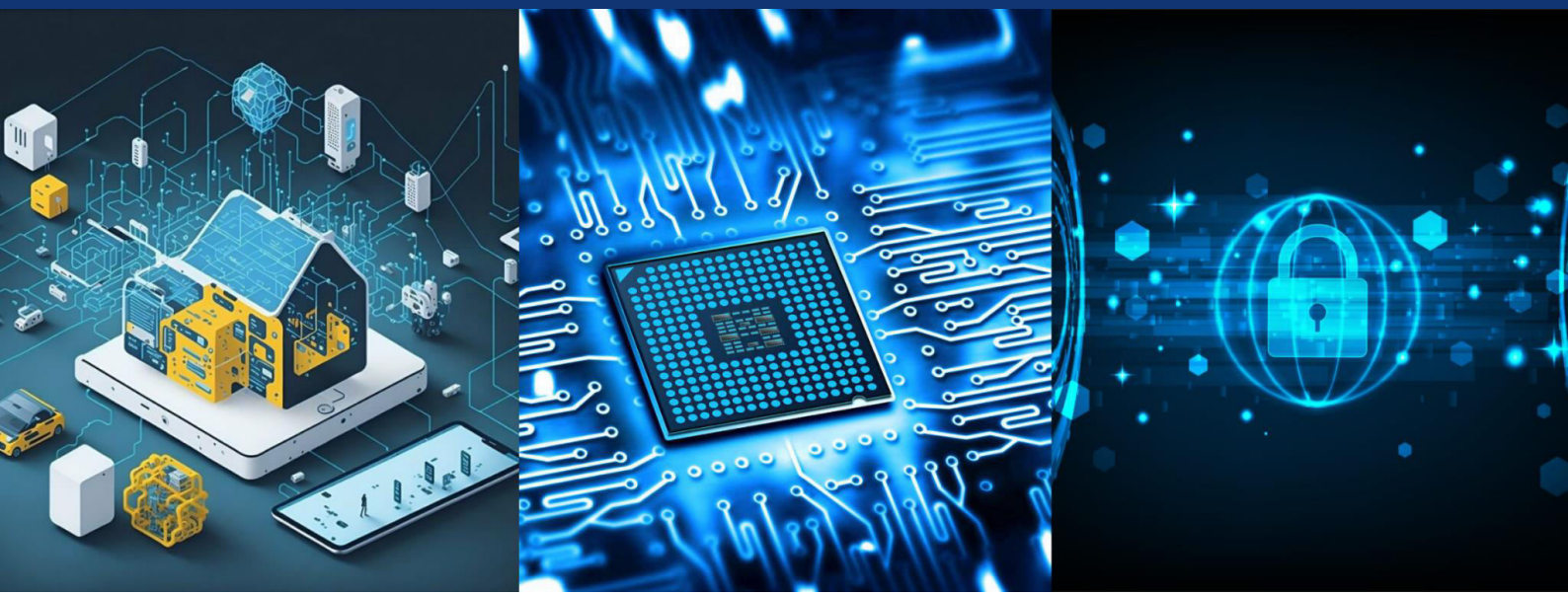
IJIRCCE

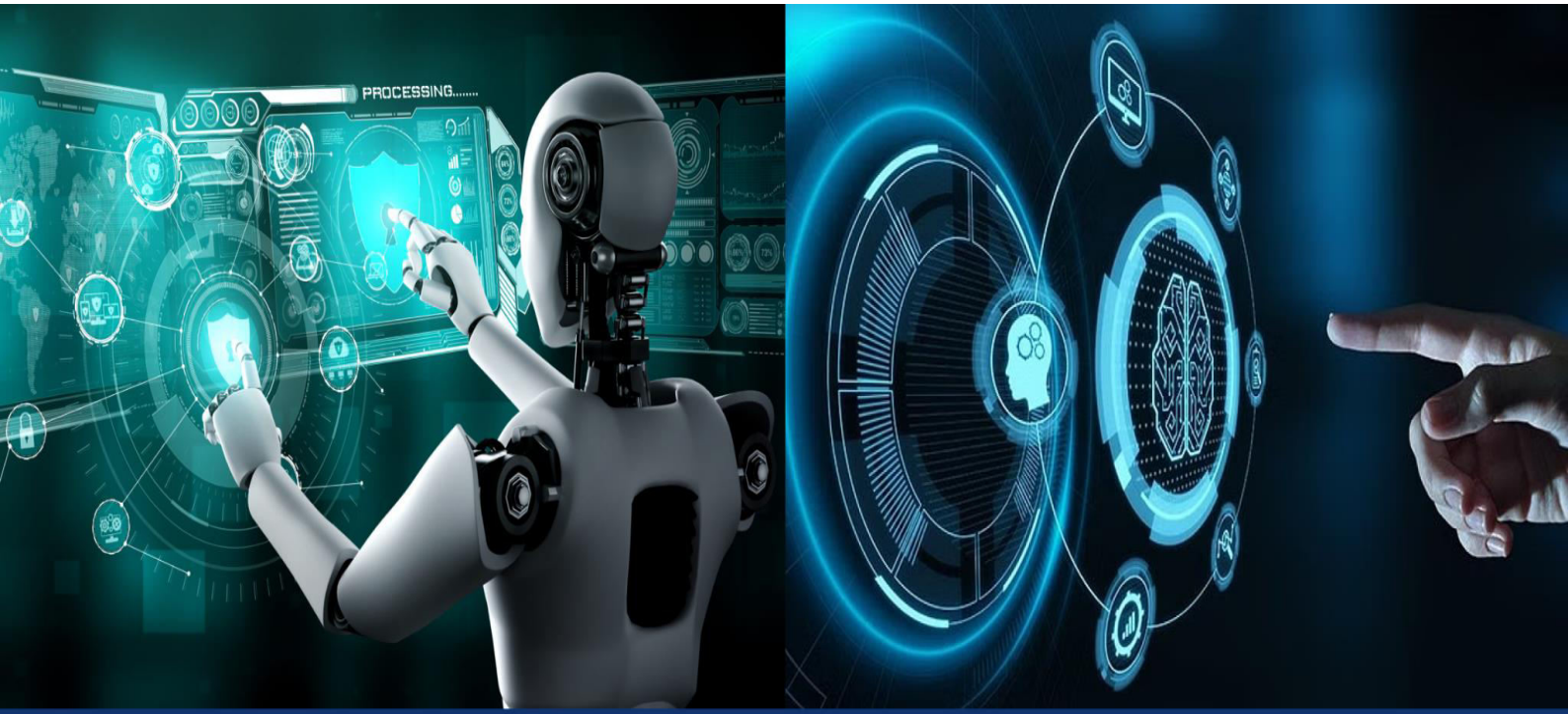
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 14, Issue 4, April 2026

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404019

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Hybrid Authentication System using JSON Web Tokens and Multi-Factor Authentication for Securing Web Applications

Chede Yaswanth[1], Desireddy Gopal Reddy[1], Javvaji Navya[1], Kasturi Gowtham[1], Kristavarapu Jagadeesh[1], M.Ganesh Babu[2]

B. Tech Student, Department of CSE, Sir C R Reddy College of Engineering, Eluru, A.P., India[1]

Assistant Professor, Department of Computer Science and Engineering, Sir C R Reddy College of Engineering, Eluru, A.P., India[2]

ABSTRACT: As online services and web applications continue to grow rapidly, secure user authentication has become a critical concern in modern cybersecurity. Traditional authentication methods that rely solely on usernames and passwords are highly vulnerable to attacks such as brute-force attacks, phishing, credential theft, and session hijacking. This research proposes a Hybrid Authentication System that integrates JSON Web Tokens (JWT) and Multi-Factor Authentication (MFA) to enhance web application security. JWT is utilized for stateless session management, while Time-Based One-Time Passwords (TOTP) provide an additional layer of security. The system is implemented using FastAPI and Streamlit frameworks.The results demonstrate improved security, scalability, and stronger resistance to unauthorized access compared to traditional authentication systems.

KEYWORDS: Cybersecurity, JSON Web Token (JWT), Multi-Factor Authentication (MFA), TOTP, Web Security, Authentication Systems

I. INTRODUCTION

Web applications play a crucial role in modern digital services such as banking, e-commerce, and cloud computing. These applications handle sensitive user data, making authentication a fundamental aspect of system security [4], [15]. Traditional authentication systems rely on single-factor methods (username and password), which are highly susceptible to attacks such as phishing, brute-force attacks, and password reuse [9], [17]. Weak credentials can be easily exploited, leading to unauthorized access.To address these issues, modern systems have adopted advanced authentication techniques such as Multi-Factor Authentication (MFA) and token-based authentication. JWT provides a secure and scalable way of handling authentication without maintaining server-side sessions [1]. Meanwhile, MFA enhances security by requiring multiple verification factors [10].This paper proposes a hybrid authentication system that combines JWT and MFA to provide a secure, scalable, and efficient authentication solution for web applications.

II. RELATED WORK

Michael Jones et al. [1] introduced JSON Web Token (JWT), enabling stateless authentication and efficient session management in web applications. However, JWT alone lacks protection against token theft and replay attacks due to the absence of additional verification layers.Similarly, Dick Hardt [11] proposed the OAuth 2.0 framework, and the OpenID Foundation [12] extended it with OpenID Connect for identity management. While these frameworks enhance authorization, they rely primarily on token-based mechanisms and do not inherently enforce multi-factor authentication. Guidelines from the OWASP Foundation [9] and the National Institute of Standards and Technology [10] emphasize Multi-Factor Authentication (MFA) as a critical security measure. Although MFA improves protection, it introduces challenges such as usability issues, system complexity, and deployment overhead. Research by Arunesh Das et al. [17] highlights the vulnerabilities of password-based systems due to reuse and weak credentials, reinforcing the need for stronger authentication methods. Industry reports from Microsoft [18] and Duo Security [19] show that MFA significantly reduces attack risks, but improper implementation can limit its effectiveness.

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404019

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

From an implementation perspective, tools like PyOTP [7] support TOTP-based authentication, while frameworks such as FastAPI [5] enable scalable system development. However, existing approaches often treat JWT and MFA separately rather than integrating them into a unified hybrid authentication model.

III. PROPOSED SYSTEM

The proposed system integrates:

- JWT for secure session management [1]
- MFA using TOTP for additional verification [7]

DATABASE DESIGN

Database design defines how data is stored and organized in the system.
The proposed system uses **SQLite database** to store user information and authentication logs.

Field	Data Type	Description
user_id	Integer	Unique identifier
username	Text	Username of the user
password_hash	Text	Encrypted password
totp_secret	Text	TOTP secret key

Tab-5: User Table

Field	Data Type	Description
log_id	Integer	Log identifier
username	Text	User name
action	Text	Authentication event
timestamp	DateTime	Event time

Tab: Audit Log Files

WORKING PROCESS

User → UI → FastAPI → Auth Service → DB
↓
OTP Service
↓
JWT Service
↓
Response

1. User registers with credentials
2. User logs in using username and password
3. System generates OTP (TOTP) [7]
4. User verifies OTP
5. JWT token is generated [1]
6. User gains access to protected resources

sThis ensures that even if credentials are compromised, unauthorized access is prevented through MFA [10].

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404019

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

3.1 Representation

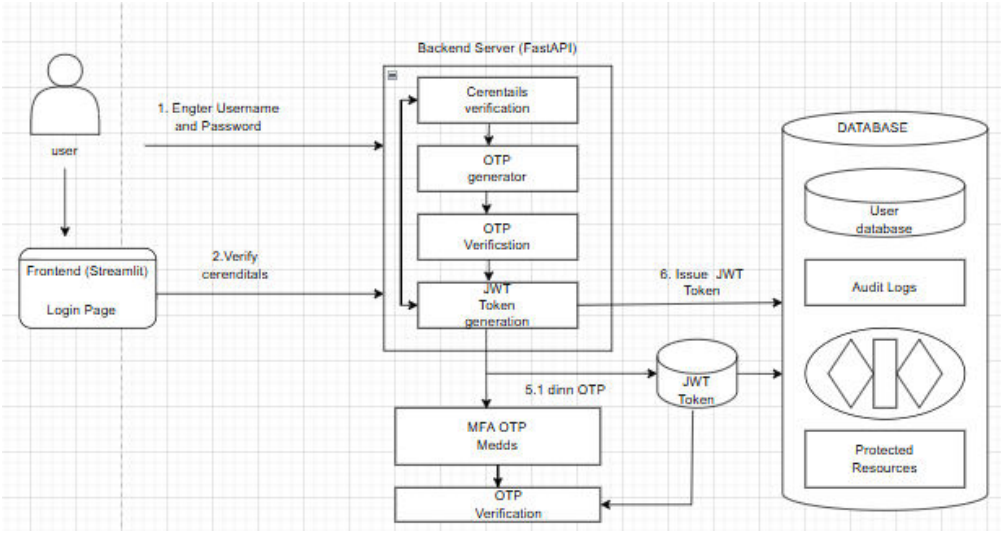


Fig : Architecture of Hybrid Authentication System using JWT and MFA

IV. IMPLEMENTATION

The system is implemented using modern web technologies:

- FastAPI handles API requests [5]
- Streamlit provides UI interface [6]
- JWT ensures stateless authentication [1]
- OTP ensures multi-layer security [7]

The application supports:

- User registration
- Login system
- OTP verification
- Secure session handling

V. RESULTS AND DISCUSSION

Performance Improvements:

Feature	Traditional System	Proposed System
Security	Low	High
Authentication	Single Factor	Multi-Factor
Session Management	Server-based	Token-based
Scalability	Limited	High

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404019

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

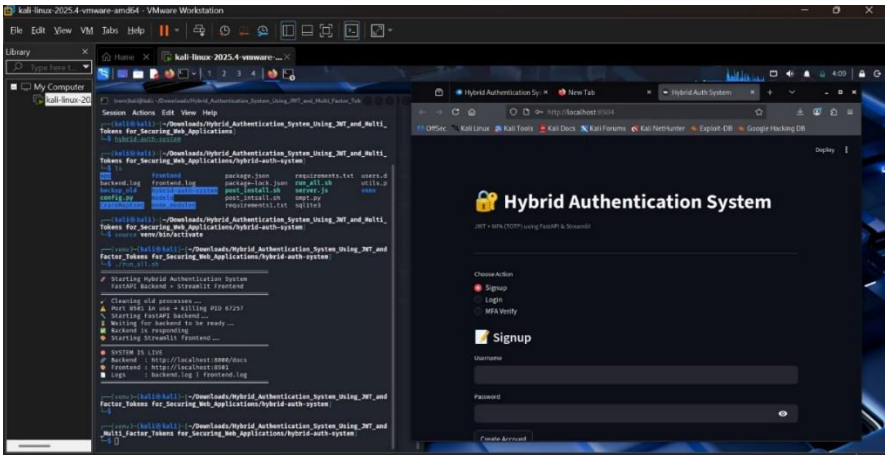


Fig : System Execution Environment (Kali Linux)

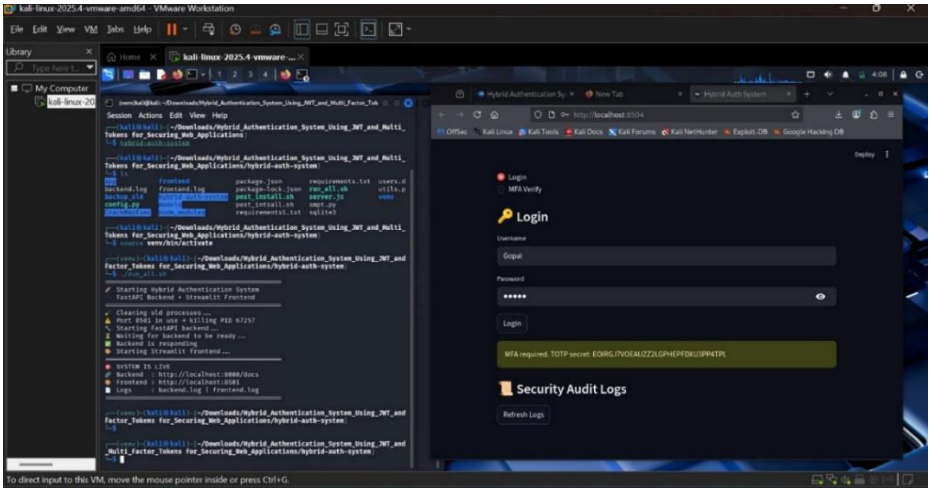


Fig : Login Interface

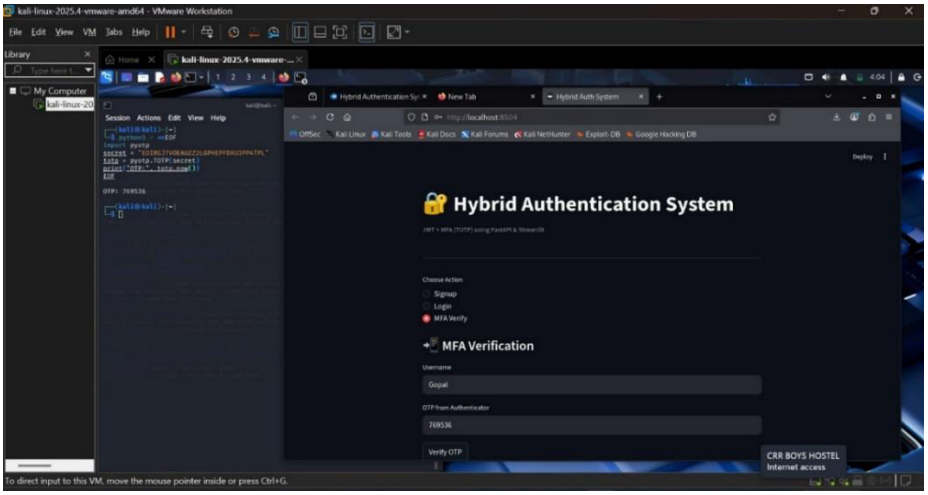


Fig : MFA OTP Verification

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404019

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

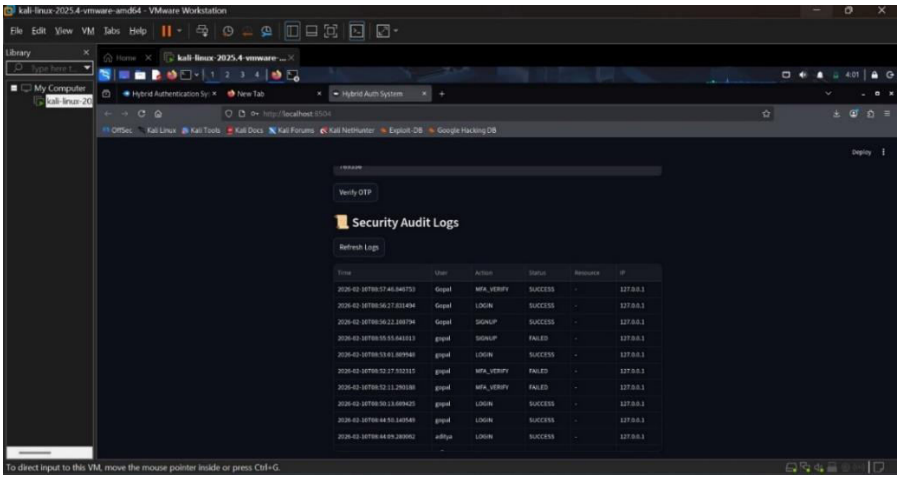


Fig: Security Audit Files

Observations:

- Reduced unauthorized access
- Improved resistance to cyber attacks
- Efficient session handling
- Better scalability

VI. CONCLUSION

The Hybrid Authentication System combining JWT and MFA significantly improves web application security. By integrating password-based authentication with TOTP verification [7], the system provides strong protection against unauthorized access. JWT enables secure and scalable session management [1], while MFA enhances identity verification [10]. The implementation using FastAPI and Streamlit ensures efficiency and usability [5], [6]. Overall, the system offers improved security, scalability, and reliability compared to traditional authentication methods.

VII. FUTURE SCOPE

1.**AI-Based Adaptive Authentication:** Apply dynamic security through the analysis of user behaviour using AI and deploying the appropriate measures in accordance with the risks.
2.**Passwordless Authentication:** Use such technologies as passkeys and WebAuthn to get rid of passwords altogether.
3.**Blockchain-Based Identity Management:** Decentralized systems can be used to safely handle user identities and do not allow tampering of data.
4.**Zero Trust Security Model:** Always check users and devices rather than believing them once they have been logged in.
5.**Continuous Authentication:** Track the activity of users in real-time and identify anomalies when they have active sessions.
6.**Quantum-Resistant Security:** Implementation of post-quantum cryptography as a preventive measure.
The innovations will improve security, scalability and future-proofing of the system to the emerging cyber threats.

REFERENCES

[1] M. Jones, J. Bradley, and N. Sakimura, “JSON Web Token (JWT),” Internet Engineering Task Force (IETF), RFC 7519, 2015.
[2] T. Dierks and E. Rescorla, “The Transport Layer Security (TLS) Protocol,” IETF RFC 5246, 2008.
[3] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson Education, 2017.
[4] M. Goodrich and R. Tamassia, *Introduction to Computer Security*. Pearson, 2015.
[5] “FastAPI Documentation.” [Online]. Available: https://fastapi.tiangolo.com

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[6] "Streamlit Documentation." [Online]. Available: https://docs.streamlit.io
[7] "PyOTP Documentation." [Online]. Available: https://pyauth.github.io/pyotp/
[8] "SQLite Documentation." [Online]. Available: https://www.sqlite.org/docs.html
[9] OWASP Foundation, "Authentication Security Guidelines," 2023. [Online]. Available: https://owasp.org
[10] National Institute of Standards and Technology (NIST), "Digital Identity Guidelines," 2020. [Online]. Available: https://pages.nist.gov
[11] D. Hardt, "The OAuth 2.0 Authorization Framework," IETF RFC 6749, 2012.
[12] OpenID Foundation, "OpenID Connect Core 1.0," 2014.
[13] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," *Advances in Cryptology*, 1984.
[14] S. Kent and K. Seo, "Security Architecture for the Internet Protocol," IETF RFC 4301, 2005.
[15] N. Ferguson, B. Schneier, and T. Kohno, *Cryptography Engineering*. Wiley, 2010.
[16] Google, "BeyondCorp: A New Approach to Enterprise Security," 2014.
[17] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The Tangled Web of Password Reuse," *NDSS*, 2014.
[18] Microsoft, "Multi-Factor Authentication Security Best Practices," 2022.
[19] Duo Security, "The State of Multi-Factor Authentication," 2021.
[20] S. Josefsson, "Base64 Data Encodings," IETF RFC 4648, 2006.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details