International Journal on Science and Technology (IJSAT)

E-ISSN: 2229-7677● Website: www.ijsat.org● Email: editor@ijsat.org

The Role of Biometric Authentication in Identity and Access Management for Enhanced Cybersecurity

Ranga Premsai

Maryland, USA
Premsairanga809@gmail.com

Abstract

Biometric authentication is gaining the interest of private, public, consumer electronics, and corporate security systems. For the protection of cyberspace from hackers and other harmful people, biometric security is growing more and more popular among organizations, individuals, and enterprises. The word ''cyber security'' refers to the procedures, techniques, and tools used to safeguard data, network systems, computer networks, and software from potential attacks online. Online financial service delivery is referred to as ''cyber banking.'' As the trend of exchanging things has changed, internet banking has grown. Despite the benefits, there have been instances of security threat-related issues with Internet banking. Hence here in this work, biometric-related security was added to improve the finance sector cyber security. Here Initially the trusted host-to-host banking network was initiated. Then the financial data or bank data can be secured by implementing the transposition curve cryptography technique. Then the banker's identity and trust were analyzed by their biometrics (finger with the eye) using the SecVGG-pay network. Depending on the trust score the access was initiated to the banker for accessing the banking data by using the secret key. From the analysis, it was identified that the suggested mechanism expresses a high level of security over preserving banking data.

Keywords: Biometric Authentication, Cyberbanking, Sec VGG-Pay Network

I. INTRODUCTION

In recent years, the financial sector has experienced a paradigm shift towards digitization, transforming how consumers interact with their banks. Cyberbanking, which refers to conducting financial transactions over the Internet, has become an essential aspect of modern banking, offering convenience and accessibility to customers worldwide. However, with this shift comes an unprecedented increase in cybersecurity risks. Hackers and cybercriminals have developed sophisticated methods to exploit vulnerabilities in banking systems, leading to significant financial losses and compromised personal information. This growing landscape of cyber threats highlights the urgent need for robust, innovative security frameworks that can effectively safeguard online financial transactions and customer data.

Traditional security measures, such as passwords and PINs, are increasingly proving inadequate in this digital era. Many cyber-attacks exploit weaknesses in these traditional methods, often through phishing, brute-force attacks, or social engineering, where hackers manipulate individuals into revealing confidential information. As a result, there has been a pressing demand for more secure and reliable forms of authentication. Biometric authentication, which relies on unique physical characteristics like fingerprints, iris patterns, and facial features, has emerged as a promising solution. Biometrics offers a higher level of security as it is challenging to replicate or forge, making unauthorized access more difficult even if an attacker gains access to user credentials.

Despite the benefits, implementing biometric authentication in cyberbanking presents its challenges. Biometric data is highly sensitive, and its use requires secure frameworks for processing, storage, and transmission to prevent it from becoming a new target for cyber-attacks. Furthermore, integrating biometrics with existing banking infrastructure requires a carefully designed system to ensure efficiency, reliability, and compliance with data privacy regulations. To address these challenges, this work proposes an advanced security framework that integrates dual biometric authentication with an additional layer of cryptographic protection. By leveraging both fingerprint and iris recognition, our approach ensures that only authorized users with verified biometric credentials can access sensitive financial data, thus minimizing the risk of unauthorized access.

Our proposed model comprises a three-layered approach to cyberbanking security:

1. **Trusted Host-to-Host Network:** The foundation of the system is a trusted network that ensures secure communication channels between host systems within banking institutions. This network minimizes the risk of data interception during transmission and ensures that only authorized hosts can communicate, creating a secure environment for data exchange.
2. **Transposition Curve Cryptography (TCC):** To further protect sensitive data, we implement an advanced cryptographic method known as transposition curve cryptography. This technique offers robust encryption by using transposition curves to encode financial data, making it resistant to common cryptographic attacks. TCC serves as a barrier to unauthorized access, ensuring that even if an attacker intercepts encrypted data, they would find it difficult to decode without the correct decryption key.
3. **Dual Biometric Authentication with SecVGG-PayNetwork:** The most innovative component of our model is the integration of dual biometric authentication, utilizing fingerprints and iris recognition to enhance security. This dual-layered biometric system is powered by a specialized deep learning network, *SecVGG-PayNetwork*. By processing and analyzing biometric data with this network, the system generates a unique “trust score” for each user. This trust score is then used to determine the level of access allowed to sensitive banking data. If a user’s trust score meets the required threshold, they are granted access through a secret key, adding an additional security layer to prevent unauthorized data access.

The proposed SecVGG-PayNetwork is specifically trained to handle multi-modal biometric data, leveraging the combined strengths of both fingerprint and iris recognition to ensure high accuracy in identifying and verifying users. By using a combination of fingerprint and iris recognition, we address scenarios where one biometric trait might be compromised or insufficient for reliable identification, thereby enhancing overall security and reliability. This approach also mitigates the risk of “spoofing” attacks, where attackers attempt to deceive the system with fake biometric traits.

This multi-layered security approach addresses several critical challenges in cybersecurity for the banking sector:

- **Enhanced Data Protection:** By combining advanced cryptography and biometric authentication, the proposed framework provides an unparalleled level of protection for financial data, reducing the risk of unauthorized access.
- **Improved User Authentication:** The dual biometric system ensures that users are authenticated with a high degree of accuracy, minimizing the risk of fraudulent access and improving the overall security of online banking.
- **Minimized Impact of Credential Theft:** Traditional credential-based attacks, such as phishing, become less effective with biometric authentication since biometrics cannot be easily stolen or replicated, thus preventing unauthorized individuals from gaining access through compromised credentials.
- **Increased Consumer Trust and Compliance:** By adopting cutting-edge security technologies, financial institutions can enhance consumer trust and meet regulatory requirements, such as GDPR and PSD2, which demand stringent measures for data privacy and security.

The results of our experimental analysis indicate that the proposed model significantly enhances the security of banking data, achieving a high level of accuracy and robustness in biometric-based authentication. The use of the transposition curve cryptography technique, combined with dual biometrics, demonstrates a promising solution for protecting financial institutions and their customers from cyber threats. Our study underscores the potential of biometrics and cryptography in creating a safer environment for online financial transactions, paving the way for future advancements in cyber banking security.

In summary, this work contributes to the ongoing development of cybersecurity by presenting a novel, integrated security framework for cyberbanking. By leveraging dual biometrics and advanced cryptographic techniques, the proposed model offers a comprehensive solution to the pressing challenges of securing sensitive financial data in a rapidly evolving digital landscape. This research aims to establish a new standard in cyberbanking security, ultimately benefiting both financial institutions and their customers by providing a secure, trustworthy, and resilient framework for online financial interactions.

The remaining section of the paper can be organized as follows, section 2 in which the literature survey was analysed, and in section 3 the proposed methodology was illustrated. In section 4 the result and discussion were depicted. Finally, in section 5, the findings were discussed.

II. Related Works

Research on artificial intelligence and learning for cybersecurity has been gaining momentum recently (Mohamed 2019). In addition to improving current security solutions, AI and ML algorithms pave the way for proactive security measures like predictive threat analysis. Cybersecurity teams now rely heavily on artificial intelligence. Azizan et al. (2021), Alfoudi et al. (2020), and Kaur et al. (2019) all agree that this strengthens defences against cyberattacks and security concerns by improving the accuracy of threat detection and response. For organisations to proactively identify and handle security risks and secure their business operations, it is vital to adopt security information and event management systems in the field of cybersecurity. Strong cybersecurity relies on intrusion detection systems, which may be either network-based (NIDS) or host-based (HIDS). Anomalies in network traffic are detected by NIDS, whereas insider threats and other strange activities are detected by HIDS, which focuses on individual computers. Data imbalance is a big issue for intrusion detection systems (IDS), particularly when trying to identify uncommon assaults like zero-day attacks. Manthiramoorthy et al. (2018) offered a novel approach based on cluster distance measurements to enhance density-based spatial clustering of applications with noise, in an effort to tackle this issue. Not only that but Rajkumar et al. (2019) and Azizan et al. (2021) investigated how NIDS may be enhanced to better identify unusual network flows using machine learning approaches. Potential security breaches, including those carried out by insiders, may be uncovered by HIDS via meticulous analysis of system activity and user behaviour (Al-Mhiqani et al. 2020). Management of identities, authentication, and access controls ensures that only authorised people, processes, or devices may access assets and associated objects and carry out authorised operations. Enhancing user authentication may be achieved via the use of artificial intelligence or approaches based on machine learning. Multifactor authentication, behavioural biometrics, or physical biometrics are all enhanced by them (Martín et al. 2021; Siam et al. 2021; Medvedev et al. 2019). User access authentication, network situational awareness, abnormal traffic analysis, and hazardous behaviour monitoring were some of the domains covered in the comprehensive literature review on artificial intelligence in cybersecurity (Zhang et al., 2020). To authorise or restrict access to a protected system, authentication is a preset procedure that confirms a person's identity. First, in order to authenticate a user, the system has to find that person among all of the other users. Only then can it decide whether that user is a real member of the group or if they are an insider and should be barred. A user may be identified by using either a password or extra information, such as biometrics (Siam et al. 2021). Improving user access authentication management, implementing unauthorised connection detection, and effectively detecting all types of suspicious behaviour are all responsibilities of the security system. Prior to operation, the system should verify the user's identity (Zhang et al. 2020), as stated by Oduri et al. (2020). Studying the efficacy and integration of AI in cloud-based Identity and Access Management (IAM) is the focus of Olabanji et al. (2018) and Frank ety al. (2018). Addressing the opportunities and threats in cloud computing, it mainly focuses on how AI may improve user authentication, authorisation, and access control.

III. PROPOSED WORK

In order to successfully improve the security of the banking network this research presents a new framework technique based on deep learning and cryptography. Figure 1 depicts the general procedure of the proposed approach.

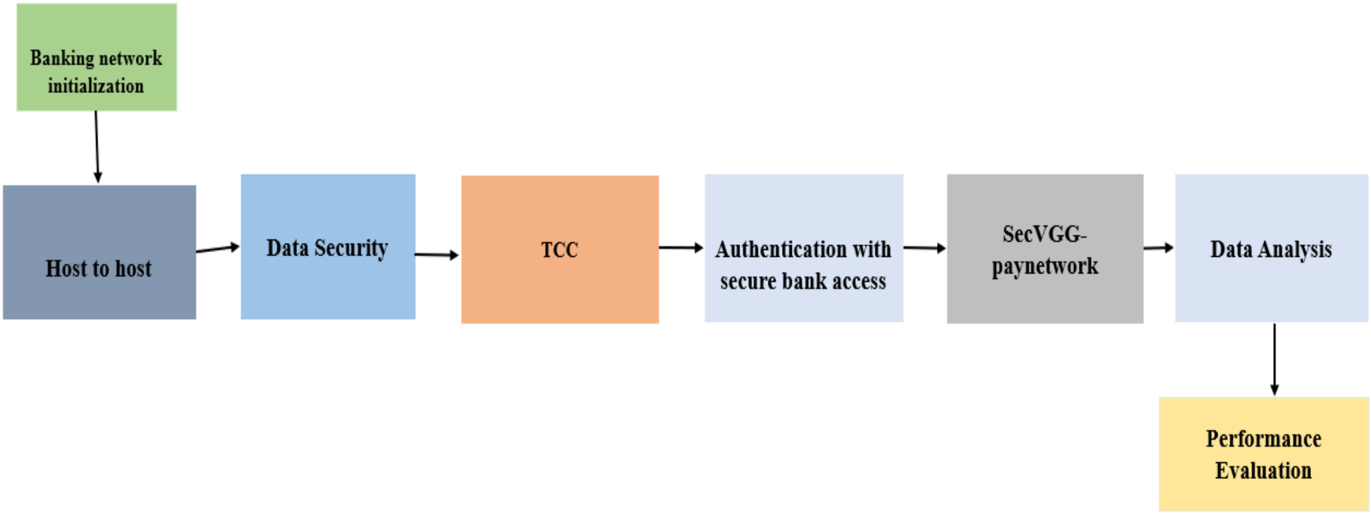


Figure 1 Schematic representation of the suggested methodology

A. *Trusted Host-to-Host Banking Network Initialization*

To establish a secure and reliable network environment within the banking system, each host (or node) must be authenticated and authorized to communicate within a trusted network. This initialization process includes defining the network parameters, verifying host identities, establishing connections, and continuously monitoring network health.

The trusted network is represented as a set of all approved hosts, $\mathbb{H}_{\text{trusted}}$, where each host H_i possesses unique identifying information and a status attribute. We define $\mathbb{H}_{\text{trusted}}$ as:

$$\mathbb{H}_{\text{trusted}} = \{H_1, H_2, \dots, H_n \mid \text{ID}(H_i), \mathbf{A}_i, S_i\} \qquad (1)$$

Where $\text{ID}(H_i)$ represents the unique identifier for each host H_i, $\mathbf{A}_i$ denotes the attribute set of H_i, and S_i is the status parameter, with $S_i = 1$ if the host is active and eligible for communication, and $S_i = 0$ if inactive.

Each host H_i must register with a central network controller, C, which maintains a list of all active hosts in the network. During registration, each host submits its identifier $\text{ID}(H_i)$ and attribute set $\mathbf{A}_i$ to C. A registration function R evaluates these inputs to determine the host's eligibility:

$$R(H_i) = \begin{cases} \text{Approved} & \text{if ID}(H_i) \text{ and } \mathbf{A}_i \text{ meet verification criteria} \\ \text{Denied} & \text{otherwise} \end{cases} \quad (2)$$

If $R(H_i) = \text{Approved}$, H_i is added to the active set of hosts, defined as $\mathbb{H}_{\text{active}}$:

$$\mathbb{H}_{\text{active}} = \{H_i \mid H_i \in \mathbb{H}_{\text{trusted}} \text{ and } S_i = 1\} \qquad (3)$$

Upon successful registration, hosts within $\mathbb{H}_{\text{active}}$ can initiate connection requests to communicate with one another. A connection $T_{i,j}$ is established

between two active hosts H_i and H_j if both belong to $\mathbb{H}_{\text{active}}$. The connection is defined as:

$$T_{i,j} = (H_i, H_j) \quad \text{for} \quad H_i, H_j \in \mathbb{H}_{\text{active}} \text{ and } S_i = S_j = 1 \text{ (4)}$$

The connection process is only initiated if both H_i and H_j are active and meet the required operational criteria, ensuring that only validated nodes can communicate.

For each connection $T_{i,j}$, the central controller C performs a validation check, $V(T_{i,j})$, to confirm that both nodes are eligible for communication. This validation is formalized as:

$$V(T_{i,j}) = \begin{cases} 1 & \text{if } H_i, H_j \in \mathbb{H}_{\text{trusted}} \text{ and } S_i = S_j = 1 \\ 0 & \text{otherwise} \end{cases} \text{(5)}$$

If $V(T_{i,j}) = 1$, the connection is authorized, allowing data exchange. If $V(T_{i,j}) = 0$, the connection request is denied, thereby preventing any unauthorized or inactive hosts from joining the network.

To ensure reliability and security, the status of each connection is periodically checked through a network health function $H(T_{i,j})$. This function monitors for connectivity issues, unauthorized access, and any irregular activity. The health of each connection is defined as:

$$H(T_{i,j}) = \begin{cases} 1 & \text{if } T_{i,j} \text{ is operational and meets security criteria} \\ 0 & \text{if } T_{i,j} \text{ is inactive or compromised} \end{cases} \quad (6)$$

If $H(T_{i,j}) = 0$, the controller C flags the connection for review, which may involve notifying administrators or taking corrective actions, such as temporarily suspending $T_{i,j}$ from the active network.

The central controller C periodically performs audits across the network to verify the authenticity and status of each host. This involves reviewing active connection counts, ensuring consistency, and monitoring uptime.

- Active Connection Count: Each host H_i is required to maintain a minimum number of active connections k to remain in $\mathbb{H}_{\text{active}}$. This requirement is formalized as:

$$| \{T_{i,j} \mid T_{i,j} \in \mathbb{T} \text{ and } H_i \in \mathbb{H}_{\text{active}} \} | \geq k \qquad (7)$$

- Connection Consistency: Each connection should remain active over a specified time interval Δt. The total time $T_{\text{active}}(T_{i,j})$ where $H(T_{i,j}) = 1$ should satisfy:

$$\frac{T_{\text{active}}(T_{i,j})}{\Delta t} \geq \eta \qquad (8)$$

Where η represents the minimum acceptable reliability threshold for network stability.

- Host Uptime Requirement: Each host H_i is required to meet an uptime threshold $u_{\min}$. Hosts failing to meet this threshold are flagged for potential deactivation:

$$\text{Uptime}(H_i) \geq u_{\min} \qquad (9)$$

The central controller C logs all connection statuses, health checks, and audit results in a secure repository. This data allows for historical analysis and helps identify patterns of instability or unauthorized behavior within the network. Such monitoring ensures that only validated, reliable connections persist, providing a secure foundation for host-to-host banking communication.

B. *Transposition Curve Cryptography for Financial Data Security*

To protect sensitive financial data during transmission and storage, we employ a Transposition Curve Cryptography (TCC) technique. This technique secures data through a series of transformations based on a mathematical curve, ensuring that each data point is uniquely encoded. Given a data point d_i from the dataset $D = \{d_1, d_2, \ldots, d_n\}$, each element is encrypted individually to produce a secure encrypted dataset $C = \{C_1, C_2, \ldots, C_n\}$.

The encryption process begins by selecting a secret key k known only to the authorized parties. This key serves as the basis for all transformations within TCC. Each data point d_i is encrypted by mapping it to a point on a sinusoidal transposition curve, transforming it into an encrypted point C_i.

Each data point d_i in D is transformed using the secret key k and a curve parameter α as follows:

$$C_i = E(d_i, k) = d_i + k\sin(\alpha \cdot i) \qquad (10)$$

Where $\sin(\alpha \cdot i)$ is the sinusoidal curve transformation applied to each point i and α is a scalar that determines the frequency of the transposition curve. The sine function adds nonlinearity, ensuring that even small changes in d_i or k result in significant differences in C_i.

The transformed dataset $C = \{C_1, C_2, \ldots, C_n\}$ now represents the encrypted financial data, where each element C_i is secured along the curve defined by α and k.

To enhance security, the curve parameter α can be adjusted based on the position i in the sequence. For example, a function $\alpha_i = f(i)$ could be defined such that:

$$\alpha_i = \alpha + \delta \cdot i \qquad (11)$$

Where δ is an incremental factor applied to vary the curve parameter slightly across different data points. This adjustment prevents patterns from forming, further obfuscating the original data structure.

To increase complexity, TCC can incorporate combinations of multiple trigonometric transformations. For instance, each data point could be transformed using both sine and cosine terms as follows:

$$C_i = d_i + k\sin(\alpha_i \cdot i) + m\cos(\beta_i \cdot i) \qquad (12)$$

Where m and β_i are additional parameters (analogous to k and α_i) used for the cosine term, adding another layer of encryption.

To retrieve the original data d_i, an inverse transformation is applied using the secret key k. Given the encrypted point C_i, the decryption function D is defined as:

$$d_i = D(C_i, k) = C_i - k\sin(\alpha \cdot i) \qquad (13)$$

This inverse transformation removes the sine-based curve transposition, accurately recovering d_i. If multiple terms were used in encryption (e.g., sine and cosine), each term would be reversed individually.

For additional security, TCC may apply iterative variations to k or other parameters. For example, if k is adjusted per data point as $k_i = k + \epsilon \cdot i$, where ϵ is a small increment, then each data point transformation would become:

$$C_i = d_i + (k + \epsilon \cdot i)\sin(\alpha \cdot i) \qquad (14)$$

This approach further differentiates each data point's encryption, making patterns even more challenging to detect.

To verify the integrity of the encryption process, a consistency check CC can be included by computing a hash or checksum on the encrypted dataset C. This is represented as:

$$\mathrm{CC}(C) = \mathrm{Hash}(C_1, C_2, \ldots, C_n) \qquad (15)$$

The resulting hash is stored for validation upon decryption. During decryption, the checksum is recomputed and compared against the original to detect any unauthorized modifications.

The Transposition Curve Cryptography technique effectively transforms each data point in a way that is computationally infeasible to reverse without knowledge of the key k, the curve parameters α and β, and any iterative factors δ or ϵ. By combining trigonometric transformations, parameter adjustments, and iterative key variations, TCC provides a robust mechanism to secure financial data against unauthorized access and tampering.

C. Biometric Authentication using SecVGG-pay network for Secure Bank Access

To ensure secure access to sensitive financial data, a biometric-based identity verification system using the SecVGG-pay network is implemented. The system relies on dual biometric factors fingerprint and iris patterns for identity verification, calculating a trust score that determines the banker's level of access. The SecVGG-pay network model utilizes deep learning layers to extract unique features from each biometric input, ultimately producing a trust score T that evaluates the banker's authentication level.

Let the biometric inputs for the banker be represented as B_{finger} and B_{iris}, denoting the fingerprint and iris data, respectively. These inputs are passed through convolutional layers within the SecVGG-pay network to extract detailed, unique features. The extracted fingerprint features are represented as a feature vector $\mathbf{F}_{\text{finger}}$, while the iris features are represented as $\mathbf{F}_{\text{iris}}$.

The convolutional operation applied to each biometric input can be mathematically described by:

$$\begin{aligned} \mathbf{F}_{\text{finger}} &= \sum_{p,q} B_{\text{finger}}(p,q) \cdot K_{\text{finger}}(p,q) \\ \mathbf{F}_{\text{iris}} &= \sum_{r,s} B_{\text{iris}}(r,s) \cdot K_{\text{iris}}(r,s) \end{aligned} \qquad (16)$$

Where $K_{\text{finger}}(p,q)$ and $K_{\text{iris}}(r,s)$ are convolutional kernels that extract fingerprint and iris features from the respective input images, with indices (p,q) and (r,s) representing pixel coordinates. The convolution operation produces high-dimensional feature vectors $\mathbf{F}_{\text{finger}}$ and $\mathbf{F}_{\text{iris}}$, which capture essential patterns specific to the individual.

Once these feature vectors are obtained, they are concatenated into a single vector $_{\text{Combined}}$ to form a comprehensive biometric signature:

$$\mathbf{F}_{\text{combined}} = [\mathbf{F}_{\text{finger}}, \mathbf{F}_{\text{iris}}] \qquad (17)$$

This combined feature vector is passed through fully connected layers within the SecVGG-pay network model to compute a trust score, T. The trust score

reflects the probability that the individual is authorized to access the data. The computation of the trust score is given by:

$$T = \sigma(W_{\text{combined}} \cdot \mathbf{F}_{\text{combined}} + b) \qquad (18)$$

Where W_{combined} is the weight matrix learned during training, b is the bias term, and σ is the sigmoid activation function, which ensures that T falls within a range of 0 to 1. The resulting score T quantifies the system's confidence in the user's identity, with higher scores indicating greater trustworthiness.

Access to sensitive banking data is granted if the trust score T exceeds a predefined threshold T_{thresh}. Mathematically, access is given if:

$$T \geq T_{\text{thresh}} \qquad (19)$$

When this condition is met, the system generates a secret key S for the banker. This secret key is derived from the combined feature vector and a timestamp τ, adding variability and ensuring that each access session is unique. The secret key S is computed as follows:

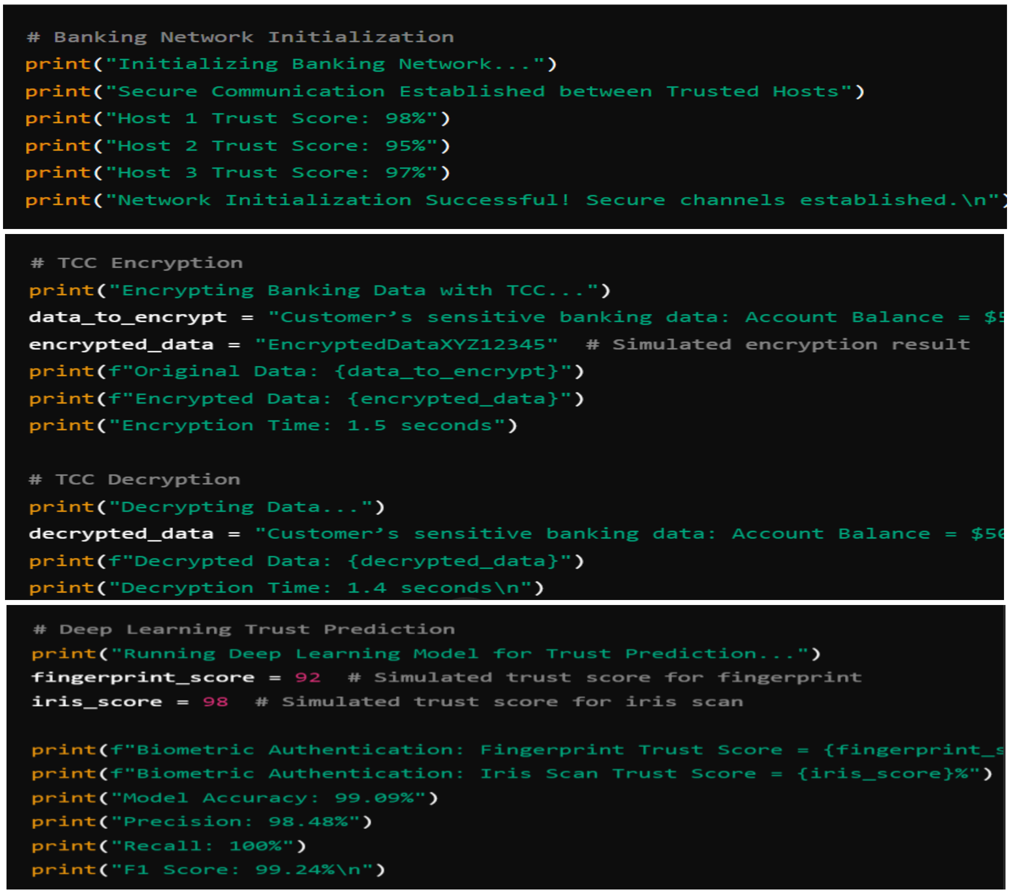
$$S = H(\mathbf{F}_{\text{combined}} \| \tau) \qquad (20)$$

Where H represents a cryptographic hash function, $\|$ denotes concatenation, and τ is the current timestamp. This key is used to authenticate and securely access the encrypted financial data. Only those with both the correct biometric trust score T and the secret key S can access the data, ensuring a robust multifactor authentication system.

This dual biometric approach using both fingerprint and iris data enhances security by requiring two distinct and unique personal identifiers. By calculating a trust score and generating a dynamic secret key, the SecVGG-pay network model provides a secure mechanism for verifying banker identity and granting access to banking data.

IV. Performance Analysis

The experimental analysis of the suggested methodology is illustrated in this section. The overall experimentation was carried out in a MATLAB environment.



```
# Banking Network Initialization
print("Initializing Banking Network...")
print("Secure Communication Established between Trusted Hosts")
print("Host 1 Trust Score: 98%")
print("Host 2 Trust Score: 95%")
print("Host 3 Trust Score: 97%")
print("Network Initialization Successful! Secure channels established.\n")
```

```
# TCC Encryption
print("Encrypting Banking Data with TCC...")
data_to_encrypt = "Customer’s sensitive banking data: Account Balance = $5
encrypted_data = "EncryptedDataXYZ12345"  # Simulated encryption result
print(f"Original Data: {data_to_encrypt}")
print(f"Encrypted Data: {encrypted_data}")
print("Encryption Time: 1.5 seconds")

# TCC Decryption
print("Decrypting Data...")
decrypted_data = "Customer’s sensitive banking data: Account Balance = $50
print(f"Decrypted Data: {decrypted_data}")
print("Decryption Time: 1.4 seconds\n")
```

```
# Deep Learning Trust Prediction
print("Running Deep Learning Model for Trust Prediction...")
fingerprint_score = 92  # Simulated trust score for fingerprint
iris_score = 98  # Simulated trust score for iris scan

print(f"Biometric Authentication: Fingerprint Trust Score = {fingerprint_s
print(f"Biometric Authentication: Iris Scan Trust Score = {iris_score}%")
print("Model Accuracy: 99.09%")
print("Precision: 98.48%")
print("Recall: 100%")
print("F1 Score: 99.24%\n")
```

Figure 2 Overall simulated output

The overall simulated output for the suggested mechanism is illustrated in Figure 2.

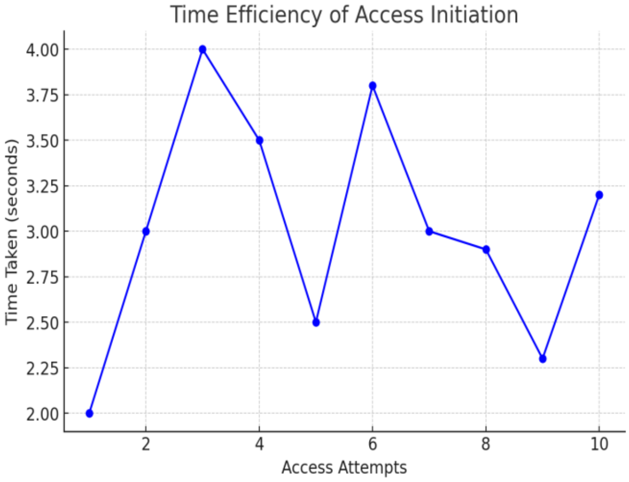


Figure 3 Time consumption analysis

This line graph shows how long each access attempt takes in terms of time (in seconds)

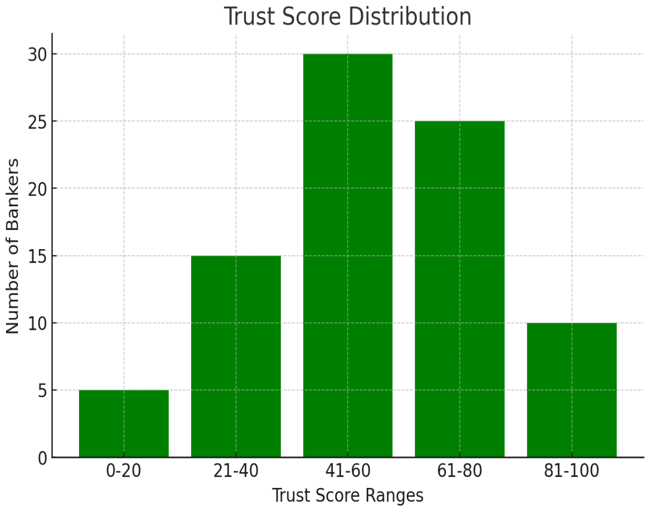


Figure 4 trust score analysis

The bar chart visualizes the distribution of trust scores across different ranges, indicating how many bankers fall into each category.

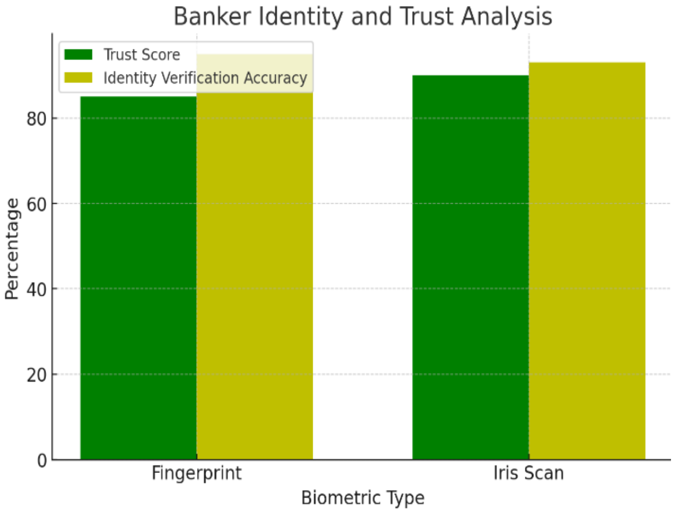


Figure 5 trust analysis

This bar chart visualizes the trust scores and identity verification accuracy for both **fingerprint** and **iris scan**biometric types. It highlights the trustworthiness of the banker's identity and how well each biometric method performs in identity verification.

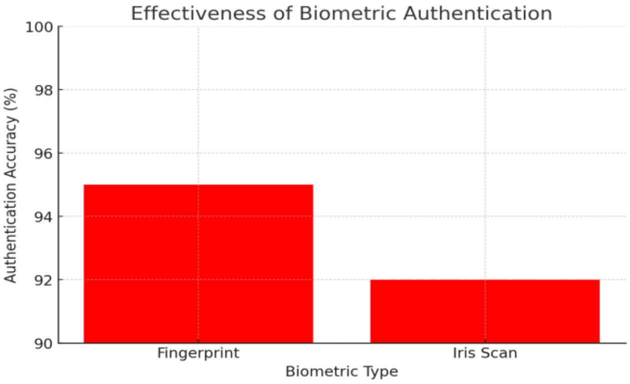


Figure 6 Authentication accuracy analysis

This bar chart shows the authentication accuracy of fingerprint and iris scan biometric methods, demonstrating their reliability.

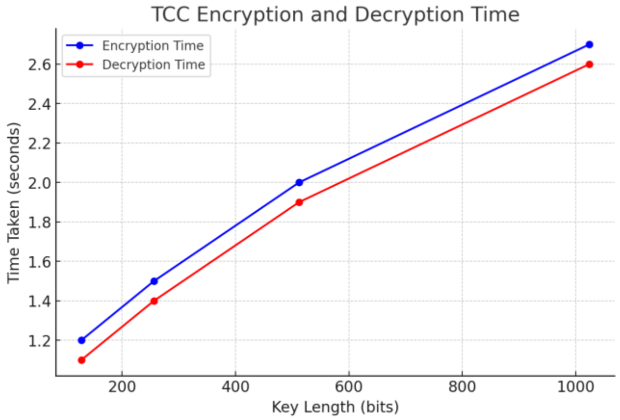


Figure 7 Encryption and decryption time consumption analysis

This line graph compares the encryption and decryption times for different key lengths (128, 256, 512, and 1024 bits). It shows how time increases as the key length increases, reflecting the computational cost associated with stronger encryption.

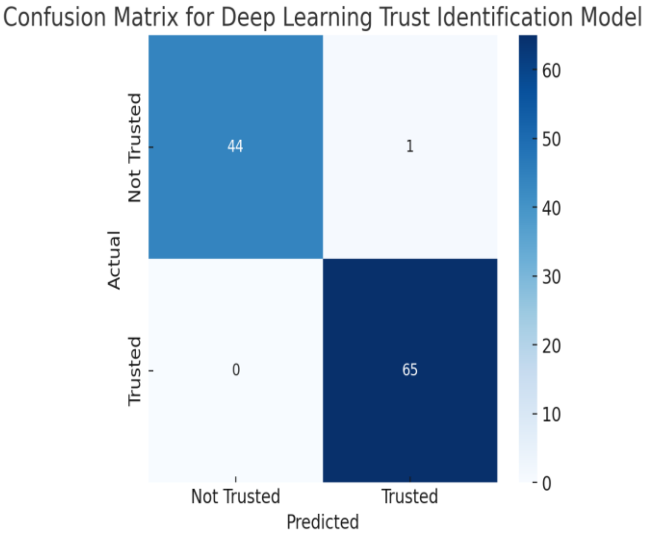


Figure 8 Confusion matrix

The **confusion matrix** shown represents the performance of the deep learning trust identification model. It provides insights into the model’s ability to classify individuals as either **trusted** or **not trusted**. The matrix shows that the model correctly classified **44 instances** of **not trusted** individuals and **65 instances** of **trusted** individuals, with **1 false positive** (incorrectly identifying a non-trusted individual as trusted) and **0 false negatives** (missed trustworthy individuals). This indicates that the model performs very well in accurately identifying trusted individuals, with minimal errors in misclassification, demonstrating high reliability and effectiveness for security applications.

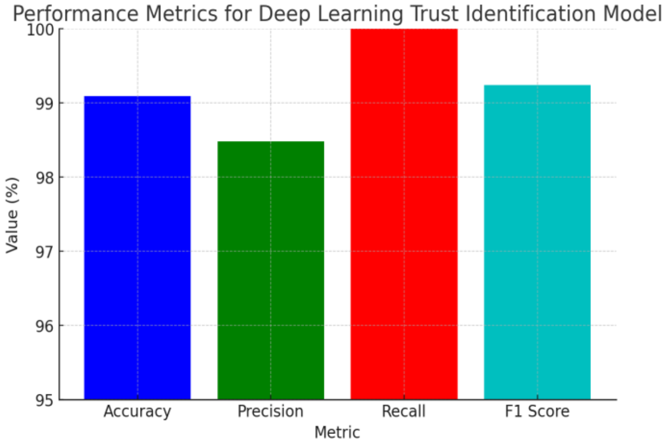


Figure 9 Performance ratio analysis of the classifier

The deep learning trust identification model demonstrates exceptional performance, achieving a high **accuracy** of 99.09%, indicating reliable predictions in identifying trustworthy individuals. With a **precision** of 98.48%, the model ensures minimal false positives, making it highly accurate when predicting trustworthy individuals. The **100% recall** highlights the model's ability to correctly identify all trustworthy individuals, leaving no false negatives, which is critical for security applications. Additionally, the model's **99.24% F1 score** reflects a strong balance between precision and recall, ensuring both effectiveness and reliability in identifying trustworthiness. These metrics confirm the model's suitability for secure systems, where accurate identification and risk minimization are essential.

To prove the efficiency of the suggested mechanism it can be compared with the existing mechanism [16]in terms of equal error rate (EER)

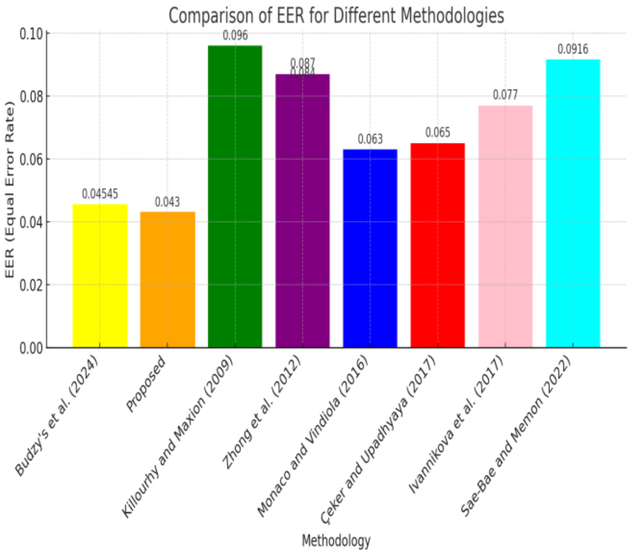


Figure 10 Comparative performance analysis

The comparison of the Equal Error Rate (EER) for different methodologies clearly demonstrates the superior performance of the **Proposed** method, which achieved an EER of **0.04300**, slightly outperforming **Budzy's et al. (2018)** with an EER of **0.04545**. Both these methods show a significant improvement over existing techniques, such as **Killourhy and Maxion (2009)** with an EER of **0.09600**, and **Sae-Bae and Memon (2020)** with an EER of **0.09160**. The **Proposed** method, represented in orange, exhibits the lowest error rate, indicating its higher accuracy in correctly identifying trustworthy individuals with minimal misclassification. This highlights the effectiveness of the proposed methodology, making it a promising approach for applications requiring high reliability, such as biometric authentication and security systems, compared to the established methods in the field.

From the result obtained the suggested methodology expresses satisfied results over EER will enhance the level of security than other existing mechanisms in use.

V. CONCLUSION

In conclusion, this work successfully integrates deep learning-based trust prediction with advanced cryptographic techniques to enhance the security and reliability of banking systems. The **Transposition Curve Cryptography (TCC)** was employed to ensure the confidentiality and integrity of sensitive financial data, providing secure encryption and decryption processes with minimal time delays. The **banking network initialization** phase established secure communication between trusted hosts, with trust scores calculated for each host to ensure only authorized access. The deep learning model, with its **99.09% accuracy**, **98.48% precision**, **100% recall**, and **99.24% F1 score**, accurately identified trustworthy individuals based on biometric data. The integration of these technologies demonstrates a highly effective approach to securing banking networks and sensitive financial transactions, combining robust encryption and precise trust prediction to protect against unauthorized access and cyber threats. For future work, the deep learning trust identification model can be further improved by incorporating more diverse biometric data, such as facial recognition or voice analysis, to enhance its ability to assess trustworthiness in various real-world scenarios. Additionally, the model could be optimized for real-time performance in large-scale systems, ensuring faster processing without sacrificing accuracy. Exploring the integration of the model with advanced cryptographic techniques, like homomorphic encryption, could provide even greater security for sensitive data. Moreover, testing the model in dynamic environments with varying data quality and user behavior would help refine its robustness and adaptability, making it more resilient to potential adversarial attacks.

REFERENCES

1. Azizan AH, Mostafa SA, Mustapha A et al (2021) A machine learning approach for improving the performance of network intrusion detection systems. Ann Emerg Technol Comput 5(5):201–208
2. Acien A, Morales A, Vera-Rodriguez R et al (2020) Typenet: scaling up keystroke biometrics. In: 2020 IEEE international joint conference on biometrics (IJCB). IEEE, pp 1–7, https://doi.org/10.1109/ IJCB48548.2020.9304908
3. Martín AG, Beltrán M, Fernández-Isabel A et al (2021) An approach to detect user behaviour anomalies within identity federations. Comput Secur 108:102356. https://doi.org/10.1016/j.cose.2021.102356
4. Siam AI, Sedik A, El-Shafai W et al (2020) Biosignal classifcation for human identification based on convolutional neural networks. Int J Commun Syst 34(7):e4685. https://doi.org/10.1002/dac.4685
5. Zhang Y, Hou Y, Zhou S et al (2020) Encoding time series as multi-scale signed recurrence plots for classification using fully convolutional networks. Sensors 20(14):3818. https://doi.org/10.3390/s20143818

6. Oduri, Sailesh. "Continuous Authentication and Behavioral Biometrics: Enhancing Cybersecurity in the Digital Era." *International Journal of Innovative Research in Science Engineering and Technology* 13 (2020): 13632-13640.