

Enhancing Cloud Security: A Multi-Factor Authentication and Adaptive Cryptography Approach Using Machine Learning Techniques

K. SASIKUMAR  AND SIVAKUMAR NAGARAJAN 

School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, India

CORRESPONDING AUTHOR: SIVAKUMAR NAGARAJAN (e-mail: nsivakumar@vit.ac.in).

This work was supported by Vellore Institute of Technology, Vellore 632014, India.

This article has supplementary downloadable material available at <https://doi.org/10.1109/OJCS.2025.3538557>, provided by the authors.

ABSTRACT The rapid expansion of cloud computing underscores the critical need for advanced security measures to protect sensitive data on remote servers. Authentication is crucial for safeguarding these data. Despite various proposed methods, vulnerabilities persist. This article introduces a novel multi-factor authentication system integrated with a hybrid cryptographic framework that dynamically changes encryption algorithms using machine learning techniques based on an intrusion-detection system. The proposed system employs passwords, conditional attributes, and fingerprint authentication to derive the encryption key from fingerprint data. It uses a dual-encryption strategy that combines five algorithm pairs: AES + HMAC (SHA-256), ECC + HMAC (SHA-512), HMAC-MD5 + PBKDF2, Twofish + Argon2, and Blowfish + HMAC SHA3-256. A Hybrid CNN-transformer model predicts and classifies attacks by dynamically adjusting an encryption algorithm to secure the data. The framework exhibited strong resilience against brute force, spoofing, phishing, guessing, and impersonation attacks. The proposed model achieved a commendable accuracy of 96.8%, outperforming other models. Implementing this framework in a cloud authentication environment significantly enhances data confidentiality and protects against unauthorized access. This study highlights the potential of combining multi-factor authentication and adaptive cryptography to obtain robust cloud security solutions.

INDEX TERMS Adaptive cryptography, attack prediction, cloud security, dual encryption, dynamic encryption algorithms, hybrid CNN-transformer model, machine learning techniques, multi-factor authentication.

I. INTRODUCTION

The advent of cloud computing [CC] has fundamentally changed how businesses and individuals store and manage data [1]. CC allows data and application software to be stored with minimal administrative effort while offering on-demand services via the internet [2]. The integration of four essential elements can convert any platform into a cloud-based infrastructure: self-service on demand, wide network accessibility, resource pooling, and rapid scalability [3]. CC offers excellent services to individuals through the Internet, and is essential for everyday software solutions. Many cloud-supported applications rely on user, personal, and location information that can pose security and privacy risks. Research on cloud services

primarily focuses on developing secure user authorization methods to protect sensitive data from potential threats in cloud computing environments [4]. User authentication in cloud systems can be conducted using four widely recognized methods: knowledge-based (what the user knows), ownership-based (what the user has), characteristic-based (what the user is), and location-based (where the user is). Each of these methods is referred to as an authentication factor [5], as illustrated in Fig. 1. Common authentication methods such as password-based, certificate-based, token-based and multi-factor techniques play a crucial role in preventing unauthorized entry to applications, information, products, services, and resources [6].



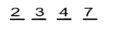







Evidence of Knowledge	 Password	 Security Question	 PIN
Evidence of Ownership	 Smartphone	 Smart card	 Hardware Token
Evidence of Characteristic	 Fingerprint	 Retina Pattern	 Face Recognition
Evidence of Location	 Location		

FIGURE 1. Key authentication factors.

Common authentication techniques such as passwords and user names pose significant risks to online banking services, financial systems, and users [7]. However, these risks can be effectively managed by implementing multi-factor authentication (MFA). An MFA uses different levels of authentication, making it difficult for hackers to penetrate the system because they must bypass multiple steps before compromising the security [8]. An MFA is vital for cloud security because it requires users to provide multiple forms of verification before accessing resources or services. This enhances security in the digital age for several reasons. They offer better protection against theft, meet compliance requirements, secure remote access, prevent unauthorized access, support risk-based authentication, protect against insider threats, and foster customer trust and confidence. As a crucial element of a robust cybersecurity strategy, MFA provides an essential defense layer against various threats and vulnerabilities in the interconnected digital world.

Employing multiple encryption methods to protect passwords is a strategy to enhance the security of sensitive data such as user passwords stored in databases. This approach encrypts passwords multiple times using different algorithms or keys thereby making it more difficult for hackers to crack them. Common techniques include hashing, salt hashing, key derivation functions (KDFs), and multiple encryption layers [9]. Machine learning has the potential to transform authentication methods by offering more secure and user-friendly options than the traditional approaches. By leveraging behavioral, biometric, or contextual data, machine learning can authenticate users and devices more effectively. This involves collecting and analyzing data that reflects the unique characteristics or behaviors of a user or device. Such data may include biometric traits such as facial recognition, fingerprints, voice, or iris scans as well as behavioral patterns such as typing style, mouse movements, or device usage. Models can be developed using machine learning algorithms to differentiate between legitimate and fraudulent users or devices. There are numerous benefits of using machine learning for authentication. This improves security by detecting and preventing identity theft, impersonation, and spoofing attacks. In addition, machine learning can adapt to changing threats and behaviors by continuously updating models based on new data and feedback [10], [11].

Finding the most secure authentication method that is widely accepted by users is a major challenge in cloud computing because of various threats that can compromise the login process. Developing a trustworthy authentication method for cloud services requires detailed awareness of potential threats and techniques to prevent them. Over the last several decades, many user authentication systems and cryptographic techniques have been proposed for securing personal information in the cloud. However, recent research indicates that existing cloud computing systems lack adequate security measures for user authentication and management. The primary findings of this study are as follows.

- 1) We propose an innovative framework that enhances security through a multi-factor authentication system using passwords, conditional attributes, and identities, supported by hybrid cryptography techniques that provide multiple layers of protection for user credentials.
- 2) The security algorithm adapts dynamically based on user numbers and limitations, allowing users to switch authentication methods, as needed.
- 3) Machine learning techniques predict prevalent attacks, enabling automatic updates or changes in security algorithms at specified intervals.
- 4) We evaluated the reliability, efficiency, and security of the proposed authentication technique against threats such as man-in-the-middle attacks, eavesdropping, credential stuffing, account hijacking, and impersonation.

The rest of this article is organized as follows. Section II presents an overview of previous research findings, Section III elaborates on the proposed method, and Section IV, introduces a machine-learning approach for attack prediction. Section V discusses the selection of the dynamic encryption algorithm based on predicted attacks. Section VI discusses the performance findings and Section VII concludes the article.

II. LITERATURE SURVEY

Tan et al. [12] introduced a more secure biometric authentication approach using ring learning with error cryptography (ring-LWE), a post-quantum cryptosystem designed to protect user data. They proposed a delay-optimized high-accuracy method for efficiently extracting fingerprint features from images. After extraction, the ring-LWE technique was applied, and number theoretic transform (NTT) polynomial multiplications were used to accelerate the process of encoding and decoding. This leads to a significant decrease in the processing time for fingerprint authentication, ensuring the effective protection of fingerprint data. The simulation results demonstrate that the framework has a minimal processing duration and is suitable for real-time authentication systems. However, further research and analysis are required to fully understand the security and limitations of ring-LWE cryptography in fingerprint authentication systems. Charanjeet et al. [13] developed a three-tier multi-factor authentication solution specifically for cloud computing. This approach integrates two-level password encryption, OTP verification, and

graphical screen interaction. The two-level encryption feature enhances security by combining the SHA-1 and AES algorithms. Multi-factor authentication significantly reduced the risk of data leakage.

Sagar et al. [14] proposed a password authentication framework that enhances security by integrating elliptic curve cryptography (ECC) and attribute-based encryption. In this framework, passwords are converted into hash values using ECC, and then transformed into negative passwords using a specialized algorithm. These negative passwords are further encrypted into Encrypted Negative Passwords (ENPs) using multi-iteration encryption that combines cryptographic hash functions, negative passwords, and symmetric key algorithms. This method strengthens the protection against dictionary attacks without requiring additional elements. Future improvements in negative password generation algorithms could increase complexity and randomness, further enhancing security. Another study [15] aimed to improve the cloud image security by introducing a biometric authentication technique. The proposed approach has two stages: picture compression with the discrete wavelet transform method, and encryption with a hybrid of SHA and Blowfish. However, this method is vulnerable to spoofing.

In this study [16], the authors introduced a secure authentication approach combining layered encryption with a two-step verification process, specifically designed to prevent cyber intrusion, such as replay and MiTM attacks. Khan et al. [17] presented a secure system that authenticated patients by using their names, passwords, and biometric data. The SHA-512 algorithm was used to ensure data integrity. Once verified, the patient's mobile sensor device is activated and continuously sends information to the cloud system. To securely transmit sensor information, the system employs a Caesar cipher and enhanced elliptic-curve cryptography (IECC). The combination of improved ECC and SHA-512 enhances data integrity and security, with the upgraded ECC incorporating an additional secret key for increased security. However, the report did not provide a comprehensive comparison with the other encryption algorithms.

This study [18] introduces a secure mutual authentication system based on hashing, incorporating measures such as mathematical hashing features, signatures, nonce metrics, user IDs, and passwords to protect against various attacks. By combining hashing and certification with traditional authentication methods, the system ensures confidentiality and integrity. Mutual authentication is emphasized when both parties verify each other. Regular password updates were implemented to prevent prediction attacks. The registration process involves upgrading certificates to align them with user preferences, enhancing the dynamic nature of the system, and providing robust secure authentication. The traditional one-factor authentication strategy is ineffective owing to the risk of disclosing critical information. To resolve this problem, Prabha et al. [19] suggested an SKMA-SC multi-factor authentication approach. This solution securely maintains client information in a cloud storage database and enhances

privacy protection by using suppression techniques. SKMA-SC improves privacy, authentication accuracy, and computing complexity by combining factors, such as passwords, one-time tokens, and conditional features. The experimental results show that SKMA-SC increases privacy protection while reducing computing complexity compared with previous approaches. Future research could explore other cryptographic algorithms for the SKMA-SC.

Saleem et al. [20] introduced a convenient and affordable multi-factor authentication system that did not require any special setups. During registration, users choose and memorize three images as graphical passwords, that they must correctly identify when logging in. This system effectively prevents keyloggers and screen capture attacks. However, there are potential security risks associated with relying solely on graphical passwords, such as vulnerabilities related to image memorization. Kumar et al. [21] developed a biometric authentication system to grant user access to a cloud-based environment. The system combines biometric authentication with cryptographic methods. It captures fingerprint features from images using a self-learning algorithm, stores them in a database for authentication, and converts them into bio keys using hash functions. The suggested approach is more cost-effective in terms of computing and communication resources than the current techniques. Researchers have suggested that future improvements could involve the use of other biometric methods to enhance user authentication processes.

Raju et al. [4] introduced a new HMO-ISOA scheme using iris and fingerprint biometrics to secure cloud computing environments. This approach involves a pattern-based feature extraction process to obtain characteristics from biometric data, which are then used in a hybrid social spider and dragonfly algorithm to determine optimal solutions. These solutions serve as keys for the AES encryption process, which encodes data before it is sent to the cloud. Simulations have demonstrated improved resistance against man-in-the-middle attacks, and future enhancements may include the utilization of compression models for better performance. Ubada et al. [22] proposed the MAVHRE scheme to enhance cloud security authentication by incorporating multiple factors. This method focuses on efficiently restricting access and dynamically generating a one-time-use password (OTUP) for services. It prioritizes confirming the user's OTUP before granting access to a cloud. Once the OTUP is verified, user authentication is validated through graphical user authentication. This innovative approach is highly efficient and streamlines cloud-computing tasks. Future security measures could include facial recognition. Kaur et al. [23] introduced a new two-factor authentication system for cloud computing security to improve traditional methods. This system helps prevent unauthorized access, session hijacking, MITM attacks, and replay attacks by combining one-way hashes and nonce-based verification with standard approaches. Security was further strengthened by incorporating email and mobile OTP verifications.

Carrillo et al. [24] discussed an MFA system that uses a non-biometric method, eliminating the need for additional

hardware. This innovative approach relies on images and connections and requires users to create a personalized link between two photos to complete the authentication process. By incorporating both text and images, the password space can be expanded, thereby enhancing the security and robustness of the system against various threats. However, a drawback of this MFA technique is that users might struggle to remember their authentication components over time, especially the relationships between the images. Vengala et al. [25] proposed a concept for improving cloud storage security using a Modified ECC and three-factor authentication. This model employs SHA-512, CHA, and MECC to authenticate and secure the data transfers. During the verification process, the SHA-512 algorithm was combined with CCP for added security. The proposed method offers improved security compared to the current methods. Future studies could expand this approach to store data in distributed cloud storage, thereby achieving higher security levels. In addition, it is crucial to analyze the resistance of the model to various attacks. Rajeshkumar et al. [26] introduced an innovative three-factor authentication (3FA) scheme and optimized the MR architecture to securely transmit healthcare Big Data over a cloud platform. This was achieved by integrating the SHAXECC algorithm to ensure network protection against unauthorized access. The SHAXECC algorithm has also been used to improve data security and confidentiality in cloud-enabled healthcare systems.

Khan et al. [27] used a combination of unsupervised and supervised techniques in intrusion detection systems (IDS) to address advanced network threats. The DAE+SVM neural network technique has proven effective in classification and performance, improving the resilience of the model against evolving and adaptive network attacks in dynamic threat landscapes. Chiew et al. [28] demonstrated that various machine learning algorithms can effectively detect network intrusions, with the CNN-LSTM-SA approach outperforming traditional classifiers. The CNN-LSTM-SA method achieved the highest F1 score of 93.26% and an accuracy of 93.72% in both the binary and multiclass tests. Future research could explore more sophisticated methods for deep learning and machine learning to further improve the detection performance.

Aljamal et al. [29] described a network-based anomalous detection technique designed for the virtual machine level in the cloud. This system achieved an accuracy of 84.3% using a hybrid method that combines k-means clustering and SVM classification. Although this approach enhances the intrusion detection system, there is potential for further improvement to increase the accuracy, including classifying features based on different attack methods. Alserhani et al. [30] developed a research methodology involving eight classifiers to increase the accuracy and resilience of an NIDS. The classifiers included K-Nearest Neighbors, Random Forest, Logistic Regression, Decision Tree, XGBoost, CatBoost, Support Vector Machine, and Artificial Neural Networks. Each classifier was trained using various techniques depending on the design specifications. However, this study focuses on specific ensemble methods

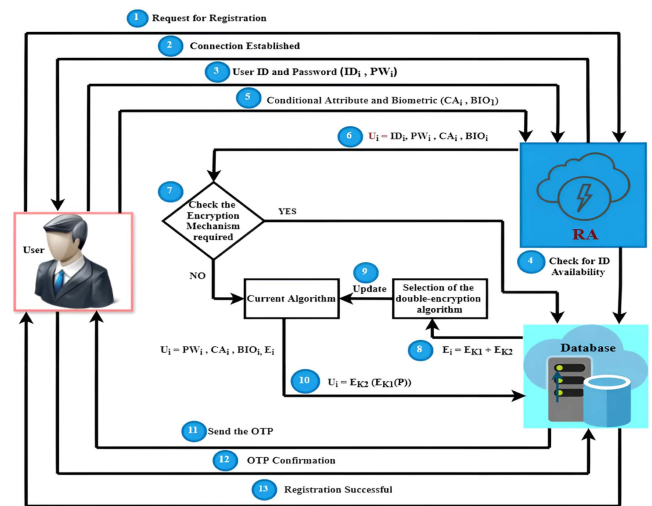


FIGURE 2. Registration phase.

and algorithm pairings, potentially overlooking other effective strategies. Further exploration of the classifications based on different attack types is required.

The current literature suggests that both multi-factor authentication (MFA) and anomaly detection systems require significant enhancement. MFA systems require improvements in user-friendliness, security optimization, and comprehensive method analysis, with further research on advanced techniques, biometrics, and cryptographic methods. Anomaly detection systems should focus on refining hybrid methods, enhancing attack-specific classification, boosting real-time performance, and conducting thorough security analysis. Addressing the challenges of various attack types and ensuring cost efficiency are critical. Resolving these issues can significantly improve the security, accuracy, and performance of cloud-based anomaly detection and authentication systems.

III. PROPOSED SCHEMA

In this section, we present an improved multi-factor authentication framework designed for cloud environments. The proposed scheme involves three key phases: (1) registration, (2) login and authentication, and (3) identity update.

A. USER REGISTRATION PHASE

The user initiates a request for a new registration. Once a request is received, the Registration Authority (RA) establishes a secure communication channel. User (U_i) then proceeds with the registration process using RA, as shown in Fig. 2.

- To begin the registration process, user (U_i) submits its selected user ID (UID_i) to the Registration Authority (RA). The RA then verifies the availability of UID_i by checking it against the existing User List. If UID_i is already obtained, the user is prompted to select a different UID_i . Once a unique UID_i is confirmed, the user is instructed to create a strong password (PW_i). After successfully setting the password, the registration proceeds to the next stage of the process

- The Registration Authority (RA) initiates the creation of conditional attributes (CA_i) for each user by administering a series of security questions. Users are required to select more than one conditional attribute, defined according to the following formula:

$$ID_i \rightarrow (CA_1, CA_2, \dots, CA_n)$$

Next, users submit their biometric information (BIO_i) during this phase, which involves feature extraction techniques [31], [32] to derive relevant features. From these extracted features, Biometric Master Key (BMK_i) was generated [33]. Finally, the RA obtains all the information from the user.

$$U_i \rightarrow (UID_i, PW_i, CA_i, BIO_i, BMK_i)$$

- During the encryption algorithm selection phase, RA verifies the status of the encryption machine to determine the appropriate encryption algorithm. This selection process adheres to a specific rule in which cryptographic mechanisms are rotated periodically for groups of N users.
- The value of N is chosen to ensure that the computational overhead is optimal and the security is not compromised. The database already contained a list of five pairs of encryption mechanisms.
- Based on the chosen encryption mechanisms, a dual encryption approach was applied to encrypt specific U_i details such as (PW_i, CA_i, BIO_i, E_i). These encrypted details, along with information about the encryption techniques (E_i) are stored securely in a database. The Biometric Master Key (BMK_i) generated from the user's biometric data (BMK_i) is split into two keys: K_1 for the first encryption mechanism (E_1) and K_2 for the second encryption mechanism (E_2).
- Subsequently the OTP was sent to the user's mobile number and email account. Once the OTP is confirmed by the user during registration, the registration process is completed.

In this study, five sets of dual encryption algorithms were employed to encrypt user information. A hybrid encryption algorithm was chosen for each user based on specific conditions and then used to encrypt the information. The dual encryption algorithms used were AES + HMAC (SHA-256), ECC + HMAC (SHA-512), HMAC-MD5 + PBKDF2, Twofish + Argon2, and Blowfish + HMAC SHA3-2.

B. AUTHENTICATION PHASE

During the authentication phase, the client's identity is confirmed before they can access the cloud data services. This process occurs when clients submit requests for cloud services.

- Upon receiving the login request, the proposed framework initiates a multi-factor authentication process. Initially, the users were prompted to enter their UID_i and PW_i . Subsequently, the RA verifies the existence of the UID_i . If a UID_i exists, the PW_i is encrypted and compared with the encrypted password in the database. If

a match is found, then the process proceeds to the next authentication step.

- At this stage, the user is prompted to provide necessary CA_i information after verification by the server. If the verification is successful, the user is permitted to input the BIO_i information. These data were processed and compared with server records. If a match is found, the login will be successful; otherwise, it will fail.

Although fingerprint biometric authentication is widely recognized for its convenience and effectiveness, it is essential to acknowledge its limitations. Various factors, including skin conditions, moisture, quality of the fingerprint reader, unavailability of the scanner, and difficulties with fingerprint recognition owing to issues such as worn or damaged skin, can impede its overall performance. To address these challenges, we incorporate the concept of "skip" as a fallback mechanism when biometric authentication fails or is unavailable. This allows us to explain how the skip concept can be utilized in MFA systems with biometric authentication. There are several types of skip concepts are available, such as one-time tokens (OTT), hardware tokens, and push notifications, and we chose the OTT method for our implementation.

- When the user is directed to fingerprint authentication, users are presented with the option of skipping the connection if they are unable to provide necessary the biometric details. The skip concept can only be used by users under unavoidable circumstances. When the User selects the skip connection option, the server generates a new OTT. The OTT password was randomly generated by the system using the formulation provided below.
 $UID = OTT$ where $OTT = \{r\}$
- The OTT for a specific UID_i is generated by randomly choosing a large prime number 'r' using the method described above. Every time a new OTT is generated for UID_i , it is sent to the user's mobile number and email account via a secure channel. This OTT is intended for single login use, ensuring that only authorized users with an OTT can access the authentication process
- In our system, we implemented various approaches to address the issue of the excessive use of the skip option. We closely monitored its usage and established specific boundaries to deter its overreliance. If someone exceeds the limit, we promptly notify both the individual and administrator. In addition, we introduced a system that restricts users to a set number of skips per month, typically three, in order to strike a balance between convenience and security. A visual representation of the authentication phase is shown in Fig. 3.

C. IDENTITY UPDATE PHASE

The Identity Update Phase is an essential part of the user management system responsible for managing modifications to a user's identity details while safeguarding the security and accuracy of the data stored. In this phase, users (U_i) have the option to update various aspects of their identity information, namely, their password (PW), Conditional Attributes (CA), or

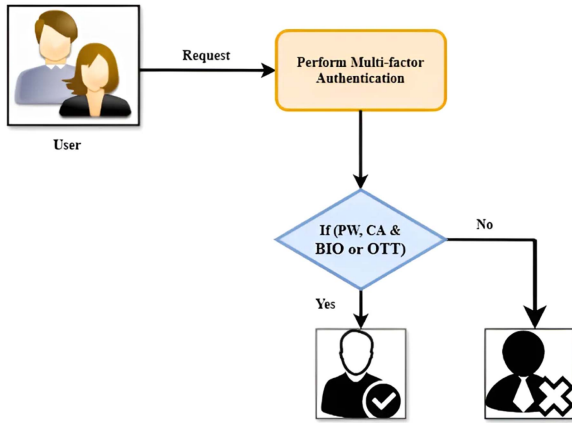


FIGURE 3. Authentication phase flow processes.

Biometric Information (BIO). The procedure begins with the user choosing the desired update option using the interface provided by the system. The following procedures were performed, depending on the selected option.

- **Updating Password (PW):** The user inputs their previous password (PW_{old}) and BIO to authenticate their identity. Subsequently, the user inputs and confirms the new password (PW_{new}). OTP to the user's registered mobile number and email account for additional verification. Upon receiving and confirming the OTP, the new password undergoes dual encryption using two keys, K_1 and K_2 to enhance security ($PW = E_{K_2}(E_{K_1}(PW_{new}))$). The encrypted password is then stored securely in a database.
- **Updating Conditional Attributes (CA):** To update the conditional attributes, the user must first input their biometric information (BIO_i) and the current password (PW_i) for authentication. The system then presents a selection of security questions, from which the user must choose and answer three questions. After completing this step, the OTP is sent to the user's mobile phone and email. The user confirms that the OTP and the new conditional attributes are encrypted using the dual-encryption scheme ($CA = E_{K_2}(E_{K_1}(CA_{new}))$). These encrypted attributes were stored in a database.
- **Updating Biometric Information (BIO):** When updating the biometric information, the user must input their current password (PW_i) and conditional attributes (CA_i). Once authenticated, the system grants access to the fingerprint-update interface, where the user can provide new biometric information (BIO_{new}). The system verifies the new biometric information against existing data to ensure that the update is legitimate. The OTP was sent for further verification. After the user confirms the OTP, the new biometric information is encrypted ($BIO = E_{K_2}(E_{K_1}(BIO_{new}))$) and stored securely in the database.

Upon the successful completion of the biometric update process, the recently acquired biometric information is input

into the key-generation algorithm to produce a biometric key. Subsequently, this key was compared with to existing key. If there are any differences, then the PWD, CA, and BIO of the respective users are encrypted using the newly generated key and stored securely in the database. For each update type, the system maintains an audit log containing the user ID, timestamp, and authentication method to ensure traceability and accountability.

IV. HYBRID CNN-TRANSFORMER MODEL FOR ATTACK PREDICTION

The UNSW-NB15 [34] dataset, developed by the Australian Center for Cyber Security (ACCS) using the IXIA PerfectStorm tool, is a valuable resource for testing network intrusion detection systems (NIDS). It includes contemporary attack scenarios and regular activities, making it ideal for evaluating and comparing machine-learning methods for network anomaly detection. The dataset consists of raw network packets captured using Wireshark, extracted features, and labeled data, with 49 attributes categorized into various types. Table 1 lists these data fields and their descriptions. This data set consist of

Feature Categories:

- 1) **Flow Features:** Basic features derived from network flows. Examples: Duration, protocol type, service, source and destination bytes.
- 2) **Basic Features:** Features related to TCP/IP connections. Examples: Source and destination IP addresses, port numbers, and timestamps.
- 3) **Content Features:** Information extracted from the packet payload. Examples: Number of failed login attempts, and shell prompts.
- 4) **Time-based Features:** Information based on time-based patterns. Examples: Number of connections to the same host within a certain time frame.
- 5) **Additional Generated Features:** Features created by analyzing traffic patterns. Examples: Number of packets, number of bytes, and average packet size.

A. DATA PREPROCESSING

The UNSW-NB15 dataset underwent thorough preprocessing to enhance its quality and usability for training machine learning models. The process involved importing the datasets into Pandas DataFrames, conducting exploratory data analysis to understand the attack category distribution, addressing class imbalances, removing irrelevant columns, and ensuring no missing values. Categorical features were transformed into a numerical format using the one-hot encoding method, and both the training and testing datasets were merged for consistent preprocessing. Feature normalization was applied through min-max scaling to ensure equal contributions of all features during model training. To address class imbalances, a Feedforward Neural Network (FNN) was used to generate synthetic samples for minority classes, resulting in a balanced dataset. The final step involved separating the class labels

TABLE 1. Examples of Data Fields and Their Descriptions in the UNSW-NB15 Dataset

Features	Description	Features	Description
srcip	Source IP address	sttl	Source to dest. time to live value
sport	Source port number	dttl	Dest. to source time to live value
dstip	Destination (Dest.) IP address	sloss	Source packets retransmitted or dropped
dsport	Destination port number	dloss	Dest. packets retransmitted or dropped
proto	Protocol type (e.g., TCP, UDP)	service	http, ftp, smtp, ssh, dns, ftp-data ,irc
state	State of the connection (e.g., FIN, SYN)	Sload	Source bits per second
dur	Duration of the connection	Dload	Dest. bits per second
sbytes	Source-to-destination bytes	Spkts	Source to destination packet count
dbytes	Dest.-to-source bytes	Dpkts	Dest. to source packet count
label	Attack type or normal	swin	Source TCP window advertisement value

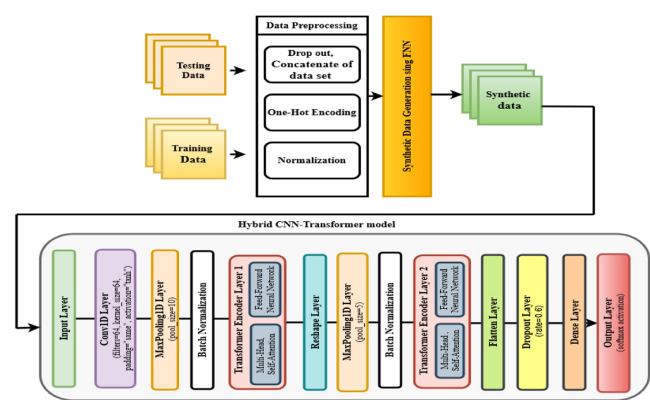


FIGURE 4. Hybrid CNN - transformer model.

from the features and preparing the dataset for machine learning tasks. These preprocessing steps transformed the original UNSW-NB15 dataset into a structured, balanced, and normalized format, thereby improving the learning capabilities and prediction accuracy of the model.

B. IMPLEMENTATION OF THE PROPOSED MODEL

Various machine and deep learning techniques have been employed to create effective attack classification systems. We propose a hybrid Convolutional Neural Network (CNN) transformer model, as depicted in Fig. 4. This model leverages the strengths of both CNNs and transformers to enhance classification accuracy.

The proposed model integrates an FNN for synthetic data generation. These synthetic data, produced by the FNN, augment the training set and improve the ability of the model to generalize and accurately classify attacks. Once generated, the synthetic data are passed to the hybrid CNN transformer model for classification. The CNN component effectively captured the spatial hierarchies in the data, whereas the transformer component captured long-range dependencies, thereby boosting the overall performance of the model. This hybrid model was implemented using the Jupyter Notebook platform, which provides an interactive environment for the coding, visualization, and testing of the model.

The effectiveness of the proposed model was evaluated by comparing it with other models, including artificial neural networks (ANN), Gradient Boosting Classifier (GBC), and Random Forest Classifier (RFC). Each of these models represents a different approach to attack classification and provides a comprehensive benchmark for the proposed model. The results demonstrate that the proposed hybrid CNN-transformer model outperforms the other models, achieving the highest accuracy rate of 96.8%. This indicates that the integration of the CNN and transformer architectures, along with the use of synthetic data generation, significantly enhances the ability of the model to accurately classify attacks, making it a robust tool for cybersecurity applications.

C. TRAINING OF MODELS AND EVALUATION OF SYSTEMS

The process of model training involves utilizing 5-fold cross-validation with stratified KFold to ensure a balanced representation of classes. SMOTE was employed to address the class imbalance. Each training and validation fold included compiling and fitting of the model using the Adam optimizer and categorical cross-entropy loss. The accuracy and loss metrics were monitored throughout the epochs. After training, the performance of the model was evaluated using the out-of-sample data for each fold. This evaluation includes computing metrics such as accuracy and confusion matrices to assess the effectiveness of classification across different attack categories. In addition, ROC curves were constructed to graphically examine the model’s multiple-class classification performance in terms of true-positive and false-positive rates, thereby providing a comprehensive understanding of its predictive capabilities.

V. DYNAMIC ENCRYPTION ALGORITHM SELECTION BASED ON PREDICTED ATTACKS

After predicting the likelihood of an attack using UNSW-NB1, an optimal encryption algorithm based on anticipated attack types was dynamically selected. Refer to Fig. 5(a) for details on the encryption algorithms employed and their respective resistance to the predicted attack scenarios.

The process commences with the utilization of a trained Feedforward Neural Network (FNN) and scaled input features

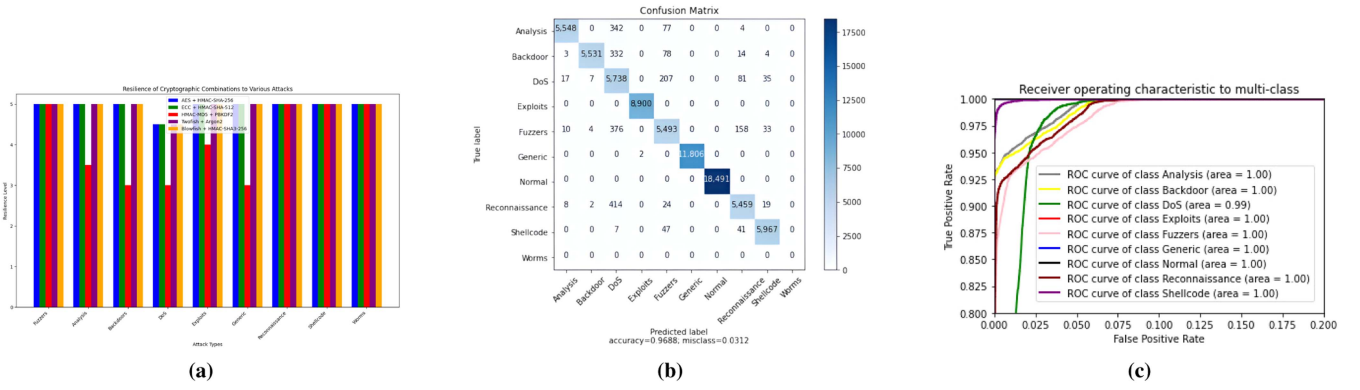


FIGURE 5. (a) Resilience of cryptographic combinations to various attacks, (b) confusion matrix, and (c) ROC curve for the proposed model.

to predict attack types. Subsequently, the predicted attack type was used to determine a suitable encryption algorithm. This selection is based on a predefined mapping that associates each attack type with specific algorithms, such as AES + HMAC (SHA 256), ECC + HMAC (SHA512), HMAC-MD5 + PBKDF2, Twofish + Argon2, and Blowfish + HMAC SHA3-256. Data encryption was implemented accordingly, and the encrypted credentials were updated in the database using SQL queries. This automated workflow guarantees the security of sensitive information against anticipated threats, and dynamically adjusts encryption methods based on real-time threat predictions.

VI. RESULT AND DISCUSSION

It is crucial to compute a range of evaluation metrics, including accuracy, precision, recall, and F1-score, to evaluate and compare the performance of the machine learning model utilized in this research. The effectiveness of the models can be evaluated by analyzing these metrics based on specific criteria. These metrics provide important information regarding the precision and reliability of the models, and further analysis can be conducted based on these calculations.

- **Accuracy:** Accuracy, commonly known as the true positive rate, assesses the overall accuracy of a model's predictions. This value was determined using the following formula:

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)}$$

- **Precision:** Precision indicates the proportion of accurate positive predictions. This was computed using the following equation:

$$Precision = \frac{(TP)}{(TP + FP)}$$

- **Recall:** Recall, also known as the amount of sensitivity or true-positive rate, is the percentage of genuine positive cases recognized properly by the model. The formula used to calculate the recall is as follows:

$$Recall = \frac{(TP)}{(TP + FN)}$$

- **F1-score:** The F1-score is a balanced statistic that includes precision and recall using a weighted average. This computation can be performed using the following equation:

$$F1 - score = 2 * \frac{(Precision * Recall)}{(Precision + Recall)}$$

By computing these metrics, we gained a comprehensive understanding of the model's effectiveness, encompassing accuracy, precision, recall, and the overall balance between precision and recall, as represented by the F1-score. In our study, we utilized various machine learning algorithms. The confusion matrix for the proposed model is shown in Fig. 5(b), which shows the obtained performance metrics. the detailed outcomes are presented in Table 2 .


According to these findings, it is clear that the proposed model exhibits higher accuracy in attack classification. The ROC curve is shown in Fig. 5(c). This superior performance makes the FNN model an ideal choice for our study, which focuses on dynamically adapting encryption algorithms in response to the predicted attacks. By leveraging the high classification accuracy of the Hybrid CNN - Transformer model, we aim to enhance the security of our system by selecting the most appropriate encryption algorithm based on the specific type of attack detected. This dynamic approach not only improves the robustness of our security mechanisms but also ensures optimal protection against a wide range of potential threats. The integration of the proposed model with our adaptive encryption strategy represents a significant advancement in secure authentication in cloud environments. The findings of the feature extraction, biometric key generation, and dual encryption algorithm results based on passwords, conditional attributes, and fingerprint data credentials are outlined below.

Feature extraction: The first step involves identifying crucial features from the user's fingerprint data. To ensure the precise collection and depiction of these biometric attributes for evaluation, sophisticated techniques were employed. The fingerprint image used for the sample output was sourced from the 'Fingerprint-Feature-Extraction' repository by Deshmukh [35] and the findings are presented in Table 3.

TABLE 2. Performance Metrics of Different Models

Model	Accuracy	Precision	Recall	F1-Score	Training Time	Prediction Time
GBC	0.75	0.54	0.64	0.54	22,927 sec	9 sec
RFC	0.76	0.83	0.75	0.77	22,900 sec	9 sec
ANN	0.94	0.94	0.93	0.93	22,800 sec	7 sec
Proposed Model	0.97	0.97	0.96	0.96	23,100 sec	10 sec

TABLE 3. Fingerprint Feature Extraction and Minutiae Points

Fingerprint Image	All Minutiae Points	Selected Minutiae Points
	Ridge Ending 1.(40,313), 2.(55,275), 3.(65,208), 4.(68,333), 5.(72,233), ... 78.(671,367), 79.(676,216), 80.(678,312), 81.(679,325), Bifurcation 82.(52,276), 83.(60,209), 84.(70,328), 85.(132,411), 86.(140,194), ... 278.(590,260), 279.(639,308), 280.(639,315), 281.(670,252), 282.(679,301)	1. (544, 425) - Ridge Ending 2. (169, 408) - Ridge Ending 3. (208, 169) - Bifurcation 4. (189, 201) - Bifurcation 5. (180, 229) - Bifurcation 6. (643, 392) - Ridge Ending 7. (535, 241) - Ridge Ending 8. (639, 315) - Bifurcation 9. (476, 275) - Ridge Ending 10. (312, 208) - Bifurcation

Biometric Key Generation: By implementing the extracted fingerprint features, a strong mechanism for generating biometric keys was developed. This guarantees the creation of distinct and secure cryptographic keys directly from the fingerprint information of the user. By incorporating biometric identifiers into the key generation procedure, the overall security framework is fortified, thereby improving the protection against unauthorized access and data breaches. The extracted master key is provided below, from which two keys, K_1 and K_2 , are derived.

Master Key- be485bd3c02003812274fd2fb6c9d59787630387846891dbf2e677e9e0da1b1a9abc55535ebf8b42602552cca942d9243289450f12f846c21b167a8bfb3a7548
Key 1- be485bd3c02003812274fd2fb6c9d59787630387846891dbf2e677e9e0da1b1a
Key 2- 9abc55535ebf8b42602552cca942d9243289450f12f846c21b167a8bfb3a7548

The implementation and adoption of multifactor authentication (MFA) anticipates several significant threats. These prominent threats directly impact the scope of our current research on MFA threat modeling. Below, we outline these key threats and describe how our proposed framework addresses and mitigates them.

- 1) **Biometric Spoofing:** Biometric verification methods may be sensitive spoofing attacks, where malicious actors create counterfeit biometric information to deceive the authentication system. Our framework mitigates this risk by combining biometric authentication with passwords and conditional attributes, thereby providing additional security layers against such attacks.
- 2) **Credential Stuffing:** Hackers may exploit stolen MFA credentials to gain unauthorized access to other accounts owned by the same user. Using biometric information, which is inherently more secure and cannot

- be easily replicated, our framework effectively prevents credential-stuffing attacks.
- 3) **Denial of Service (DoS) Attacks:** Hackers can carry out DoS attacks on the authentication system and stop registered users from accessing account information. Although the use of biometric data for cryptographic keys does not directly prevent DoS attacks, it complicates automated attempts, thereby enhancing security. Further research is necessary to fully address this issue.
- 4) **Insider Threats:** Employees or freelancers with access to highly confidential systems may use their privileges to circumvent or obtain credentials for MFA. Our framework reduces the risk of insider threats by generating unique cryptographic keys through biometric authentication, thereby minimizing the possibility of key-sharing. Dual encryption further bolsters security.
- 5) **Malware:** Infected devices may be targeted by malware, such as keyloggers or screen capture tools, to steal MFA credentials. Our model enhances data security by incorporating biometric authentication, dual encryption, passwords, and conditional attributes, thereby reducing the risks associated with compromised biometric data.
- 6) **Man-in-the-middle Attacks:** Unauthorized parties can monitor the communication between individuals, the verification system, and steal MFA credentials. Our framework adapts to potential threats by employing varies encryption algorithms, ensuring the creation of distinct and secure cryptographic keys through biometric characteristics.
- 7) **Social Engineering:** Attackers may employ phishing or other social engineering techniques to trick users into disclosing their MFA information. By integrating biometric authentication with passwords and conditional

TABLE 4. Comparison of Authentication Methods and Their Risk to Different Attacks With the Proposed Method

Ref	Authentication Approach	Brute-Force Attack	Guess Attack	Phishing Attack	Spoofing Attack	Impersonation Attack
[20]	Face Recognition	✗	✗	✗	✓	✗
[15]	Fingerprint Scanner	✗	✗	✗	✓	✗
[36]	OTPs	✗	✗	✓	✗	✓
[37]	Password/PIN	✓	✓	✓	✗	✓
[38]	Smart Cards	✗	✗	✗	✓	✓
[39]	Voice Recognition	✗	✗	✗	✓	✗
Proposed Work	Fingerprint + Password + Conditional Attributes	✗	✗	✗	✗	✗

attributes, our framework enhances security against social engineering attacks.

By addressing these threats using our comprehensive framework, we significantly enhance the security and reliability of MFA systems. Table 4 compares our research with various existing studies on secure authentication using different approaches to evaluate their resistance to different types of attacks.

VII. CONCLUSION

Finally, this study provides a complete method for improving cloud security using a revolutionary multi-factor authentication system and adaptive cryptography framework. The system solves significant weaknesses in cloud computing environments by merging passwords, conditional attributes, fingerprint authentication mechanisms and machine learning-driven dynamic encryption algorithm updates. The dual encryption technique enhances data safety by utilizing combinations such as AES + HMAC (SHA-256) and ECC + HMAC (SHA-512), which are dynamically customized based on the discovered attack type. Furthermore, the use of a hybrid CNN-transformer based model for attack prediction resulted in good accuracy, precision, recall, and F1-Score values of 96.8% and 97.2%, respectively. 96.8% and 96.9% outperformed the standard models. This predictive capacity enables the system to preemptively alter security measures, assuring strong defense against brute force, guesses, phishing, spoofing, and impersonation assaults.

Implementing this advanced approach allows enterprises to improve the privacy and integrity of the sensitive information stored in cloud settings. The framework not only meets strict security standards but also includes adaptive capabilities to effectively combat evolving threats. This study demonstrates the efficacy of combining multi-factor authentication and adaptive cryptography, opening the way for resilient and secure cloud computing systems in the face of growing cybersecurity threats. Future improvements could leverage real-time datasets for more accurate attack predictions. Deploying this framework in live cloud environments enhances security and readiness against evolving cyber threats. By employing behavioral analysis techniques, abnormal usage patterns of the skip mechanism can be detected and mitigated, thereby preventing potential misuse.

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](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/10.3390/cryptography2010001).
- [6] S. Sudha and S. S. Manikandasan, "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](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/10.4018/IJCAC.2020040104).
- [19] K. M. Prabha and P. V. Saraswathi, "Suppressed K-anonymity multi-factor 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](https://doi.org/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/NCCCC49330.2021.9428806](https://doi.org/10.1109/NCCCC49330.2021.9428806).
- [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](https://doi.org/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/IJC-SNS.2022.22.9.62](https://doi.org/10.22937/IJC-SNS.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](https://doi.org/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](https://doi.org/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](https://doi.org/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 SHAX-ECC," *Multimedia Tools Appl.*, vol. 24, pp. 68363–68391, 2024, doi: [10.1007/s11042-024-18147-6](https://doi.org/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](https://doi.org/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](https://doi.org/10.37934/araset.44.1.225238).
- [29] I. Aljamal, A. Tekoğlu, K. Bekiroglu, and S. Sengupta, "Hybrid intrusion 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](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/10.61916/prmn.2023.v0101.004).
- [34] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. Mil. Commun. Inf. Syst. Conf.*, 2015, pp. 1–6, doi: [10.1109/Mil-CIS.2015.7348942](https://doi.org/10.1109/Mil-CIS.2015.7348942).
- [35] U. Deshmukh, "Fingerprint-feature-extraction," Accessed: Jun. 10, 2024. [Online]. Available: <https://github.com/Utkarsh-Deshmukh/Fingerprint-Feature-Extraction>
- [36] H. Kim, J. Han, C. Park, and O. Yi, "Analysis of vulnerabilities that can occur when generating one-time password," *Appl. Sci.*, vol. 10, no. 8, 2020, Art. no. 2961, doi: [10.3390/app10082961](https://doi.org/10.3390/app10082961).
- [37] R. V. Adiraju, K. K. Masanipalli, T. D. Reddy, R. Pedapalli, S. Chundru, and A. K. Panigrahy, "An extensive survey on finger and palm vein recognition system," *Mater. Today: Proc.*, vol. 45, pp. 1804–1808, 2021, doi: [10.1016/j.matpr.2020.08.742](https://doi.org/10.1016/j.matpr.2020.08.742).
- [38] S. Bobba and V. Paruchuri, "Single sign-on using contactless smart cards and fingerprint authentication," in *Proc. 16th Int. Adv. Conf. Broad-Band Wireless Comput., Commun. Appl.*, 2022, pp. 158–166, doi: [10.1007/978-3-030-90072-4_16](https://doi.org/10.1007/978-3-030-90072-4_16).
- [39] S. Debnath, K. Ramalakshmi, and M. Senbagavalli, "Multi-modal authentication system based on audio-visual data: A review," in *Proc. Int. Conf. Advance. Technol.*, 2022, pp. 1–5, doi: [10.1109/ICONAT53423.2022.9725889](https://doi.org/10.1109/ICONAT53423.2022.9725889).



K. SASIKUMAR received the Bachelor of Technology degree in computer science and engineering from Dr. M.G.R University, Chennai, Tamil Nadu, India, in 2010, and the Master of Engineering degree in computer science and engineering in 2013 from St. Peter's University, Chennai, where he is currently working toward the Ph.D. degree with the Vellore Institute of Technology, Vellore, Tamil Nadu. His research interests include cryptography, network security, machine learning, and deep learning and focuses on the construction of cryptography algorithms tailored for limited contexts as well as the incorporation of machine learning approaches into security.



SIVAKUMAR NAGARAJAN received the B.E. degree in computer science and engineering from the University of Madras, Chennai, Tamil Nadu, India, the M.Tech. degree in computer science and engineering from Dr. M.G.R. Educational and Research Institute, Chennai, the M.B.A. degree in human resource management from Alagappa University, Karaikudi, Tamil Nadu, the LL.B. and LL.M. degrees from Sri Venkateswara University, Tirupati, Andhra Pradesh, India, the M.Sc. degree in cyber forensics and information security from the University of Madras, and the Ph.D. degree in computer science and engineering from Anna University, Chennai. He is currently an Associate Professor with the School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu. His research interests include image processing, artificial intelligence and machine learning, cyber forensics and cyber security, and wireless sensor networks.