IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Dynamic Risk-Based Multi Factor Authentication For Securing Critical Systems

[1]Sangeetharani M, [2]Sandhiya B, [3]Mr.M.L.Srinivasan M.E(PHD)

[1]Student at Rajalakshmi Institute of Technology, [2]Student at Rajalakshmi Institute of Technology, [3] Assistant Professor at Rajalakshmi institute of Technology,

[1]Rajalakshmi Institute of Technology, Chennai, India

Abstract:

Modern cybersecurity threats require adaptive authentication systems because they continue to evolve. The traditional Multi-Factor Authentication (MFA) systems implement static authentication patterns at all times, which produces security vulnerabilities while degrading user satisfaction.This paper presents Dynamic Risk Based Multi-Factor Authentication that adapts authentication based on factors like IP address, location and device patterns unlike traditional MFA, which follows same static procedure.User attempts to log in are classified as low, medium or high-risk based on a system analysis of IP address and device information and geolocation details.High-risk situations require authentication strengthening through the implementation of Zero-Knowledge Proof (ZKP) validation [6] while the system supports varied authentication requirements according to risk categories. The system runs through Node.js as its backend platform and React.js for frontend development alongside PostgreSQL as its database solution and AES encryption with Snark.js for enhanced encryption security. The experimental evaluation shows substantial progress in securing logins through a system that cuts down extra authentication procedures for reliable users while boosting protection levels against unauthorized activities.

Keywords: Multi-Factor Authentication (MFA), Dynamic Authentication,Risk-Based Authentication, Cybersecurity, Zero-Knowledge Proof (ZKP), Contextual Authentication, React.js, Spring Boot, PostgreSQL, AES Encryption, Snark.js, Secure Data Transmission.

I. INTRODUCTION

Past security platforms no longer offer sufficient protection as cyber threats continue to evolve. Multi-Factor Authentication (MFA) functions as a common security solution to protect against unauthorized access yet its traditional authentication methods use fixed security policies[19].Regardless of the authentication method, device, or location, the system follows a single standardized authentication procedure, leading to performance inefficiencies and security vulnerabilities[17].

The primary disadvantage of traditional MFA is its inability to adapt security measures to changing risk levels, leading to two major problems:

1. User Frustration and Poor Usability:

All users performing logins from established secure locations undertake identical complicated authentication procedures which match those required from unknown locations.

The duplicated authentication process causes users to lose their time and experience poor usability which in turn decreases productivity while also increasing their frustration. Research proves that complicated login authentication systems drive people to stop their sessions thus impacting operational performance[8].

2. Security Vulnerabilities and Increased Risk Exposure:

Traditional MFA lacks the ability to evaluate vital risk information that includes devices used by users and their location data and their reputations. As a result, attackers leveraging phishing, credential stuffing, or session hijacking can bypass authentication, as the system fails to adjust security measures dynamically.

Security measures for high-risk login attempts match those from low-risk attempts thus creating an opportunity for unauthorized access by attackers[16].

A. Problem Statement

Traditional MFA systems present two critical problems: they make organizations vulnerable to cyberattacks and create unfavorable user experiences. Current authentication systems lack intelligent policies, failing to distinguish between normal logins and potentially risky access attempts. Current authentication systems lack intelligent policies, failing to distinguish between normal logins and potentially risky access attempts. Organizations must deal with two major obstacles because of this situation.

The static approach of MFA fails to adjust to shifting security priorities because of which advanced cyberattacks including Man-in-the-Middle and SIM-swapping methods can defeat authentication controls.

Users experience decreased efficiency together with elevated frustration when they need to complete many authentication procedures within low-risk situations[10].

B. Motivation and Need for Dynamic Risk-Based MFA

The increasing security breaches demand a risk-adaptive authentication mechanism that uses context-aware approaches. The SolarWinds attack demonstrates how cyber attackers take advantage of vulnerable authentication systems at high security levels. Risk evaluation methods need to become part of modern authentication systems because they help security measures adapt automatically to current environmental factors[21].

Modern MFA solutions need the following primary factors for implementation success:

1.Advanced authentication approaches are needed because AI attacks combined with improved social engineering require protection methods that change according to circumstances.

2.User-friendliness continues to be essential in security because forcing authentic users to perform multiple authentication steps will decrease productivity and lower compliance rates.

3.Safety models which blend behavioral analytics with AI risk evaluation allow organizations to improve their security posture while maintaining user-friendly operations[18].

C. Objective of the Proposed System

Our proposed Dynamic Risk-Based MFA System seeks to build authentication security while making it more usable by means of adaptive risk evaluation[15]. Specifically, the system aims to:

Assess Risk Levels Dynamically:

The system uses contextual elements like user operations and device information and geolocation and IP address data points to generate a risk assessment score for login verification[14].

Login attempts are categorized as low, medium, or high risk based on computed risk scores.

Risk-oriented factors control the authentication process:

Low-Risk Attempts: Require only a password and OTP[4].

Medium-Risk Attempts: Add an additional layer, such as a security question[9].

High-Risk Attempts: Users facing high-risk authentication attempts need to submit verification through advanced measures that incorporate Zero-Knowledge Proof (ZKP) authentication[5].

Enhance Security with Zero-Knowledge Proofs:

Users can authenticate their identity through cryptographic validation making it possible to verify their identity securely without sharing delicate details[12].

Implement Secure Session Management:

User sessions can be secured with session tokens together with protection against unauthorized access.

Strong security measures involve both role-based authorization systems and automatic session termination mechanisms for security defense[11].

Improve User Experience:

The system should present fewer authentication windows for basic operations since it allows users to easily navigate their accounts without making their security vulnerable.

II. RELATED WORK

A. Two-Factor Authentication(2FA)

The security system, Two-Factor Authentication (2FA), demands users present two different authentication elements to confirm their identity.While 2FA enhances security compared to single-factor authentication, it remains static since users follow the same authentication steps, regardless of environmental factors[2].

B. Public Key Cryptography for Authentication

PKC stands as one of the most utilized authentication security methods to protect data flow and verify system users.The cryptographic security that PKC-based authentication delivers can assure data safety through asymmetric encryption yet shows no automatic capability to adjust security measures according to varying levels of risk [12].

C. Adaptive Authentication Models

Research investigates dynamic authentication methods which modify security controls by processing context-related data about device patterns and user activities and IP reputation profiles[22]. The existing risk management solutions struggle to achieve two key features: detailed scoring based on risk assessment and cryptographic ZKP-based validation.

III. PROPOSED SYSTEM

The Dynamic Risk-Based MFA System builds upon conventional authentication by employing instantaneous risk evaluation and adaptable authentication along with protected session maintenance to provide secure protection together with reduced user challenges[14][17]. Three distinct modules form the basis of the system design.

A. Risk Assessment Module

This module takes available contextual elements during login attempts to spot potential security dangers that need investigation[4]. It evaluates:

The IP Reputation component establishes if an incoming login request comes from an established reputable IP or from suspicious or prohibited IP addresses.

System infrastructure monitors login attempts to discover suspicious requests that appear in intriguing geographical locations linked to danger zones[11].

Device Recognition: Distinguishes between previously used and new or suspicious devices.

User Behavior Analysis: Monitors login frequency, time-of-day patterns, and unusual activity[7].

The dynamic risk score that determines the authentication level is built from all risk indicators.

Figure 1 illustrates the system architecture, showing how the frontend, backend, risk assessment, authentication, and session management components interact to ensure secure and adaptive authentication.

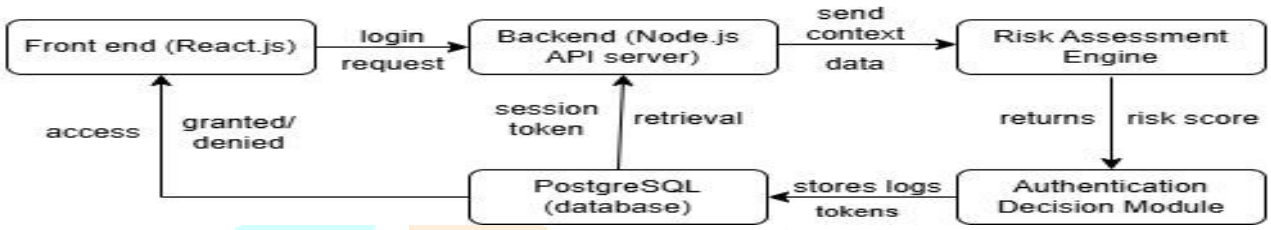

Figure 1. System Architecture of the Dynamic Risk-Based MFA System.

B. Adaptive Authentication Engine

Upon calculating the risk score this module uses it to transform authentication steps in real time.

The overall **risk score RRR** is computed as follows:

$$R=w1F1+ w2F2+ w3F3+ w4F4 \quad (1)$$

where:

- F1 = **IP Reputation Score** (e.g., trusted or suspicious IPs)
- F2= **Device Trust Score** (e.g., known or new device)
- F3 = **Login Frequency Anomaly** (e.g., unusual login time)
- F4= **Geolocation Risk Score** (e.g., known or unknown location)
- w1,w2,w3,w4= **Weight factors** determined based on historical authentication patterns

The calculated **risk score RRR** is compared against predefined thresholds to determine the authentication method:.

Low Risk (Score <30%) → Password + OTP (Minimal Disruption).
Medium Risk (Score 30-70%) → Password + OTP + Security Question.
High Risk (Score >70%) → Password + OTP (Zero-Knowledge Proof (ZKP))Verification.

The system enables high-risk scenarios to activate strict authentication methods while avoiding security threats to preserve user experience during authentication processes.

C. Secure Session Management System

The system generates token access codes during authentication which serve to verify session identity as well as prevent session hijacking attacks. This module ensures:

Safe session control is managed through JWT tokens and database tokens within token-based authentication.

For the purpose of reducing potential security risks, the session token lifespan determines automatic expiration with session renewal.

When suspect activity is detected in session content, the user is re-authenticated using MFA[14].

D. Zero-Knowledge Proof (ZKP) Mechanism

Zero-Knowledge Proof (ZKP) serves as a cryptographic framework which allows authentication to take place while maintaining complete secretiveness of delicate information[3]. ZKP in the proposed system enables users to authenticate their identity through unexposed password and personal data[20]. Credentials remain out of reach for attackers who want to perform phishing or MitM attacks through this system. The security system functions through zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) that produce authentication proof statements which authenticate users without disclosing their identity sources. The authentication request remains protected from revealing user credentials because attackers would obtain no valuable information[5].

IV. COMPARISON WITH THE PROPOSED SYSTEM

Table 1 compares Traditional MFA with the proposed Dynamic Risk-Based MFA system across various security, usability, and performance factors. Traditional MFA implements a standardized authentication approach while showing limited response to risks at varying levels. Dynamic MFA implements risk-based authentication through real-time assessments that protect users by finding optimal security-user experience equilibrium[19]. The proposed system implements Zero-Knowledge Proofs (ZKP) specifically for critical situations to boost its immunity against security threats.

Dynamic MFA implements session management through secure session tokens which sustain authentication with no sacrifice to security. Although Dynamic MFA has minimal implementation challenges, its strong security measures and adaptable features outweigh these drawbacks. Dynamic MFA gives users superior protection through its security features that keep legitimate users from facing excessive authentication requirements[22].

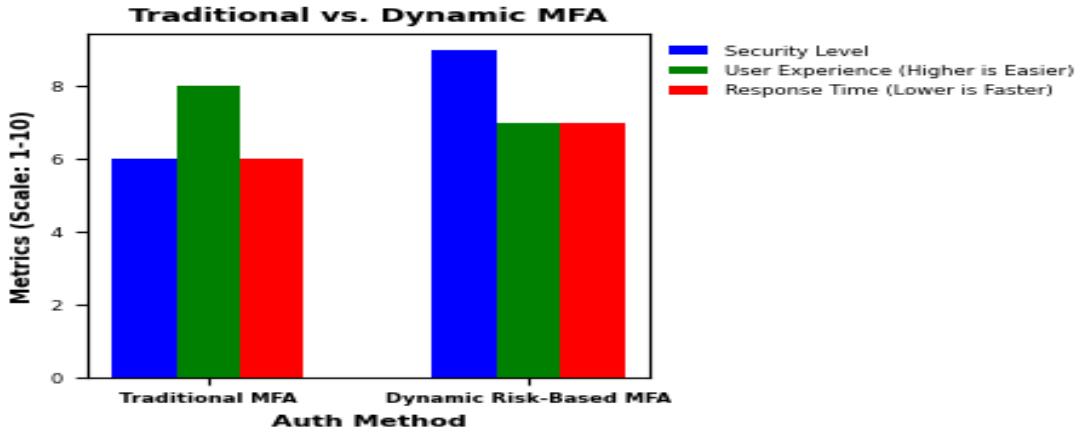

Figure 2. Comparison of Traditional MFA and Dynamic Risk-Based MFA based on security, user experience, and response time.

From Figure 2, we can see that Dynamic MFA achieves better results compared to Traditional MFA in terms of security, response time.The visual presentation reveals the new system achieves greater security along with enhanced user experience and prompt response times which proves it as an improved authentication process.

V. IMPLEMENTATION

Feature	Traditional MFA	Proposed Risk-Based MFA
Authentication flow	Predefined steps(Password+ OTP)	Dynamic authentication based on risk evaluation
Context sensitivity	Lacks adaptation	Considers user behaviour, IP address, device context
Security vs. Usability	High security,lower convenience	Optimised balance between security and usability
Adaptability to Risk	Does not adapt authentication based on risk	Dynamically adjusts authentication based on risk score
Zero-Knowledge proofs	Not implemented	Used for authentication in high risks scenarios
Session Management	No adaptive session security measures	Secure session tokens with expiration

Table 1.Comparison between traditional MFA and Dynamic MFA

The proposed Dynamic Risk-Based MFA system demonstrates its entire authentication method through Figure 3. The flowchart depicts the process which starts with user login request processing followed by contextual risk assessment for dynamic authentication step adjustment based on the calculated risk score. Secure and convenient user access is managed through the session control mechanism of the system.

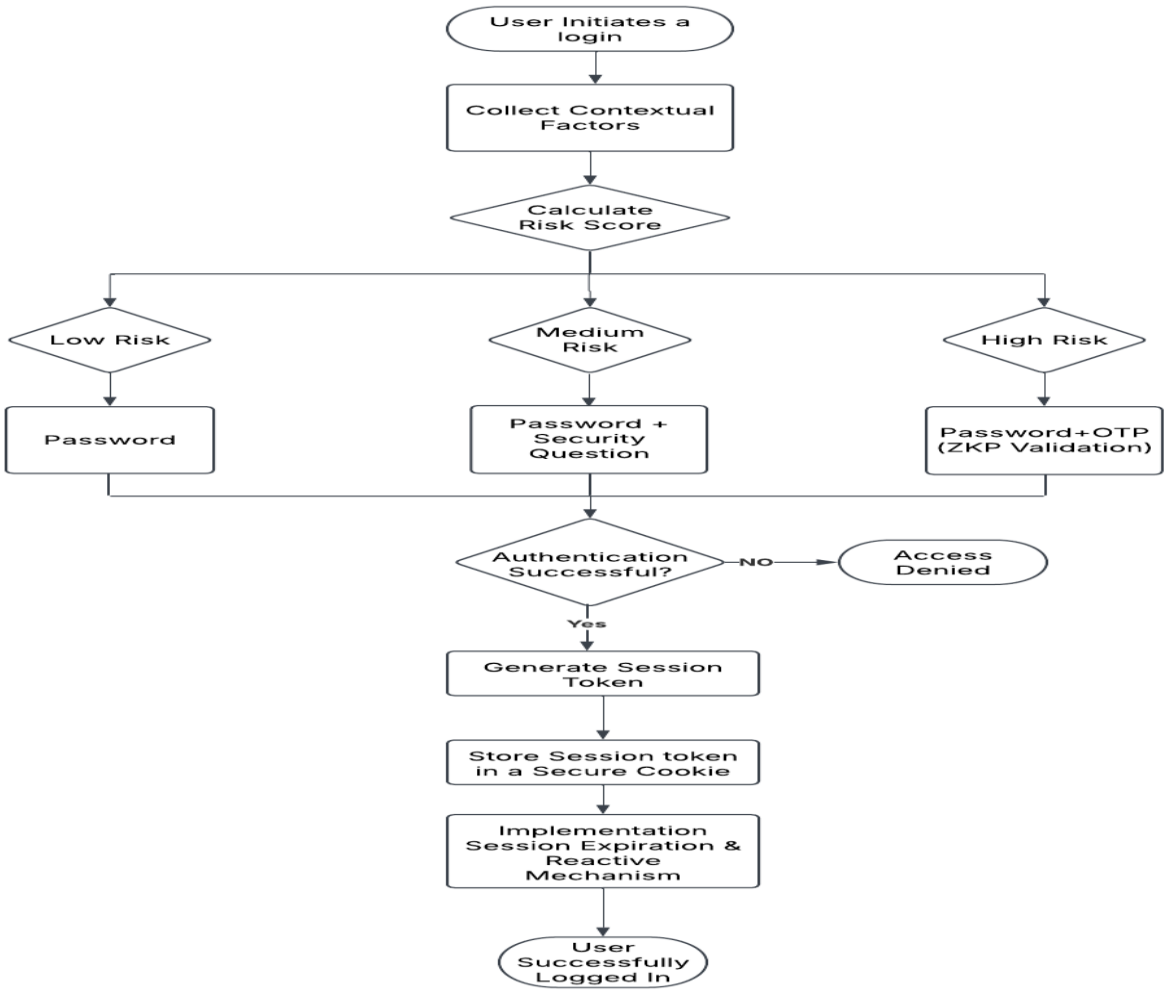

Fig 3: Full Authentication System Flowchart depicting risk evaluation, adaptive authentication, and secure session management..

Frontend: React.js (User Interface, Authentication UI)
Node.js functions as the backend component by building the API along with performing risk assessments.
Database: The database utilizes PostgreSQL to store both user authentication information as well as maintain risk logs.
Security: AES Encryption (Data security), Snark.js (Zero-Knowledge Proofs)

The deployment of the Dynamic Risk-Based MFA System has these components:

User Authentication Module:

The system gathers authentication credentials while recording IP address devices along with location data Computes a dynamic risk score.

Adaptive MFA Module:

Risk levels determine which authentication procedure will be needed[13].

Implements ZKP for high-risk authentications.

Session Management:

Secure access depends on Issues creating encrypted session tokens.

VI. CHALLENGES AND LIMITATIONS

The implementation of Dynamic Risk-Based MFA encounters three major obstacles which include authentication delays and privacy issues coupled with risks in scoring optimization. The security improvements of Zero-Knowledge Proofs reduce system scalability because these proofs require high computing resources. The implementation of existing authentication systems through OAuth and SAML

proves to be complex and difficult to integrate. Executed implementation requires these challenges to be solved in order to achieve both efficiency and security.

VII. FUTURE WORK

The proposed system reaches high levels of security combined with usability but additional improvements can potentially be incorporated. The implementation of blockchain for creating authentication structures which cannot be altered guarantees both security and enhanced auditing capabilities. Zero-Knowledge Proofs (ZKP) should expand their usage to establish decentralized authentication systems which maintain user privacy. Future biometric research into facial recognition alongside behavioral authentication methods will enable more secure authentication processes that users can easily use.

VIII. CONCLUSION

Traditional authentication methods are surpassed by the Dynamic Risk-Based MFA System since it implements security adjustments through assessments of contextual risks. The system improves security capabilities through ZKP and blockchain authentication without compromising user convenience. The platform implements scalable authentication security through its React.js and Node.js and PostgreSQL design framework. Stricter development work will optimize this system's efficiency and make it more adaptable toward safeguarding users from modern cyber threats.

IX. REFERENCE:

[1] Arun Ross and Anil K Jain, "Multimodal Biometrics: an Overview" 2004.
[2] A. M. Rieke, "Systems and methods for two-factor authentication," 2009.
[3] J. Lum and B. Jun, "Implementing Zero-Knowledge Authentication with Zero Knowledge" 2010.
[4] B. Laurie, A. Langley, and E. Kasper,"Time-based One-time Password Algorithm" 2011.
[5] N. Datta, "Zero knowledge password authentication protocol" 2013.
[6] Salman H Khan, M Ali Akbar, Farrukh Shahzad, Mudassar Farooq and Zeashan Khan, "Secure biometric template generation for multi-factor authentication" 2015.
[7] S. K. Sood, A. K. Sarje, and K. Singh, "Risk-Based Multilevel and Multi Factor Authentication Using Device Registration and Dynamic QR Code Based OTP Generation" 2015.
[8] A. Yohan, N. W. Lo, and H. R. Lie, "Dynamic Multi-Factor Authentication for Smartphone" 2016.
[9] R. H. Steinegger, D. Deckers, P. Giessler, and S. Abeck, "Risk-Based Authenticator for Web Applications" 2016.
[10] N. A. Lal, S. Prasad, and M. Farik, "A Review of Authentication Methods" 2016.
[11] D. Wang, Z. Zhang, P. Wang, J. Yan, and X. Huang, "Targeted Online Password Guessing: An Underestimated Threat" 2016.
[12] S. K. Sood, A. K. Sarje, and K. Singh"Multi-Factor Authentication Using Threshold Cryptography" 2016.
[13] L. Dostalek, "Multi-Factor Authentication Modeling" 2019.
[14] S. Wiefling, T. Patil, M. Dürmuth, and L. Lo Iacono, "Evaluation of Risk-Based Re-Authentication Methods" 2020.
[15] H. F. Atlam, M. A. Azad, M. O. Alassafi, A. A. Al Shadadi, and A. Alenezi, "Risk-Based Access Control Model: A Systematic Literature Review," 2020.
[16] A. Hassan, B. Nuseibeh, and L. Pasquale, "Engineering Adaptive Authentication" 2021.
[17] S. Wiefling, P. R. Jørgensen, S. Thunem, and L. Lo Iacono, "Pump Up Password Security! Evaluating and Enhancing Risk-Based Authentication on a Real-World Large-Scale Online Service" 2022.
[18] Y. Zhang, X. Li, and J. Wang, "A Security Protection Technology Based on Multi-factor Authentication," 2023.

[19] S. Wiefling, J. D. Tolsdorf, and L. Lo Iacono, "Privacy Considerations for Risk-Based Authentication Systems" 2023.
[20] A. K. Das, "Analysis of Zero-Key Authentication and Zero-Knowledge Proof," 2023.
[21] M. Fanti, “Implementing Multi Factor Authentication: Protect Your Applications from Cyberattacks” 2023.
[22] A. Büttner and N. Gruschka, "Evaluating the Influence of Multi-Factor Authentication and Recovery Settings on the Security and Accessibility of User Accounts," 2024.