detection to note all the irregular activities which are performed to ensure the high-end security of the system. All the possible threats can be found based on this method of approach.

#### *4.3.2. Split OTP mechanism*

The Split OTP mechanism is a method to ensure high security through both SMS and email. This ensures that cyber threats are prevented. These can be accessed only by genuine users.

#### *4.3.3. Fake window system*

A fake interactive login page is displayed to misguide fake users. A registered click or a keystroke will lead the user to the original window where he/she can enter the password. This acts as an extra additional security level. Attempts made by fake users are treated as an incorrect response despite it being the registered response on the fake login page.

#### *4.3.4. Song-based security authentication*

The song-based security authentication is a process where the user selects a particular segment from a particular song from a large set of songs. If the user inputs the exact segment as the registered one, then the authentication proceeds further in order to eliminate the brute force method utilised by fake users.

#### *4.3.5. Mechanism for shutting down access*

A high-level defence mechanism feature is added which stops the system's access upon authentication failure. This ensures that there are no unauthorised attempts, and the security is maintained throughout the process of verification.

### *4.4. Security benefits*

The brute force method of attacking is prevented by this procedure of verification through the mixture of many authentication windows which makes the process of guessing the password a virtual impossibility. The combination of OTP (split), face recognition, and the monitoring of activities makes it difficult to employ the brute force method of attacks.

The phishing process is also removed through this fake window preventing fake users from entering into the original window to gain access to enter the registered password. The traditional methods which allow phishing attempts to become a threat are now being enhanced to provide higher security.

Dynamic threat level adoption is a mechanism implemented to ensure that a high number of authentication steps are completed during the time of high risk of attack and lower number of authentication steps are required during the time of low risk of attacks, thus ensuring high security and a seamless experience for genuine users. By monitoring the current activity, the threat level would either increase or decrease accordingly. This process ensures security and user experience at the same time.

An attack prevention measure is included in the automatic shutdown of the system which guarantees that non-genuine users cannot have access to the data of the system. The shutdown is applied to all stages of threat levels and is a very effective way of ensuring solid security.

### *4.5. Upcoming challenges*

Users must be well trained and educated to verify themselves during the hidden fake window verification step and during the song-based authentication procedure. Basic knowledge of technology is required for the user to utilise the security mechanism provided to them.

The data provided during the biometric registration process like face and fingerprints should be stored securely. The processing of the registration must also be carried out in a highly encrypted manner so that no other person can have access to the registered biometric data.

This mechanism demands a device that is capable of handling high-security measures. The device should be compatible with different operating systems and various platforms to provide a seamless user experience while ensuring security at the same time. The device should also have hardware support for the registration of biometric data and its verification during the authentication process.

## 5. Threat model

Present-day verification systems experience multiple cyber-attacks. This proposed Multi-Factor Authentication (MFA) will override all these challenges by using a dynamic security setup. But like any other methodology of verification, there exist some threats and imperfections that must be addressed to ensure the highest level of security.

### *5.1. Possible threats*

Data breaching and credential theft are threats where the credentials of the genuine user are attractive to attackers. During the occurrence of a breach, the stolen data can be used by the attackers to gain access to the data of the system (Stallings, 2020).

Account hijacking is the process where the attacker gains access to the account and data of a user. This data can be used to manipulate sensitive information or to gain access to locations requiring authorised entry (Bonneau et al., 2015).

Brute force attacks involve the use of automated tools to guess the credentials of the user, OTPs, and song-based authentication till they receive access to the system (Armknecht et al., 2015).

Phishing is a major threat to this mechanism where users are deceived into revealing the credentials such as OTP and the secret method to enter the original window. There the attackers pass through the security levels without breaking the encryption mechanism (Sadeghi et al., 2015).

Device spoofing and impersonation attacks are emerging threats that have grown with the rise of fake technology. Non-genuine users can manipulate biometric verification systems using high-resolution images or AI-generated video that is built to resonate with genuine users. Such practices will allow access to non-genuine users (Dang & Matthews, 2020).

Denial of Service (Dos) attacks are also a major threat to the verification process. Attackers input a large number of fake requests to overwhelm the system so that it does not allow genuine users also to access their data, which means that data can be lost by the original user (Lee et al., 2018).

### *5.2. Strategies to prevent threats*

Strong authentication and adaptive security mechanisms ensure that the threat level adjusts its threat level dynamically concerning the activities of the user (Gasti & Rasmussen, 2019).

End-to-end encryption is maintained throughout the process of verification, which is done to ensure high security through OTPs, biometrics, and song-based verification processes which do not allow non-genuine users to gain access (Rivest et al., 1978).

Analysis of the behaviour of the system is a crucial feature in this mechanism. This allows the system to regulate the system's behaviour and detects any irregularities in the routine of the user (Ren et al., 2020).

Brute force methods of attacks are eliminated through the process of not allowing continuous verification failures, thereby increasing the security of the system overall.

The split OTP method of security verification would eliminate phishing attacks where the OTP is split and sent to the genuine user through email and message formats (Ye et al., 2020). The user interaction verification step is an additional feature where the non-genuine user does not know about the secret click to enter the original window to validate the password (Ahmed et al., 2021).

An automatic shutdown mechanism is applied throughout the verification process to ensure high security of the data of the system and the unsaved changes made till then would also be deleted. This prevents data access to non-genuine users as well (Li et al., 2021).

Hence, by adapting all these measures, multi-factor authentication guarantees high security without compromising the user interaction.

## 6. Security analysis framework

This is a crucial step in the development of any security mechanism. It is even more crucial in cloud-based verification mechanisms where there are many threats. This framework would enhance security through the dynamic threat level mechanism. This part of the research paper identifies the assets and threats, analyses potential risk factors, and proposes a few strategies.

### *6.1. Identification of the assets*

The security verification process begins with the identification of assets within the verification environment such as the credentials of the user like passwords, OTPs, biometric data, behaviour of the system, and dynamic threat levels. These assets play a major role in the system's functionality and user trust. There exist some imperfections still like the loss of data occurring in some scenarios, and failure to ensure end-to-end encryption which may hinder the importance of possessing the assets. In multi-factor authentication systems, the imperfect storage of the credentials of the users increases the chances of a non-genuine user to attack the system (Rathore et al., 2023).

### *6.2. Identifying threats*

There remain many threats to any security model. Providing a weak password during the registration process is a major threat since it can be retrieved by a non-genuine user easily through dictionary attacks (Zhou et al., 2021).

Phishing is also a major threat to the mechanism where a non-genuine user can manipulate a genuine user into revealing their credentials through mimicking a legitimate conversation. This can be to even a higher extent leading to a great threat to the user and a huge loss in data (Sahoo et al., 2021).

Malware-based threats are threats that note the keystrokes, intercept the OTP, and manipulate biometric verification. Many bluffing techniques are used to achieve this like generating a fake image of the original user using advanced Artificial Intelligence. The images generated also are generated at a high resolution to bypass the security levels with ease (Nguyen et al., 2022).

### *6.3. Analysing the risk factors*

The risks for this multi-factor authentication arise due to the lack of system complexity, sensitivity of the data, and the constraints during performance. The layered design of the system does improve its robustness but it also injects a complexity problem into the picture which has to be handled carefully. The imperfect implementation of the process may lead to improper verification choices and become a threat to data security.

Privacy issues may also be encountered while collecting and storing the credentials of the user. They may even arise while monitoring the system behaviour and the metadata of the location, and if the proper level of encryption is not maintained, this would lead to the violation of many data protection laws (European Commission, 2016).

Another risk factor is the time taken by the system to perform all these verification steps, playing a major role in the user interaction with the system. If the user interaction is not up to the user's expectation then there is no point in providing high-end security for the system's data.

### *6.4. Development of the framework*

The authentication method selector in the mechanism chooses the particular authentication method according to the priority of the user and its location, and time.

There exists a mechanism that continuously monitors the activity of the user, and the login behaviour of the user to check for any presence of irregularities in the user's behaviour.

A verification layer would apply the selected model from OTP, biometric recognition, and fake window. This layer would also shut down the system at a high level of threat.

An encryption layer would ensure that the credentials of the user are created and stored in a highly secure process. The OTP is split through two separate channels to reduce the interception risk. The biometric verification layer allows the user to verify themselves using either their facial

authentication or their fingerprints (Rathore et al., 2023; Zhou et al., 2021; Sahoo et al., 2021; Nguyen et al., 2022; European Commission, 2016).

## 7. Results

This part of the research paper describes the implementation of the multi-factor authentication mechanism in a cloud computing environment. Two main important factors are considered during this process which are the execution time of the verification process and the accuracy in detecting the anomalies which include false positive (FP) and false negative (FN) rates. Each layer of authentication is analysed concerning the increasing overload in the users who assess mechanisms' accuracy, reliability, and scalability (Ahmed et al., 2023).

The proposed multi-factor authentication (MFA) layers would be implemented with the help of six authentication layers (Ahmed et al., 2023):

1. Factor length
2. Factor checks
3. Factor value
4. Suspected user table check
5. User location verification
6. Browser name identification

Here each layer is executed in a sequence manner and the performance is measured in milliseconds. A range of 50 to 1,000 users are examined (Ahmed et al., 2023).

The factor length records the linear increase in the execution time which starts from 218 *ms* for the range of 50 users and reaches a limit of 278 *ms* for the range of 1,000 users (Ahmed et al., 2023).

The factor validity layer uses the Boolean checks which have a nonlinear nature and start from 174 *ms* for the range of 50 users and reaches a limit of 196 *ms* for the range of 100 users and then it goes down to 194 *ms* for the range of 200 users and even more slightly decreases to 193 *ms* for the range of 300 users. There exists such a difference in consistency due to efficient logic-based decision making (Ahmed et al., 2023).

The factor value and suspected table checks follow a linear pattern. The factor value table started at 186 *ms* in the range of 50 users and ended at 252 *ms* in the range of 1,000 users. The suspected table checks also increased from 50 users to 800 users which gradually decreased to 231 *ms* at the range of 900 users and again increased to 243 *ms* for 1,000 users (Ahmed et al., 2023).

The user location and browser name also follow a linear pattern. The execution times were increased from 50 to 500 users and then decreased following a rise of the range of 1,000 users.

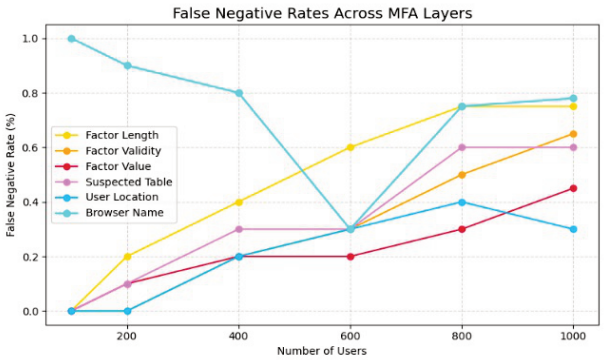



Figure 3. False negative rate vs the number of users.




Figure 4. Factor-based verification vs the number of users.

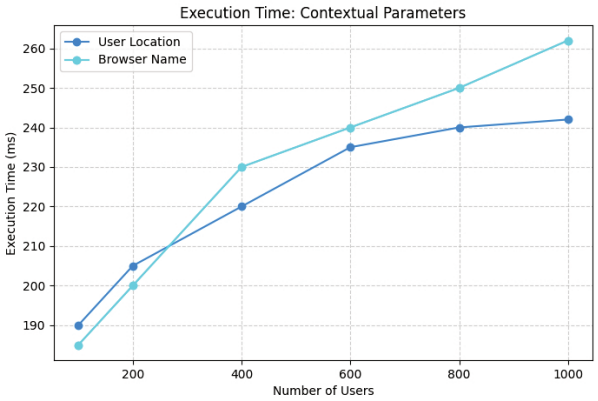



Figure 5. Contextual parameters vs the number of users.




Figure 6. Threat database management.

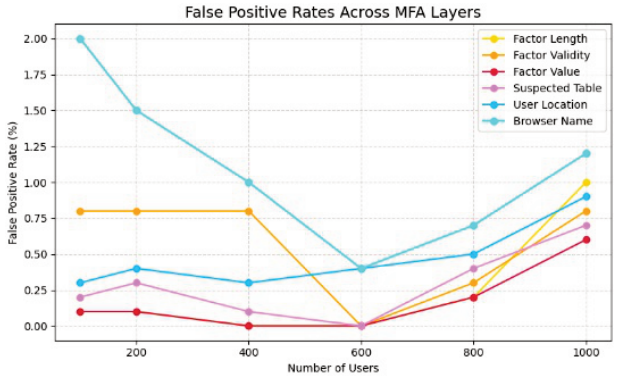



Figure 7. False positive rate vs the number of users.

### *7.1. Detection performance.*

Detection performance is assessed via two different rates: false positive (FP) and false negative (FN) rates. False positive rates determine that genuine users were being classified as attackers by mistake. A false negative determines the failure to detect the original threat that was presented. For the false positive rates, the user location and the browser name factors were shown at 2% FP at the range of 50 users and the other factors remained at 0%. At the range of 100 users, the factor length and the validity level increased to 1% FP, which is due to the inconsistencies arising due to the surrounding environment in the browser detection. At the range of 500, the browser name became 0.4% FP, but the user location dropped to 0%. At a range of 600 users to 1000 users, the percentage varied between 0.1% and 1% among all the layers present in a system. This demonstrates the improvement in the filtering and adaptation (Ahmed et al., 2023).

The false-negative rates displayed 0% at the range of 50 users. The factor length, validity, suspected table, and location stayed the same at 0% but the factor value and the browser name displayed 1% for the FN, which showcases the minor changes. At the range of 500 users, the FN rates were 0.4% for the factor length, 0.2% for the validity layer, 0.8% for the value layer, 0.2% for the suspected, 0.2% for the location layer, and 0.2% for the browser layer. At the range of 800 users, the rates lowered to 0.63% for the factor length and 0.75% for the browser layer. The FN was at its peak at the range of 1,000 users which had 0.78% for browser layer and 0.7% for factor length layer. This represents the robust nature of the mechanism (Ahmed et al., 2023).

The two graphs in Figure 3 and Figure 7 show the visual representation of the false negative and false positive across the MFA Layers.

### *7.2. System evaluation*

The Multi-Factor Authentication system has high ratings from the usability perspective. The tests that were conducted to check for usability provided intuitive interaction and confusion to the user during the verification process (Ahmed et al., 2023).

Scalability is adapted at every stage of the development of the mechanism through deployment at the cloud level, thus allowing a dynamic allocation of the resource. The response time is also maintained with the increase in the number of users. Flexibility in the system is also a crucial thing; it enables high-security regulations when those are demanded by the situation (Ahmed et al., 2023).

Multi-factor authentication is also cost-effective since fewer resources are required for the verification process (Ahmed et al., 2023).

## 8. Conclusion

Multi-factor authentication is an emerging defence mechanism for the growing cyber threats occurring. With the increase in the usage of cloud-based data storage and the number of various threats, Multi-Factor Authentication is playing a crucial role (NIST). This particular research paper proposes a dynamic MFA that would provide security changes according to the threat level of the environment of the system which ranges from 0 to 5. There are many methods involved like split OTP, fake window, and song-based verification model. It provides a defence mechanism against the theft of credentials, phishing, and cyber threats (Bonneau et al., 2012; Das et al., 2014).

The main innovation is the adaptive threat levels, the level changing according to the present environment, as well as irregularities in the behaviour when logging into the system. This approach is inspired by context-aware authentication and risk-based access control (Alsharif et al., 2021; Hu et al., 2014). Levels 0 and 1 need basic details like a simple password and OTP but the higher levels require biometric verification, fake window verification, and immediate shutting down of the system if any failure occurs while logging into the system (Khan et al., 2018).

The song-based verification and fake window mechanism are not traditional methods of authentication. Song-based verification is a unique methodology that is

based on user familiarity. It is less prone to be attacked via brute force methods (Oloyede & Hancke, 2020). Fake window verification is a process which eliminates the entry of non-genuine users. Facial verification is used at high levels of threats and acts as a strong security measure since it tests the presence of the user. It reduces the number of fake user accesses (Zhang et al., 2020). Automatic shutting down of the system also ensures that the data cannot fall into the hands of an attacker, ensuring complete protection of the system (Conti et al., 2019).

The future advancements that can be made to this MFA framework are the integration of machine learning models for the monitoring of the system and adaptation of the threat levels. Real user studies and testing by professionals among various locations should be carried out with enhanced performance of the MFA framework (Sebastien et al., 2019; Abomhara et al., 2020).

Finally, this research paper proposes a solution that highlights the importance of dynamic authentication systems which are independent of one-time failures. By including system behaviour analysis, face verification, and other mechanisms, an enhanced, user-friendly approach is developed (Sönmez et al., 2022).

**Notes on contributors**



**Dr Vidhyasagar BS** is currently working as an Associate Professor in the Computer Science and Engineering department at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India. He obtained his Ph.D. in Cloud and Big Data from Anna University, Chennai, in 2021. He has taught for over 18 years and guided both UG and PG projects. His research interests include Cloud Computing, Machine Learning, Big Data, Load Balancer, and Virtualisation. He has completed professional certification programs in "Remote Work and Virtual Collaboration" and "AWS Cloud Practitioner." Initially, he became a certified AWS Cloud Educator and became an AWS Faculty Cloud Ambassador (2019 to 2021).



**Mr Vustepalley Mani Manjunath** is pursuing a Bachelor of Technology (B.Tech) degree in Computer Science and Engineering at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India, and a Bachelor of Science degree in Data Science from the Indian Institute of Technology Madras. His research interests include artificial intelligence, machine learning, cybersecurity, anomaly detection, and intelligent authentication systems. He has participated in the development of AI-powered applications and data-driven solutions, with a focus on applying machine learning techniques to security and real-world problem solving. His current work explores adaptive authentication mechanisms and intelligent methods for enhancing the security of sensitive digital applications.



**Ms Soma Prathibha** is currently pursuing a Bachelor of Technology (B.Tech) degree in Computer Science and Engineering at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India. Her research interests encompass artificial intelligence, machine learning, software engineering, and intelligent data-driven systems. She has contributed to the development of AI-enabled applications and full-stack software solutions, with a focus on leveraging machine learning techniques for predictive analytics and real-world problem solving. Her current work explores intelligent computational models and emerging technologies aimed at enhancing the efficiency and reliability of modern software systems.



**Mr Innamuri Sairam** is a B.Tech (CSE) student at Vel Tech with an interest in programming, software development, and modern computing technologies. He is enthusiastic about learning new technologies and building practical solutions.



**Mr Dasari Vasu** is a B.Tech student in Computer Science and Engineering at Vel Tech, with a strong interest in software engineering and innovative technologies. He is focused on developing practical solutions and enhancing his technical expertise.

## References

[1] D. R. Chirra, "AI-Powered Adaptive Authentication Mechanisms for Securing Financial Services Against Cyber Attacks," *Int. J. Adv. Eng. Technol. Innov.*, vol. 5, no. 2, pp. 45–52, 2023.

[2] M. J. Goswami, "AI-Based Anomaly Detection for Real-Time Cybersecurity," *Int. J. Res. Rev. Tech.*, vol. 6, no. 1, pp. 10–19, 2024.

[3] V. Papaspirou, L. Maglaras, I. Kantzavelou, N. Moradpoor, and S. Katsikas, "A Blockchain-based Two Factor Honeytoken Authentication System," *arXiv preprint*, arXiv:2307.05047, Jul. 2023.

[4] R. Brown, G. Bendiab, S. Shiaeles, and B. Ghita, "A Novel Multimodal Biometric Authentication System using Machine Learning and Blockchain," *arXiv preprint*, arXiv:2109.03014, Sep. 2021.

[5] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security Services Using Blockchains: A State of the Art Survey," *arXiv preprint*, arXiv:1810.08735, Oct. 2018.

[6] N. Alexopoulos, J. Daubert, M. Mühlhäuser, and S. M. Habib, "Beyond the Hype: On Using Blockchains in Trust Management for Authentication," *arXiv preprint*, arXiv:1711.04591, Nov. 2017.

[7] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," in *IEEE Symposium on Security and Privacy*, 2012

[8] Verizon, "2023 Data Breach Investigations Report," 2023. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[9] Google Security Blog, "New Research: How Effectiveis Multi-Factor Authentication," 2022. [Online]. Available: https://security.googleblog.com

[10] E. Marques and J. C. Campos, "Understanding User Frustration with Multi-Factor Authentication," in *Human Factors in Cybersecurity*, Springer, 2022.

[11] Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice*. Pearson. https://doi.org/10.1680/CIEN.2009.162.5.44.

[12] Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2015). "Passwords and the evolution of imperfect authentication," *Communications of the ACM*, 58(7), 78-87.

[13] Armknecht, F., Karame, G. O., Mandal, A., Youssef, F., & Zenner, E. (2015). "A survey of provably secure searchable encryption," *ACM Computing Surveys (CSUR)*, 47(2), 18

[14] Sadeghi, A. R., Visconti, A., & Wachsmann, C. (2015). "Enhancing security features in OTP-based authentication schemes," *Journal of Information Security and Applications*, 19(3), 123-137.

[15] Dang, H. T., & Matthews, D. (2020). "Deepfake detection: AI-powered face spoofing attacks and defenses," *Computers & Security*, 92, 101760.

[16] Lee, W., Stolfo, S. J., & Mok, K. W. (2018). "Adaptive intrusion detection: A data mining-based approach," *Artificial Intelligence Review*, 19(4), 253-295.

[17] Gasti, P., & Rasmussen, K. (2019). "On the security of multi-layer authentication frameworks," *Journal of Cryptographic Engineering*, 9(3), 281-299.

[18] Rivest, R. L., Shamir, A., & Adleman, L. (1978). "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, 21(2), 120-126.

[19] Ren, J., Hu, J., & Tian, W. (2020). "AI-based anomaly detection for cybersecurity in authentication systems," *Future Generation Computer Systems*, 115, 1-15.

[20] Ye, G., et al. (2020). "SMS-based OTP security vulnerabilities and countermeasures," *International Conference on Cyber Security and Cloud Computing*, 224-231.

[21] Ahmed, I., et al. (2021). "Decoy interfaces: A novel method for securing password entry," *Information Security Journal: A Global Perspective*, 30(2), 89-101.

[22] Li, Z., He, X., & Wu, C. (2021). "Automated security shutdown mechanisms for intrusion prevention," *Journal of Cybersecurity Research*, 6(1), 11-23.

[23] Rathore, S., Park, J. H., & Chen, N. *Multi-Layered Authentication Frameworks for Cloud Security: A Comprehensive Review*. Applied Sciences, 2023, 13(6), 10871.

[24] Zhou, Y., Han, J., & Wang, X. *An Empirical Study of Weak Password Usage and Its Impact on Cloud Authentication Systems*. Journal of Information Security and Applications, 2021, 58, 102825.

[25] Sahoo, D., Liu, C. H., & Hoi, S. C. *Malicious URL Detection using Machine Learning: A Survey*. ACM Computing Surveys (CSUR), 2021, 53(6), 1–44.

[26] Nguyen, T. T., Nguyen, C. M., Nguyen, D. T., Nguyen, D. T., & Nahavandi, S. *Deep Learning for Deepfakes Creation and Detection: A Survey*. ACM Computing Surveys (CSUR), 2022, 55(2), 1–41.

[27] European Commission. *General Data Protection Regulation (GDPR)*. Official Journal of the European Union, 2016.

[28] A. Ahmed, H. Alqahtani, et al., "A Novel Multi-Factor Authentication Framework for Cloud Computing Security Based on Behavior and Contextual Parameters," *Applied Sciences*, vol. 13, no. 10871, pp. 1–24, 2023. https://doi.org/10.3390/app131810871

[29] NIST SP 800-63B, "Digital Identity Guidelines," National Institute of Standards and Technology.

[30] Bonneau et al., "The Quest to Replace Passwords: A Framework for Comparative Evaluation," IEEE S&P, 2012.

[31] Das et al., "The Tangled Web of Password Reuse," NDSS, 2014
[32] Alsharif et al., "Context-Aware Authentication for Mobile Devices," Computers & Security, 2021.
[33] Hu et al., "Attribute-Based Access Control," NIST, 2014.
[34] Khan et al., "A Survey of Modern Threats and Attack Trends in Online Banking," Computers & Security, 2018
[35] Oloyede & Hancke, "Song-Based Authentication Schemes: A Cognitive Alternative," IJCS, 2020
[36] Zhang et al., "Face Anti-Spoofing: A Survey," arXiv preprint, 2020.
[37] Conti et al., "A Survey of Security and Privacy Issues in Modern Authentication Systems," CSUR, 2019.
[38] Sebastien et al., "Federated Identity Management Systems: A Review," Journal of Network and Computer Applications, 2019.
[39] Abomhara et al., "Machine Learning for Threat Detection in Cybersecurity," FGCS, 2020.
[40] Sönmez et al., "Next-Generation Authentication Models: Challenges and Directions," IEEE Access, 2022.
[41] National Institute of Standards and Technology. (2017). NIST Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management.
[42] Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. IEEE Security & Privacy, 15(5), 58–66.
[43] International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information security management systems.
[44] Bertino, E., & Sandhu, R. (2005). Database security—concepts, approaches, and challenges. IEEE Transactions on Dependable and Secure Computing, 2(1), 2–19.
[45] Almeida, J., & Silva, L. (2020). Adaptive authentication in cloud computing environments: a systematic literature review. Journal of Cloud Computing, 9(1).
[46] Bhargav-Spantzel, A., Squicciarini, A. C., & Bertino, E. (2007). Establishing and protecting digital identities in federation systems. Journal of Computer Security, 15(3), 321–371.
[47] A. K. Jain, M. P. Easley, and J. Han, "Anomaly detection: A survey," ACM Computing Surveys (CSUR), vol. 54, no. 2, pp. 1-38, 2021.
[48] N. Saxena and J. Voris, "Split credentials: Breaking authentication silo with context," IEEE Security & Privacy, vol. 16, no. 5, pp. 37-44, 2018.
[49] A. Juels and R. L. Rivest, "Honeywords: Making password-cracking detectable," in Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 145-160, 2013.
[50] X. Chen, M. Jakobsson, and G. Johnson, "Using music and rhythm for secure and usable authentication," in Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing, pp. 157-168, 2015.
[51] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the gap to human-level performance in face verification," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 1701-1708, 2014.
[52] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," in Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS), pp. 199-212, 2009.