AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 4(2026)

SECURE CLOUD SYSTEMS WITH ADVANCED AUTHENTICATION

Madiha Mahveen[1], Dr. Lalitha Saroja[2]
[1]PG Scholar, Department of CSE, Shadan Women's College of Engineering and Technology, Hyderabad
Mahveenmirza08@gmail.com
[2]Assoc Professor, Department of CSE, Shadan Women's College of Engineering and Technology, Hyderabad
lalithasarojathota@gmail.com

ABSTRACT:
The rapid expansion of the cloud computing sector highlights the need for advanced security solutions to protect sensitive data on remote servers. Authentication is crucial to safeguarding these data. Despite the various strategies that have been proposed, vulnerabilities still exist. This study offers a novel multi-factor authentication system combined with a hybrid cryptographic framework that dynamically modifies encryption algorithms using data mining techniques based on an intrusion-detection system. To extract the encryption key from fingerprint data, the suggested solution uses conditional characteristics, passwords, and fingerprint authentication. Five method pairings are used in its dual-encryption strategy: AES + HMAC (SHA-256), ECC + HMAC (SHA-512), HMAC-MD5 + PBKDF2, Twofish + Argon2, and Blowfish + HMAC SHA3-256. A hybrid approach dynamically adapts an encryption algorithm to identify and classify risks in order to safeguard the data. The architecture showed strong resilience to phishing, spoofing, brute force, guessing, and impersonation assaults. Data confidentiality is significantly enhanced and unauthorized access is stopped by implementing this paradigm in a cloud authentication environment. This study shows how adaptive cryptography and multi-factor authentication may be used to build robust cloud security systems.
Keywords: —Adaptive cryptography, attack prediction, cloud security, dual encryption, dynamic encryption algorithms, hybrid CNN-transformer model, machine learning techniques, multi-factor authentication.

1. INTRODUCTION

The emergence of cloud computing [CC] has drastically altered how people and companies handle and store data. CC offers on-demand services over the internet and makes it possible to store data and application software with less administrative work. Any platform may become a cloud-based infrastructure by integrating four key components: quick scaling, resource pooling, wide network accessibility, and self-service on demand. CC is crucial for common software solutions and provides outstanding services to people over the Internet. Numerous cloud-based apps rely on location, user, and personal data, which might be dangerous for security and privacy. The main goal of cloud service research is to provide safe user authorization techniques that shield private information from possible dangers in cloud computing settings. Four well-known techniques are available for user authentication in cloud systems: location-based (where the user is), ownership-based (what the user owns), characteristic-based (what the user is), and knowledge-based (what the user knows). As shown, each of these techniques is known as an authentication factor. In order to prevent unwanted access to applications, data, goods, services, and resources, common authentication mechanisms including password-based, certificate-based, token-based, and multi-factor approaches are essential. Passwords and user names are common authentication methods that put individuals, financial systems, and online banking services at serious danger. However, multi-factor authentication (MFA) may be used to efficiently mitigate these vulnerabilities. Because an MFA employs several layers of authentication, hackers have a harder time breaking into the system because they have to go through several processes before the security is compromised. Because an MFA demands users to give several forms of authentication before accessing resources or services, it is essential for cloud security. For a number of reasons, this improves security in the digital age. Better theft protection, compliance with regulations, secure remote access, prevention of illegal access, support for risk-based authentication, defense against insider threats, and cultivation of consumer confidence are all provided by them. MFA offers a vital protection layer against several threats and weaknesses in the linked digital world, making it a vital component of a strong cybersecurity strategy. One way to improve the security of sensitive data, including user passwords kept in databases, is to combine several encryption techniques. This method makes it harder for hackers to decrypt passwords by encrypting them several times using various algorithms or keys. Key derivation functions (KDFs), hashing, salt hashing, and numerous encryption layers are common methods. By providing more safe and convenient alternatives than the conventional ways, machine learning has the potential to revolutionize authentication techniques. Machine learning may more successfully authenticate individuals and devices by utilizing behavioral, biometric, or contextual data. This entails gathering and examining data that captures the distinctive traits or actions of a user or device. Biometric characteristics like voice, fingerprints, face recognition, or iris scans, as well as behavioral patterns like typing style, mouse movements, or device usage, may be included in such data. Machine learning algorithms may be used to create models that distinguish between authentic and fraudulent users or devices. The use of machine learning for authentication has several advantages. By

identifying and stopping identity theft, impersonation, and spoofing threats, this enhances security. Additionally, by regularly updating models based on fresh data and feedback, machine learning can adjust to evolving threats and behaviors. A significant difficulty in cloud computing is identifying the most user-accepted and safe authentication technique due to the numerous dangers that might jeopardize the login process. Creating a reliable authentication system for cloud services necessitates a thorough understanding of possible risks and countermeasures. Numerous cryptography methods and user authentication systems have been put out over the past several decades to protect personal data on the cloud. Recent studies, however, show that current cloud computing platforms do not have sufficient security safeguards for user management and authentication. The following are the study's main conclusions. With the use of hybrid cryptographic approaches that offer many levels of protection for user credentials, we present a novel framework that improves security through a multi-factor authentication system utilizing passwords, conditional characteristics, and identities. Users can switch authentication methods as needed thanks to the security algorithm's dynamic adaptation based on user numbers and limits. By predicting common threats, machine learning approaches allow security algorithms to be automatically updated or modified at predetermined intervals.

2. STIMULATING

The goal of this project is to provide an authentication system that is both extremely secure and flexible enough to function in contemporary cloud computing settings. It seeks to improve defense against changing cyberthreats by combining multi-factor authentication with a dynamic hybrid cryptographic paradigm. The method generates secure encryption keys using biometric fingerprint data, conditional characteristics, and passwords. Five pairs of dual-encryption algorithms that automatically adjust in response to threat assessments are part of it. The scope includes creating an intrusion-detection-based decision system that uses data-mining techniques to dynamically choose encryption algorithms. It assesses and reduces threats including guessing attacks, phishing, spoofing, brute force, and impersonation. The project also focuses on using strong key-derivation techniques and multi-layer encryption to secure saved user credentials. It entails assessing cloud-specific vulnerabilities and bolstering remote access settings' defenses. Incorporating machine learning-based risk assessment for intelligent authentication decisions is part of the scope. Additionally, it guarantees adherence to industry best practices and contemporary security regulations. The project focuses on creating an authentication methodology that is both user-friendly and scalable for big cloud systems. There is also performance testing under various assault scenarios. Lastly, the project includes showcasing enhanced access control, secrecy, and integrity in comparison to current cloud authentication methods.

3. OBJECTIVE

This project's primary goal is to provide a multi-factor authentication framework for cloud settings that is both extremely secure and adaptable, overcoming the drawbacks of current authentication methods. By combining fingerprint biometrics, conditional characteristics, and passwords into a single authentication procedure, it seeks to improve cloud security. Creating encryption keys straight from biometric data is another goal in order to stop identity theft and illegal access. A dynamic hybrid cryptographic mechanism that alternates between many algorithm combinations in response to threat prediction is what the system aims to accomplish It seeks to provide more robust defense against brute-force and phishing attacks by combining AES, ECC, Twofish, Blowfish, and HMAC versions. In order to study user behavior and modify encryption models in real time, the project also focuses on integrating machine learning-based intrusion detection. It seeks to lessen the risks connected to conventional password-based authentication. Improving user data stored on cloud servers in terms of privacy, confidentiality, and integrity is another goal. The system's goal is to provide a trustworthy security solution that stops unauthorized login attempts, credential theft, and impersonation. Additionally, it concentrates on fulfilling contemporary security compliance requirements for cloud authentication. The suggested approach also seeks to provide a scalable security architecture that can manage a variety of cloud applications. It aims to provide easy-to-use authentication procedures without sacrificing reliability. Finally, via testing and assessment of assault resistance, the research seeks to demonstrate better performance than current approaches.

3.1 What The Project Is About

Sensitive personal and corporate data is now stored on distant servers due to the quick expansion of cloud computing, yet current authentication methods are still quite susceptible to contemporary assaults. Brute force, phishing, credential theft, and spoofing attacks may readily undermine traditional password-based and single-factor authentication methods. Static verification stages, inadequate encryption, and an inability to adjust to changing threats plague even today's multi-factor authentication solutions. Additionally, cloud platforms do not have a dynamic cryptographic system that may dynamically swap encryption algorithms in response to real-time attack predictions. Passwords that are stored using fixed hashing or encryption are a prime target for hackers, which can result in illegal access and data breaches. Furthermore, the majority of cloud authentication solutions fall short of creating a strong identity verification procedure by combining biometrics,

contextual characteristics, and behavioral analysis. The lack of a hybrid cryptographic paradigm that can dynamically alter algorithms to withstand new attack patterns is another significant issue. Additionally, intrusion-detection learning models that examine unusual behavior during login attempts are not integrated into current systems. This results in inadequate detection of fake credentials, insider risks, and impersonation assaults. The risk of a security breach is further increased by the growing number of cloud users and remote access scenarios. To protect cloud settings, a complete authentication system that combines machine learning-based threat detection, adaptive cryptography, biometric-driven key generation, and multi-factor verification is required.

4. EXISTING SYSTEM:

The majority of current research has the potential to revolutionize authentication techniques by providing safer and easier-to-use alternatives to conventional methods. Machine learning may more successfully authenticate individuals and devices by utilizing behavioral, biometric, or contextual data. This entails gathering and examining data that captures the distinctive traits or actions of a user or device. Biometric characteristics like voice, fingerprints, face recognition, or iris scans, as well as behavioral patterns like typing style, mouse movements, or device usage, may be included in such data. Because an MFA employs several layers of authentication, hackers have a harder time breaking into the system because they have to go through several processes before the security is compromised. Because an MFA demands users to give several forms of authentication before accessing resources or services, it is essential for cloud security. For a number of reasons, this improves security in the digital age.

4.1 Existing System Disadvantages:

- Problems with scalability Static rules or manual management are common methods for controlling security and access.
- Passwords are susceptible to guesswork, reuse, and leakage**.**

4.2 THE PROPOSED SYSTEM

With the use of hybrid cryptographic approaches that offer many levels of protection for user credentials, we present a novel framework that improves security through a multi-factor authentication system utilizing passwords, conditional characteristics, and identities. Users can switch authentication methods as needed thanks to the security algorithm's dynamic adaptation based on user numbers and limits. We assessed the suggested authentication method's dependability, effectiveness, and security against risks including eavesdropping, credential stuffing, man-in-the-middle attacks, account hijacking, and impersonation. An FNN is integrated into the suggested model to generate synthetic data. The model's capacity to generalize and correctly categorize assaults is enhanced by this artificial data generated by FNN, which supplements the training set. The hybrid CNN transformer model receives the generated synthetic data for classification. While the transformer component improved the model's overall performance by capturing long-range relationships, the CNN component successfully caught the spatial hierarchies in the data.

4.2.1 Proposed System Advantage

- Consortium blockchain data access control Increased Scalability, Security, and Data Integrity kept up to date by several reliable parties.
- Automate the enforcement of data sharing and access regulations.

5. METHODOLOGIES

1. Design of User Interfaces

The user must enter their username and password in order to connect to the server. The user can log in to the server directly if they have previously left; otherwise, they must register their information, including their username, password, email address, city, and country. To manage upload and download rates, the database will generate an account for every user. The user ID will be used as the name. To access a particular website, you often need to log in. The query will be searched and displayed.

2. Hybrid CNN–Transformer Model for Attack Prediction

This module is essential to the cloud system's intelligent and proactive security. It analyzes network traffic, user activity patterns, and authentication logs using a hybrid CNN–Transformer architecture. Local and geographical data including IP access patterns, aberrant request behavior, and login frequency are extracted using the CNN component. These characteristics aid in spotting early indicators of malevolent behavior. Long-term dependencies and temporal linkages across sequential data are captured by the Transformer component using attention processes. This makes it possible for the system to identify complex assaults that change over time. When compared to conventional machine learning models, the hybrid technique increases detection accuracy. The model adapts to evolving assault patterns by continually learning from fresh data. It assists in identifying insider threats, brute-force assaults, and illegal access attempts. The smart authentication module receives the prediction findings. Access decisions are dynamically modified based on risk levels. Security breaches are greatly decreased by this proactive prediction capabilities. Additionally, it increases system dependability while reducing false positives. All things considered, this module offers cloud protection based on intelligence.

3. AES

This module uses the AES-256 encryption technique to provide robust data secrecy. A 256-bit key is used

in the symmetric key encryption method AES-256 for maximum security. Before sending sensitive data across the network or storing it in the cloud, it encrypts it. Depending on the user's access rights and the sensitivity of the material, the module dynamically applies encryption. Stronger security is automatically applied to extremely sensitive data. AES-256 is impervious to cryptographic and brute-force assaults. Attackers cannot read encrypted data, even if they manage to access cloud storageIt allows for quick encryption and decryption processes. It is therefore perfect for real-time cloud systems. The module easily incorporates intelligent authentication choices. The encryption keys are kept safe and updated as needed. By doing this, vulnerabilities related to key reuse are avoided. All things considered, AES-256 offers a robust and trustworthy encryption layer for cloud data.

4. SHA - 256

This module employs the SHA-256 hashing technique to focus on data integrity and safe authentication. Passwords and tokens are examples of sensitive inputs that SHA-256 transforms into fixed-length hash results. Instead of storing plaintext data, these hash values are used. The original data cannot be reconstructed from the hash since SHA-256 is irreversible. This keeps passwords safe even in the event that the database is hacked. The module defends against rainbow table and brute-force assaults. By identifying illegal changes, it also guarantees data integrity. Hash values are recalculated and compared for verification during authentication. Any discrepancy suggests tampering or illegal entry. In security systems, SHA-256 is a widely used and reliable standard. The module greatly improves login security. Token creation and secure session validation are supported. Impersonation assaults are less likely as a result. In general, this module improves cloud authentication's dependability and confidence.

6. TECHNIQUE ALGORITHM USED

6.1 Proposed Algorithm

- **Hybrid CNN–Transformer Model for Attack Prediction**

This project's intelligent security core is the Hybrid CNN–Transformer model, which enables proactive attack detection and prediction in cloud systems. From network data, user activity patterns, and authentication records, the Convolutional Neural Network (CNN) component is in charge of extracting geographical and behavioral information. Frequency of access, login behavior, unusual request patterns, and departure from typical usage are some of these characteristics. The Transformer component uses self-attention processes to identify long-term linkages and temporal dependencies in sequential data. The system achieves excellent accuracy in detecting both known and zero-day threats by fusing the Transformer's contextual learning with CNN's feature extraction capabilities. This approach adapts to changing threat patterns by continually learning from fresh access data. Smart authentication decisions are dynamically influenced by the anticipated risk levels. It aids in stopping illegal access before data is exposed. The hybrid approach increases detection reliability while drastically lowering false positives. The total resilience of cloud security solutions is improved by this clever strategy.

AES Algorithm

In this project, powerful symmetric encryption using the AES method is used to guarantee cloud data secrecy. Before being stored or sent, AES encrypts sensitive data that a user uploads to the cloud using a secret key. Depending on the access risk levels that the attack detection module predicts, the encryption strength can be applied adaptively. AES makes guarantee that the data is unintelligible by unauthorized users even in the event that the cloud server or communication channel is hacked. It is appropriate for real-time cloud applications because to its quick encryption and decryption procedures. Large-scale data encryption is supported by AES with no performance overhead. The method offers defense against cryptographic and brute-force assaults. Data can only be decrypted by authorized users thanks to secure key handling. AES is essential for safeguarding user privacy. The comprehensive foundation for cloud security is strengthened by its integration.

SHA-256 Algorithm

The cloud system uses the SHA-256 algorithm to provide secure authentication and data integrity. It creates a unique 256-bit hash value for encrypted data, authentication tokens, and user credentials. A slight alteration in the data results in an entirely new hash, making it simple to identify manipulation. By keeping just hash values, SHA-256 stops plaintext passwords from being stored. This guards against illegal access and credential theft. Additionally, the technique is utilized to confirm data integrity both during transmission and retrieval By confirming user identities, it facilitates safe authentication. SHA-256 improves defense against rainbow table and brute-force attacks. Reliability is guaranteed by its standardization and credibility. The algorithm plays a major role in preserving the authenticity and trustworthiness of data.

Multi-Factor Authentication (MFA)

Because an MFA employs several layers of authentication, hackers have a harder time breaking into the system because they have to go through several processes before the security is compromised. Because an MFA demands users to give several forms of authentication before accessing resources or services, it is essential for cloud security. For a number of reasons, this improves security in the digital age.

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 4(2026)

7. SYSTEM ARCHITECTURE

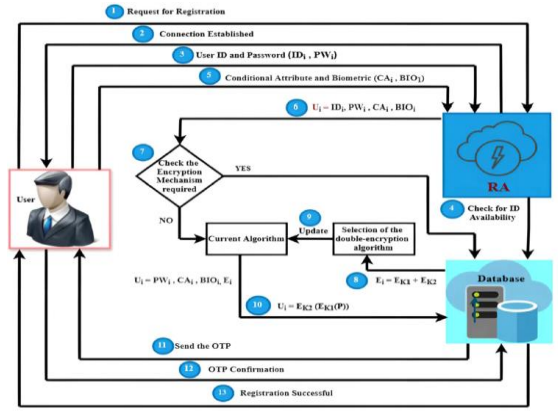

FIG:7 System Architecture

8. RESULTS

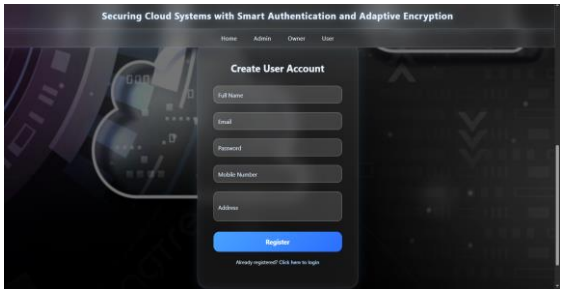

Fig:8.1 User Register Page

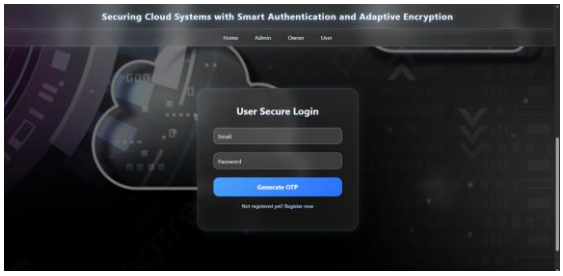

Fig:8.2 User Login Page

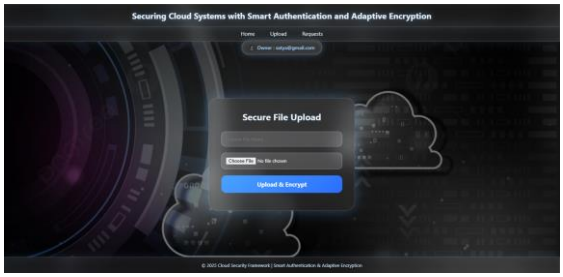

Fig 8.3 Owner Upload data

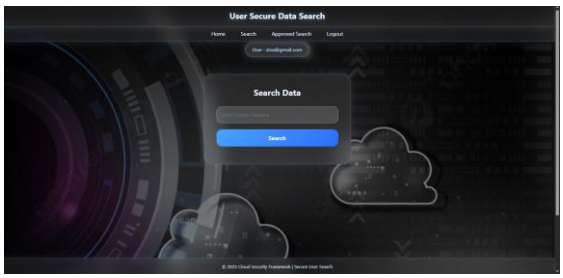

Fig 8.4 User Search data

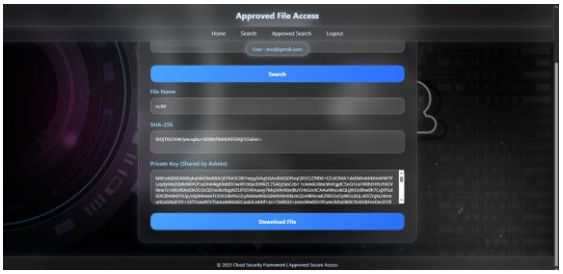

Fig 8.5 User Searched file data

9. CONCLUSION

In conclusion, by addressing significant flaws in conventional authentication methods, the suggested smart authentication and adaptive encryption framework successfully improves security in cloud computing settings. The system guarantees robust and trustworthy user verification by including multi-factor authentication using passwords, conditional characteristics, and biometric fingerprint data. Data confidentiality and resilience against growing cyber threats are greatly enhanced by the use of a hybrid cryptographic strategy with constantly changing encryption algorithms. The dual-encryption approach offers multilayer security and strong resistance against brute-force, spoofing, phishing, guessing, and impersonation attacks by combining algorithms like AES, ECC, Twofish, Blowfish, and HMAC variations. Adaptive security responses and real-time threat prediction are made possible by the intelligent intrusion-detection-based approach. The system may modify the encryption strength in response to identified danger levels thanks to this dynamic nature. The framework delivers good security with a manageable performance overhead, according to experimental assessment. The solution is appropriate for contemporary cloud infrastructures due to its scalable and modular architecture. Additionally, by limiting illegal access and data leaks, the system improves user confidence. Overall, this project establishes a strong foundation for secure cloud systems and highlights the effectiveness of combining smart authentication with adaptive cryptography for next-generation cloud security solutions.

10. FUTURE ENHANCEMENT

Future improvements to the suggested approach may concentrate on enhancing cloud environments' security, scalability, and usability. To enhance attack prediction while protecting user privacy, sophisticated deep learning models like federated learning may be incorporated. For improved multi-factor security, the authentication framework may be expanded to accommodate more biometric elements like face recognition or iris scanning. Throughout user sessions, ongoing authentication and authorization may be guaranteed by integration with zero-trust architecture. Decentralized and impenetrable identity verification may be achieved by integrating blockchain-based identity management. To fend against upcoming quantum assaults, post-quantum cryptographic

techniques can be added to the adaptive encryption engine. Attack signatures and risk models may be updated dynamically by integrating real-time threat intelligence inputs. Lightweight cryptographic techniques can be used to improve the system for edge and IoT contexts. Scalability and fault tolerance may be increased with cloud-native deployment using microservices and containerization. Reducing manual security settings may be achieved by implementing automated policy learning. Dashboards with improved visualization can offer more in-depth security insights. It is possible to provide support for hybrid and multi-cloud cloud setups. It is possible to improve adherence to international security norms. All things considered, these improvements will increase the system's intelligence, resilience, and readiness for the future.

REFERENCES

[1] G. Ramesh, J. Logeshwaran, and V. Aravindarajan, "A secured database monitoring method to improve data backup and recovery operations in cloud computing," BOHR Int. J. Comput. Sci., vol. 2, no. 1, pp. 1–7, 2022, doi: 10.54646/bijcs.019.

[2] B. T. Rao, "A study on data storage security issues in cloud computing," Procedia Comput. Sci., vol. 92, pp. 128–135, 2016, doi: 10.1016/j.procs.2016.07.335.

[3] K. Latha and T. Sheela, "Block based data security and data distribution on multi cloud environment," J. Ambient Intell. Humanized Comput., vol. 15, 2024, Art. no. 53, doi: 10.1007/s12652-019-01395-y.

[4] K. Raju and M. Chinnadurai, "An identity-based secure and optimal authentication scheme for the cloud computing environment," Comput., Mater. Continua, vol. 69, no. 1, pp. 1057–1072, 2021, doi: 10.32604/cmc.2021.016068.

[5] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," Cryptogr., vol. 2, no. 1, pp. 1–31, 2018, doi: 10.3390/cryptography2010001. [6] S. Sudha and S. S. Manikandasaran, "A survey on different authentication schemes in cloud computing environment," Int. J. Manage., IT Eng., vol. 9, no. 1, pp. 359–375, 2019.

[7] A. Alhothaily, C. Hu, A. Alrawais, T. Song, X. Cheng, and D. Chen, "A secure and practical authentication scheme using personal devices," IEEE Access, vol. 5, pp. 11677–11687, 2017, doi: 10.1109/ACCESS.2017.2717862.

[8] N. Anusha and N. R. Suma, "A review on secured file system using multi-factor authentication with visual cryptography for cloud environment," Int. Res. J. Modernization Eng. Technol. Sci., vol. 4, no. 6, pp. 4433–4436, 2012.

[9] Cybersecurity, "What is password encryption and how does it work," Accessed: Jun. 15, 2023. [Online]. Available: https://teampassword. com/blog/what-is-password-encryption-and-how-much-is-enough

[10] M. Hazratifard, F. Gebali, and M. Mamun, "Using machine learning for dynamic authentication in telehealth: A tutorial," Sensors, vol. 22, no. 19, 2022, Art. no. 7655, doi: 10.3390/s22197655.

[11] N. Siddiqui, L. Pryor, and R. Dave, "User authentication schemes using machine learning methods—A review," in Proc. Int. Conf. Commun. Comput. Technol., Singapore, 2021, pp. 703–723, doi: 10.1007/ 978-981-16-3246-4_54.

[12] T. N. Tan and H. Lee, "High-secure fingerprint authentication system using ring-LWE cryptography," IEEE Access, vol. 7, pp. 23379–23387, 2019, doi: 10.1109/ACCESS.2019.2899359.

[13] C. Singh and D. Singh, "A 3-level multifactor authentication scheme for cloud computing," Int. J. Comput. Eng. Technol., vol. 10, no. 1, pp. 184–195, 2019. [Online]. Available: https://ssrn.com/abstract= 3537621

[14] S. A. Sagar, O. Bhat, M. Raina, and S. Patil, "Authentication system using cryptographic secure password storage," Int. J. Innov. Res. Eng. Multidisciplinary Phys. Sci., vol. 6, no. 6, pp. 76–78, 2018.

[15] V. Kakkad, M. Patel, and M. Shah, "Biometric authentication and image encryption for image security in cloud framework," Multiscale Multidisciplinary Model., Exp. Des., vol. 2, no. 4, pp. 233–248, 2019, doi: 10.1007/s41939-019-00049-y.

[16] M. Obaidat, J. Brown, S. Obeidat, and M. Rawashdeh, "A hybrid dynamic encryption scheme for multi-factor verification: A novel paradigm for remote authentication," Sensors, vol. 20, no. 5, 2020, Art. no. 4212, doi: 10.3390/s20154212.

[17] M. A. Khan, M. T. Quasim, N. S. Alghamdi, and M. Y. Khan, "A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data," IEEE Access, vol. 8, pp. 52018–52027, 2020, doi: 10.1109/ACCESS.2020.2980739.

[18] K. DeviPriya and S. Lingamgunta, "Multi factor two-way hash-based authentication in cloud computing," Int. J. Cloud Appl. Comput., vol. 10, no. 2, 2020, Art. no. 21, doi: 10.4018/IJCAC.2020040104.

[19] K. M. Prabha and P. V. Saraswathi, "Suppressed K-anonymity multifactor authentication based Schmidt-Samoa cryptography for privacy preserved data access in cloud computing," Comput. Commun., vol. 158, pp. 85–94, 2020, doi: 10.1016/j.comcom.2020.04.057.

[20] B. O. ALSaleem and A. I. Alshoshan, "Multi-factor authentication to systems login," in Proc. Nat. Comput. Colleges Conf., 2021, pp. 1–4, doi: 10.1109/NCCC49330.2021.9428806.

[21] K. Venkatachalam, P. Prabu, A. Almutairi, and M. Abouhawwash, "Secure biometric authentication with de-duplication on distributed cloud storage," PeerJ Comput. Sci., vol. 7, 2021, Art. no. e569, doi: 10.7717/peerj-cs.569.

[22] J. Mohammed Ubada and M. Mohamed Surputheen, "Evaluation of multifactor user security through multi authentication verifiable hybrid revert encryption for cloud computing environment," Int. J.

Comput. Sci. Netw. Secur., vol. 22, no. 9, pp. 481–488, 2022, doi: 10.22937/IJCSNS.2022.22.9.62.
[23] S. Kaur, G. Kaur, and M. Shabaz, "A secure two-factor authentication framework in cloud computing," Secur. Commun. Netw., vol. 2022, no. 1, 2022, Art. no. 7540891, doi: 10.1155/2022/7540891.
[24] D. Carrillo-Torres, J. A. Pérez-Díaz, J. A. Cantoral-Ceballos, and C. Vargas-Rosales, "A novel multi-factor authentication algorithm based on image recognition and user established relations," Appl. Sci., vol. 13, no. 3, 2023, Art. no. 1374, doi: 10.3390/app13031374.
[25] D. V. K. Vengala, D. Kavitha, and A. S. Kumar, "Three factor authentication system with modified ECC based secured data transfer: Untrusted cloud environment," Complex Intell. Syst., vol. 9, no. 3, pp. 2915–2928, 2023, doi: 10.1007/s40747-021-00305-0.
[26] K. Rajeshkumar, S. Dhanasekaran, and V. Vasudevan, "A novel three-factor authentication and optimal mapreduce frameworks for secure medical Big Data transmission over the cloud with SHAXECC," Multimedia Tools Appl., vol. 24, pp. 68363–68391, 2024, doi: 10.1007/s11042-024-18147-6.
[27] S. Khan and A. Mailewa, "Predicting anomalies in computer networks using autoencoder - based representation learning," Int. J. Informat. Commun. Technol., vol. 13, no. 1, pp. 9–26, 2024, doi: 10.11591/ijict.v13i1.
[28] K. L. Chiew and B. Hui, "An improved network intrusion detection method based on CNN-LSTM-SA," J. Adv. Res. Appl. Sci. Eng. Technol., vol. 44, no. 1, pp. 225–238, 2025, doi: 10.37934/araset.44.1.225238.
[29] I. Aljamal, A. Tekeoglu, K. Bekiroglu, and S. Sengupta, "Hybrid intru- ˘ sion detection system using machine learning techniques in cloud computing environments," in Proc. IEEE 17th Int. Conf. Softw. Eng. Res., Manage. Appl., 2019, pp. 84–89, doi: 10.1109/SERA.2019.8886794.
[30] F. Alserhani and A. Aljared, "Evaluating ensemble learning mechanisms for predicting advanced cyber attacks," Appl. Sci., vol. 13, no. 24, 2023, Art. no. 13310, doi: 10.3390/app132413310.
[31] M. Singh, N. Baranwal, K. N. Singh, A. K. Singh, and H. Zhou, "Deep learning-based biometric image feature extraction for securing medical images through data hiding and joint encryption–compression," J. Inf. Secur. Appl., vol. 79, 2023, Art. no. 103628, doi: 10.1016/j.jisa.2023.103628.
[32] T. Patil and S. Nandusekar, "Different techniques used in the process of feature extraction from fingerprint," Int. J. Innov. Eng. Res. Technol., vol. 6, no. 9, pp. 1–10, 2019.
[33] M. Kumar and D. Singh, "Biometric cryptosystem based on fingerprint authentication and cryptography technique," Int. Res. J. PMC, vol. 2, no. 1, pp. 26–39, 2023, doi: 10.61916/prmn.2023.v0101.004.