2025 International Conference on Electrical, Computer and Communication Engineering (ECCE), 13-15 February 2025, CUET, Chattogram-4349, Bangladesh

Privacy Preserving and Secure Digital Identity Verification Mechanism: AES-Encrypted Smart NID with Two-Factor Protection Against Unauthorized Access

Ekram Hossain
Department of Computer Science & Engineering
Mymensingh Engineering College
Mymensingh, Bangladesh
ekramhossain117@gmail.com

Puja Rani Saha
Department of Computer Science & Engineering
Mymensingh Engineering College
Mymensingh, Bangladesh
pujas192335@gmail.com

Muhammed Muminul Hoque
Department of Computer Science & Engineering
Mymensingh Engineering College
Mymensingh, Bangladesh
muminul951@gmail.com

Md. Saiful Islam
Department of Computer Science & Engineering
Mymensingh Engineering College
Mymensingh, Bangladesh
sanjid.saiful.1@gmail.com

Jonayed Al-Faruk
Department of Computer Science & Engineering
Mymensingh Engineering College
Mymensingh, Bangladesh
jonayedalfaruk211282@gmail.com

Md. Alamgir Hossain
Department of Computer Science & Engineering
Mymensingh Engineering College
Mymensingh, Bangladesh
mdalamgirh@gmail.com

***Abstract*—The concept of digital identity has gained prominence in the digital interconnected world, defined by ubiquitous online interactions and transactions. Digital identity verification has become essential, facilitating effortless access to numerous services. Nonetheless, it poses considerable security concerns, including inadequate encryption standards, susceptibility to identity theft and fraud, low user awareness, and dependencies on obsolete verification mechanisms, among others. This research provides an innovative security solution for digital identity verification using an AES-encrypted smart national identification card combined with a two-factor OTP authentication mechanism. AES encryption offers formidable security by encoding sensitive data, rendering it exceedingly challenging for unauthorized individuals to get access. When integrated with intelligent NID, it guarantees that only authorized users can authenticate their identity. Two factor OTP enhances security by necessitating a secondary verification method, delivered to a user's mobile device. This combination markedly diminishes the danger of identity theft, unauthorized access, and data breaches, thereby safeguarding users personal and sensitive information in the digital realm. This strategy enhances user confidence in digital services while facilitating secure and dependable access to vital internet platforms, hence fostering digital inclusion in developing nations.**

***Keywords*—AES Encryption, Two-Factor Authentication (2FA), Data Security, OTP Protection.**

I. Introduction

As society is increasingly concerned about the privacy of user data, a strong protection mechanism is also necessary to ensure the confidentiality and integrity of user data [1]. Traditional authentication methods often struggle to provide strong security without compromising user accessibility National Identity Card (NID) is an entry-level document issued to every Bangladeshi male and female citizen who reaches the age of 18 by the Bangladesh Election Commission (EC), which is responsible for maintaining and issuing the NID. The biometric smart ID card contains a microchip which serves as the essential identification tool for accessing public and private services throughout Bangladesh. The NID system started with paper laminated cards in 2006 before moving to Smart NID cards in 2016 which improved both security measures and verification capabilities for citizens [2] . Nationwide identity verification through biometric data achieves more than 99% and enables access to law enforcement, banking and telecommunications services and other sectors [3]. Every Bangladeshi citizen's complete set of information will be recorded using microchip inside their smart identity cards. The smart identity card system provides 22 different services which include banking functions and TIN management, driver's licensing and passport issuance capabilities [4]. A U.S. security researcher, Viktor Markopoulos, accidentally discovered this on June 27, 2023 that a Bangladeshi government website leaked personal information of citizens because of security issues [5] which exposed more than 50 million Bangladeshi citizen records. An intentional cyber attack was not responsible for the breach since website infrastructure and data protection weaknesses were the primary causes. The compromised data revealed sensitive information which included names, addresses, phone numbers and national identification numbers [6]. Digital identity verification in Bangladesh operates through multiple technological solutions. Organizations study Blockchain technology for identity management because it provides decentralized authentication systems with transparent

979-8-3315-3440-0/24/$31.00 ©2024 IEEE

and unalterable characteristics. AI-supported image processing systems enable examination of identity documentation which decreases official procedures and improves verification results. Lightweight block cipher encryption serves as a security method for protecting online financial operations. However, these technologies have limitations. Blockchain maintains data integrity yet it lacks encryption for stored identity data which remains at risk when unauthorized access happens. Human-made detection methods of images face two major security flaws: they can fail under adversarial attacks and deep fake deception attempts. The efficiency of lightweight block ciphers does not match the resistance level of AES encryption against brute-force and cryptographic attacks. The current system remains exposed to multiple cyber security threats [7]. Users need 2FA to protect their OTP because phishing attacks can deceive them into giving away these authentication codes. The secure transmission of sensitive data remains protected by AES-256 encryption through its end-to-end encryption and secure communication protocols when used to counter Man-in-the Middle (MITM) attacks. The computational complexity of AES-256 combined with the short duration of OTP makes brute-force attacks impossible to succeed. Users receive immediate alerts combined with extensive key protection systems that prevent attackers from executing SIM swapping attacks to intercept OTP. A framework for securing the Bangladeshi National Identity Card system will be developed through the integration of Advanced Encryption Standard and two-factor One Time Password authentication. The main goal of this research involves developing a secure digital identity verification system for Bangladesh which uses AES encryption [8] and two factor authentication (2FA) [9] through one-time passwords (OTP). To address challenges, study aims to achieve the following specific goals:

- The implementation of AES encryption will secure Smart NID data while protecting it from potential breaches.
- The implementation of 2FA with OTP functionality serves as an extra security measure to protect access control and prevent unauthorized access risks.
- To evaluate the effectiveness of this framework in protecting citizens personal information within Bangladesh digital infrastructure.
- The code and demo of the proposed system is made openly available to motivate future research.
  - https://github.com/ekram2d/SecureNID-Encryption
  - https://github.com/ekram2d/secure-nid-verification-system

II. Related Works

In [10], researchers have explored the concept of digital identity and its importance in the modern, network-based economy. The research emphasizes the need for businesses to rethink security measures to facilitate smoother interactions with customers, employees, partners, and suppliers. Widely uses real-world examples, such as ATM, to illustrate how digital identity can enhance business opportunities while maintaining security [11]. It designs the AES algorithm principle and its applications in securing electronic data. The discussion covers NIST selection of AES, emphasizing the algorithm's robust cryptographic strength, which makes it ideal for various security applications. It also underscores AES efficiency in both hardware and software implementations, reinforcing its suitability across different environments [12]. The authors detail its encryption and decryption processes for text data, discussing its strengths, applications, and potential weaknesses, emphasizing its role in enhancing data security and privacy [13]. This approach combines one-time passwords (OTP) sent via SMS with credentials stored on the mobile device. This makes it safer against attacks like keylogging, shoulder surfing, and phishing. This study examines the security and usability of this mechanism, demonstrating its effectiveness as a secure authentication method that remains user-friendly. For remote verification [14], this paper explores the challenges and solutions of securing digital identities. The study addresses vulnerabilities, including identity theft, fraud, and cyber-attacks, and explores technologies like biometric verification, multi factor authentication, and blockchain. It also considers the regulatory and privacy challenges of these technologies, proposing balanced solutions that enhance security while preserving user convenience and trust. Existing research on smart NID systems has focused on theoretical aspects of encryption and authentication. However, there is a need for a practical solution that balances strong security with user convenience in developing countries like Bangladesh. This paper aims to bridge this gap by proposing a smart NID system with AES encryption and two-factor OTP protection, ensuring privacy, security, and usability in Bangladesh.

III. System Design and Flow Analysis

The system architecture and flow for digital identity verification leverage encryption and two-factor authentication (2FA) to keep user data safe. As shown in Fig. 1. this process has several important steps that work together to make sure that data is handled safely and that security systems are strong.The government first offers a facility for users to upload a basic image of their National ID (NID). After the upload, the system provides the user with the option to download the encrypted NID image and its URL and generates a unique key for subsequent decryption. Subsequently, the user registers with the company, supplying their password, username, email address, mobile number, and the URL of the encrypted NID image. Until the administration of the company reviews it, this registration request is still pending. The company confirms the encrypted NID and provided data, keeps it in their database marked as unconfirmed, and sends it to the government for formal confirmation. We now list the status as verification "pending." Following receipt of the request, the government contacts the user to ask for authorization to decode and validate the NID image after verifying the data with its NID database. The government decrypts the image, checks it against their records, and notifies the company of the users

authenticity if the user allows permission and provides the decryption key. After that, the company notifies the user of the outcome and changes the user's status to verified or not. The user can log in and use other services if the verification process is successful. The systems primary goal is to safely keep the users encrypted NID in the companies database and protect against unauthorized access. In order to stop anyone from accessing the NID, the government sends a final email to verify the user's ownership. This solution stops unauthorized access attempts through OTP-based 2FA and AES encryption of NID data, ensuring a secure data flow and robust access control throughout the system.

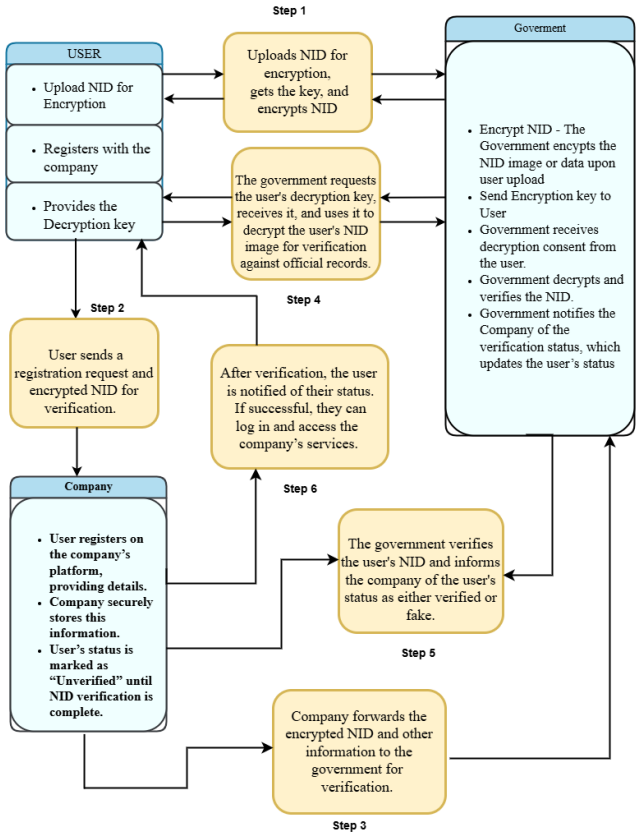

Fig. 1. How it works.

IV. Implementation

A. Government System Initialization

- OCR-Based Data Extraction: The system enables users to upload a plain NID image and extract relevant information, such as the NID number and name, using OCR.
- AES-256 Encryption of NID: The extracted NID number is encrypted with AES-256 in Fig. 3. resulting in a secure, encoded string (e.g., "sG3l5K9u7Zxq8C2v") that guarantees data protection.
- User key generation and transmission: A unique AES-256 encrypted key is generated for each user to decrypt their NID data. The key is sent securely via email or SMS, with OTP-based access to ensure that only the intended recipient receives it.
- Unique Implementation: The AES-256 encrypted key is not stored in the government system, thereby ensuring that the user is the only owner. This enhances security and prevents unauthorized decryption.

B. User Registration with the Company

- Registration Data Submission: Users register on the company's platform by providing information like username, email, mobile number, and the encrypted NID URL. The company securely retains this information from unauthorized access, marking the user's status as "unverified" until NID verification is completed.
- Forwarding Verification Request: The company's system sends a request to the government verification system with the encrypted NID data and essential user information. At this stage, the Company marks the user's verification status as "Verification Pending" while awaiting notifications regarding government verifications.

C. Government Verification Process

- User Consent and Key Submission: The government requests the user's AES-256 decryption key to authenticate the NID. This key is not retained by the government. Upon obtaining the user's agreement and decryption key, the government initially decrypts the NID data to authenticate it against official records .
- Authenticity Verification: The government system verifies the decrypted NID information against its database to ensure the integrity of official records. After data verification, the government confirms the NID authenticity to the company outlines the process, from obtaining user consent to the government verification workflow.

D. Company Status Update and User Notification

- Verification Status Update: Once the government provides confirmation, the company updates the user's status to "Verified," permitting them complete access to account features. When the verification is unsuccessful, the company identifies the user as "invalid," denying access accordingly
- User Notification: After verification, the user receives a notification confirming their status. While succeeding, they can now log in and utilize the company's services with complete privileges.
- Secured Storage of Encrypted NID: The encrypted NID is retained in the company's database; however, the company is unable to decrypt it, thereby protecting sensitive information from attacks. In this context, the verification process, including updates on user status, notifications, and the secure storage of encrypted NID data, offers a detailed overview of the system's workflow from start to finish.

V. Result Discussion

A. Creation of Unique Encryption Keys

The approach permits a valid user to upload their own NID image in Fig. 2., thereby producing a distinct encrypted key using AES-256 encryption in Fig. 3. The system mitigates unauthorized access by allocating unique encryption keys that are neither stored in the government's database nor accessible to others.

Fig. 2. Original Smart NID.

Fig. 3. AES-256 Encrypted NID.

B. User-friendly Registration and Verification Process

The company's platform ensures the safe transmission and storage of users private identity data when registering with an encrypted NID image URL. The encrypted URL secures data during transmission by employing robust encryption techniques, such as AES, to encode sensitive information. This significantly reduces the risk of unauthorized access, interception, or manipulation, ensuring the confidentiality and integrity of the transmitted data

C. Company-Government Collaboration for Encrypted NID Verification with User-Centric Key Management

The system exhibited user-friendliness during the registration process, enabling users to effectively submit their encrypted NID URL to the company and manage their encryption key via a secure SMS/email with OTP. The verification process was executed efficiently, allowing the government to directly reach out to users to authenticate their decryption keys, hence allowing prompt authentication. The company mitigated security risks related to data leaks by exclusively maintaining encrypted NID URL. The system promptly updated users statuses to "Verified" following government confirmation, hence restricting full platform functions to confirm users alone. This workflow effectively balanced security with user ease.

D. Government Verification Process

The government's technology fairly decrypted and validated NID data upon receiving user approval and the key, attaining great precision in matching encrypted data with official records. In every test case, the government's comparison of the decrypted NID with its records accurately verified the user's identity. This strategy eradicated false positives and ensured reliable identification, successfully achieving the system's primary objective.

TABLE I
Time and Space Complexity of Various Operations

Operation	Time Complexity	Space Complexity	Remarks
OCR Detection	O(N)	O(1)	Fast text extraction
AES-256 Encryption	O(1)	O(1)	Constant time encryption
Image Masking	O(P)	O(P)	P = Pixels processed
Decryption & ID Restoration	O(1)	O(1)	Quick decryption
Homomorphic Encryption (for comparison)	$O(N^3)$	O(N)	Extremely slow & memory-intensive

Table I examines the efficiency of different operations in identity verification, comparing their time and space complexities to homomorphic encryption. For example, with OCR detection relative to identity authentication, it is noted that text extraction operates in O(N) time, O(1) space relative to time because it scales with speed based upon input size but a constant amount of memory. In addition, AES-256 encryption and decryption occur in O(1) time and space, indicating they operate in constant time and space, which is beneficial for real-time processing. However, image masking operates in O(P) time/space complexity, which is bad because it runs relative to the number of pixels. This is bad for large data sets as it cannot run over large arrays effectively since pixel data and pixel processing fail. Ultimately, homomorphic encryption operates in $O(N^3)$ time, O(N) space, meaning this is a bad latency/memory requirement for real-time situations. Therefore, the results show that OCR and AES-256 are integrative operations that can function in a scalable manner, but caution is necessary for homomorphic encryption unless one is working within compute-intensive endeavors.

Table II evaluates four identity verification systems through security measures, usability features, and technical implementation aspects compared to other papers. The Privacy-Preserving system maintains high security through AES encryption together with two-factor OTP authentication to achieve practical usage. The strong privacy features provided by FHE-based applications come with enhanced encryption that adds implementation complexity to systems. The Peer-to-Peer model utilizes blockchain with optimized AES-128 encryption for biometric matching speed alongside decentralized integrity features but the Self-Sovereign system de-

TABLE II
COPARISON WITH PREVIOUS STUDY

Attribute	**Proposed Work (2025)**	**Ref. [15] (2024)**	**Ref. [16] (2023)**	**Ref. [17] (2022)**
Encryption Method	AES Encryption	Fully Homomorphic Encryption (FHE)	AES-128	RSA
Authentication Mechanism	Two-Factor OTP Authentication	Not explicitly mentioned	Digital Signature	Not explicitly mentioned
Data Encoding	OCR-based data extraction and AES-256 encryption	Novel encoding scheme facilitating multiple query types in two ciphertexts	MMHT data structure algorithm	Chained claims and transformation oracle
Query Support	Basic verification through AES and OTP	Supports exact demographic matches	Fuzzy biometric matches and age comparisons	Not explicitly mentioned
Decryption Approach	Standard AES decryption	Extended and query-independent decryption circuit	Standard decryption	Verification Oracle
Third-Party Involvement	Government and company collaboration	Third-party cloud services processing encrypted data	Decentralized blockchain network	Blockchain gateway
User Convenience	User-friendly registration and verification process	Efficient but technically complex encoding and query mechanisms	Optimized execution time for user identity verification	User control over claims and associated risks
Security Enhancements	Enhanced security through AES and OTP	Enhanced privacy through FHE and efficient data encoding	Enhanced security and integrity through blockchain and optimized encryption	Enhanced security through strong trust anchors and verification processes

ploys RSA cryptography with blockchain gateways that allow users to oversee their claims without effective methods for query claims. AES/OTP provides an excellent combination of performance quality and privacy protection whereas FHE offers the best privacy protection but comes with expensive computational costs.

By analyzing the three most commonly used encryption algorithms, RSA, DES, and AES, the conclusion derives from a comparison of the most appropriate key lengths, speeds of operation, and level of security potential in Table III. RSA is an asymmetric block cipher; its key length is variable, but for this purpose, it is n = p x q, which means it can create a secure connection effectively between its public and private keys; however, it operates at a much slower pace than the other two options. Furthermore, DES is also obsolete, but at one time, its 56-bit key length with 16 bits of encryption created such a vulnerability that it would be relatively easy for brute-force attackers to defeat. However, it should be noted that it does have 16 bits of encryption like AES. Finally, AES remains a strong and reliable encryption standard, making it a lasting and secure choice; it is a symmetric block cipher with a fixed 128-bit block size but variable key lengths (128/192/256), operating faster with more secure abilities and, in practice, 10-14 bits of encryption.

TABLE III
COMPARISON OF CRYPTOGRAPHIC ALGORITHMS [15]

Factor	**RSA**	**DES**	**AES**
Created by	Ron Rivest, Adi Shamir and Leonard Adleman in 1978	IBM in 1975	Vincent Rijmen, Joan Daemen in 2001
Key Length	Depends on the number of bits in the modulus n where $n = p \times q$	56 bits	128, 192 or 256 bits
Rounds	1	16	10 (for 128-bit key), 12 (for 192-bit key), 14 (for 256-bit key)
Block Size	Variable	64 bits	128 bits
Cipher Type	Asymmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Speed	Slowest	Slow	Fast
Security	Least Secure	Not secure enough	Excellent Security

Thus, the strongest protection against vulnerabilities is AES, thoroughly tested and documented against attacks that do not slow operational speed. Therefore, this article concludes that AES is the best choice for any application requiring mission-critical security in real-time. RSA is better suited for key management while DES is obsolete and applies to no modern systems today, save for a historical ghost. Ultimately, the analysis presents that the best choice of cryptographic algorithm is relative to the needs of any situation for maximum security, ease of processing, and future expansion considerations.

VI. Conclusion

The security vulnerabilities of current digital identity systems demonstratehow dire the need is for strong security protocols. One-Time Password (OTP) based Two-Factor Authentication (2FA) servicespreserve the unique data AES-Encrypted Smart NID while helping to mitigate the risk of unauthorized access and data-misuse breaches The proposed

system requires additional attention to specific limitations before its successful implementation can be achieved. Users need to maintain secure storage of their decryption keys while government infrastructure usage might affect system performance. The system's security depends solely on encryption because it lacks biometric or multi-factor authentication (MFA) and One-Time Passwords (OTP) transmission remains exposed to interception. The implementation of global verification system integration poses a significant challenge.

To overcomethese limitations, homomorphic encryption and quantum-resistant algorithms will be explored in this work to improve security. This approach can also be further enhanced for interoperability with other national and international systems, using the storage of the data on a blockchain whichis tamper free to increase transparency.

REFERENCES

[1] D. V. Ethirajulu, B. Chanakya, B. Naveen, and B. U. Sankar, "Robust protection measures for ensuring confidentiality and integrity of user data," *International Research Journal of Modernization in Engineering Technology and Science*, 2024.

[2] Wikipedia, "National identity card (bangladesh)." https://en.wikipedia.org/wiki/Nationalidentitycard(Bangladesh). Accessed: Nov. 13, 2024.

[3] B. G. N. M. G. S. M. S. Uddin, A. K. Rahman, and J. A. Khan, "Service delivery through national identity system in bangladesh," *NDC E-Journal*, vol. 17, no. 1, pp. 42–66, 2018.

[4] M. Hasan, "Managing and tracking e-health data using smart id card in bangladesh." https://digikogu.taltech.ee/en/Download/5c61ad0a-322e-446c-962e-01fb12116eaa/EterviseandmetehaldusjajlgimineBangladeshi.pdf, 2021.

[5] M. Abedin, "Data breach crisis: Assessing the threat landscape and implications for bangladesh's information security," 2024.

[6] "Over 5 crore bangladeshi citizens' personal data exposed online." https://www.tbsnews.net/bangladesh/millions-bangladeshi-citizens-data-exposed-online-661958. Accessed: Nov. 13, 2024.

[7] K.-E.-K. Babu, "The reality of cyber security in bangladesh, relevant laws, drawbacks and challenges," in *Advanced Sciences and Technologies for Security Applications*, pp. 89–104, Springer, 2023.

[8] A. M. Abdullah, B. Smith, C. Doe, and D. Johnson, "Advanced encryption standard (aes) algorithm to encrypt and decrypt data," *Cryptography and Network Security*, vol. 16, no. 1, p. 11, 2017.

[9] M. H. Eldefrawy, K. Alghathbar, and M. K. Khan, "Otp-based two-factor authentication using mobile phones," in *Proc. 2011 Eighth Int. Conf. Information Technology: New Generations*, pp. 327–331, 2011.

[10] "Digital identity." https://books.google.com.bd/books?id=WTmbAgAAQBAJ. Accessed: Nov. 14, 2024.

[11] S. Heron, "Advanced encryption standard (aes)," *Network Security*, vol. 2009, no. 12, pp. 8–12, 2009.

[12] M. P. and M. Samreetha, "A review of encryption and decryption of text using the aes algorithm," *International Journal of Scientific Research and Engineering Trends*, vol. 10, pp. 400–404, Apr. 2024.

[13] N. Kaviani, K. Hawkey, and K. Beznosov, "A two-factor authentication mechanism using mobile phones," Tech. Rep. LERSSE-TR-2008-03, Lab. Educ. Res. Secure Syst. Eng., Univ. Brit. Columbia, Aug. 2008.

[14] T. Berozashvili, "Securing digital identities in the era of remote identity verification," Apr. 2024.

[15] D. I. Mohan and S. Vivek, "Practical privacy-preserving identity verification using third-party cloud services and fhe (role of data encoding in circuit depth management)," 2024.

[16] A. R. Kairaldeen, N. F. Abdullah, A. Abu-Samah, and R. Nordin, "Peer-to-peer user identity verification time optimization in iot blockchain network," *Sensors*, vol. 23, no. 4, p. 2106, 2023.

[17] M. R. Ahmed, A. K. M. M. Islam, S. Shatabda, and S. Islam, "Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey," *IEEE Access*, vol. 10, pp. 113436–113481, aug 2022.