ECC Cryptography for Image and Data Storage on NAS

[1] Prof. Sharmila Kumari N, [2]Agnesh Kumar S, [3]Anusha B, [4]Jyothsna P,
[5]Neethal Niharika R
Department of CSE, Dr.T Thimmaiah Institute of Technology

Abstract: This project introduces a secure data storage framework that employs Elliptic Curve Cryptography (ECC) to encrypt various forms of digital content, including text, images, and videos. It integrates with Network-Attached Storage (NAS) to enhance efficiency in storage and accessibility. A user-centric graphical user interface (GUI) developed using Tkinter facilitates streamlined encryption and decryption operations, supporting the upload and retrieval of encrypted media. The system enhances security by applying visual obfuscation methods, such as pixelation. It delivers lightweight yet robust encryption suitable for real-time applications by merging advanced cryptographic techniques with scalable storage solutions. This implementation addresses contemporary data privacy concerns while maintaining ease of use across diverse media formats. The proposed system combines ECC and the Advanced Encryption Standard (AES) in a hybrid model, ensuring secure data management within NAS environments.

Keywords: Elliptic Curve Cryptography (ECC) ,AES (Advanced Encryption Standard) ,NAS (Network-Attached Storage) ,Base64,encryption ,decryption ,public key.

I. INTRODUCTION

In today's digital age, the exponential growth of data alongside escalating cybersecurity threats has made data protection a fundamental priority. From personal records to enterprise-level databases, ensuring the confidentiality, integrity, and secure access of information is critical. Cryptography serves as a cornerstone in safeguarding data, particularly through hybrid encryption approaches that leverage the combined strengths of multiple cryptographic algorithms. This project presents a secure data storage and transmission system that integrates Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES), supplemented by Base64 encoding, and deployed over Network-Attached Storage (NAS). ECC, a contemporary public-key cryptographic technique, provides high security with comparatively small key sizes, making it ideal for secure key exchanges in resource-constrained environments. AES, in contrast, is a widely recognized symmetric encryption method that delivers fast and robust data protection. The hybrid model employs ECC for secure key exchange and AES for bulk data encryption, thus optimizing both security and performance. Base64 encoding ensures that encrypted data, particularly binary formats such as images and videos, can be safely transmitted and stored without corruption. The system also features a centralized, scalable NAS-based storage infrastructure, making it suitable for both personal and organizational data security needs enhanced with **Base64 encoding,** and deployed over **Network-Attached Storage (NAS).**

II. RELATED WORK

Rajput and Sharma [1] proposed a novel image encryption and authentication framework leveraging chaotic maps, enhancing both data confidentiality and authenticity. Their approach strengthens image transmission security through nonlinear chaotic dynamics, demonstrating resilience against common cryptographic attacks and supporting integrity verification. Simulation-based performance metrics validated their scheme.

Luo et al. [2] developed a chaos-controlled image encryption method dependent on the original image, thereby increasing key sensitivity and producing a non-repetitive encryption process. This system shows strong resistance to differential attacks, making it suitable for secure multimedia applications due to its unpredictability and robustness.

Singh and Singh [3] applied Elliptic Curve Cryptography (ECC) to image encryption, exploiting its compact key generation and superior security. Their technique offers computational efficiency while maintaining strong encryption, making it especially appropriate for lightweight security contexts and demonstrating significant performance in secure image transmission.

Laiphrakpam and Khumanthem [4] introduced an encryption method for medical imagery based on an enhanced ElGamal scheme integrated with chaotic maps. This hybrid approach prioritizes confidentiality and data sensitivity, surpassing classical methods in randomness and encryption quality, as well as processing speed.

Xu and his collaborators [5] presented a chaotic image encryption algorithm that utilizes block scrambling combined with a dynamic index-based diffusion process. This approach increases system complexity and ensures pixel-level transformation, effectively safeguarding data against statistical and brute-force attacks while maintaining high efficiency.

Wu, Liao, and Yang [6] proposed a color image encryption technique that merges chaotic systems with the elliptic curve-based ElGamal encryption scheme. This hybrid architecture enhances overall security without compromising image quality and demonstrates robustness against known attacks with high encryption throughput.

Sun [7] devised an image encryption strategy grounded in two-by-two DNA complementary rules, incorporating biological principles into digital security. This methodology elevates pixel confusion and diffusion, offering a bio-inspired layer of protection that increases encryption complexity and novelty.

In another work, ***Laiphrakpam and Khumanthem [8]*** developed a robust image encryption scheme based on chaotic systems and elliptic curves over finite fields. Their algorithm ensures high security with computational efficiency, featuring improved confusion, diffusion, and key sensitivity, and performs well in cryptographic evaluations.

Lee and his research team [9] introduced SPRING, a parallel chaos-based image encryption algorithm. By employing parallel processing, the system achieves high encryption speed and efficiency, effectively countering various attack vectors and supporting real-time secure image handling.

Zhang [10] proposed a unified image encryption approach combining chaotic systems with a cubic S-box mechanism. This method improves security through nonlinear substitution and chaotic scrambling, offering strong encryption performance and resistance to cryptanalysis, ideal for applications requiring high data confidentiality.

III. METHODOLOGY

The methodology for implementing Elliptic Curve Cryptography (ECC) for secure image and data storage on Network-Attached Storage (NAS) involves the integration of cryptographic protocols with distributed storage infrastructure to ensure efficiency and data confidentiality. Users interact with the system via a graphical interface to upload text, image, or video files for encryption or decryption.

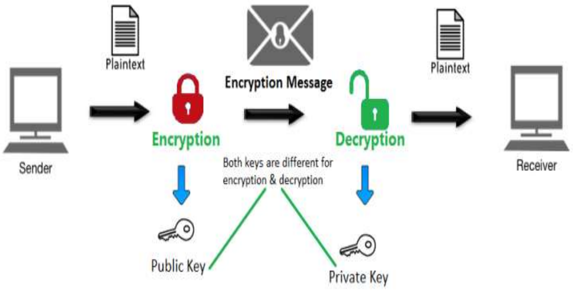
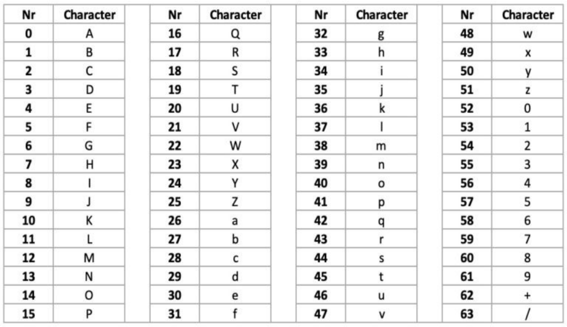


Fig.1: System Architecture

Upon receiving a file, the system generates ECC key pairs—comprising a public key for encryption and a private key for decryption. These keys are derived using mathematically robust elliptic curves to maximize both security and computational performance. For small data such as text, encryption is applied directly using ECC. For larger files, such as images and videos, a symmetric key is first encrypted using ECC and subsequently used to encrypt the data with AES, thus adopting a hybrid encryption strategy.



Nr	Character	Nr	Character	Nr	Character	Nr	Character
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Fig.2: Base-64 Table

Encrypted files are securely stored on a pre-configured NAS, which provides centralized, scalable, and reliable storage with easy access and backup capabilities. The NAS is mounted to the application server, enabling direct read and write operations on encrypted content.

During retrieval, encrypted files are fetched from the NAS, decrypted using the corresponding private key, and returned in their original form. This ensures that only authorized users can access the data, maintaining both confidentiality and integrity. The combination of ECC's lightweight key management and the high performance of AES allows for a highly secure, efficient, and scalable solution for managing sensitive digital assets.

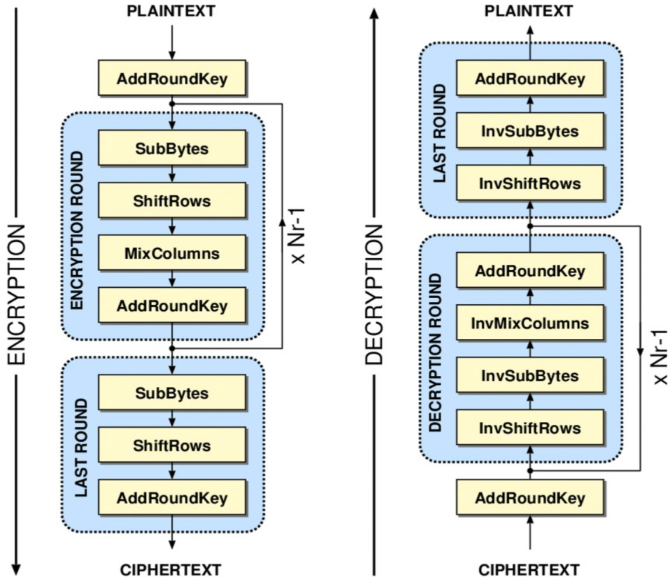


Fig 3: AES Architecture

IV. RESULT

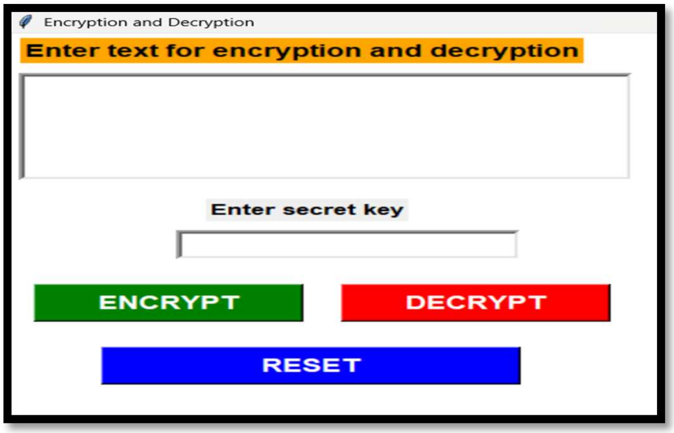
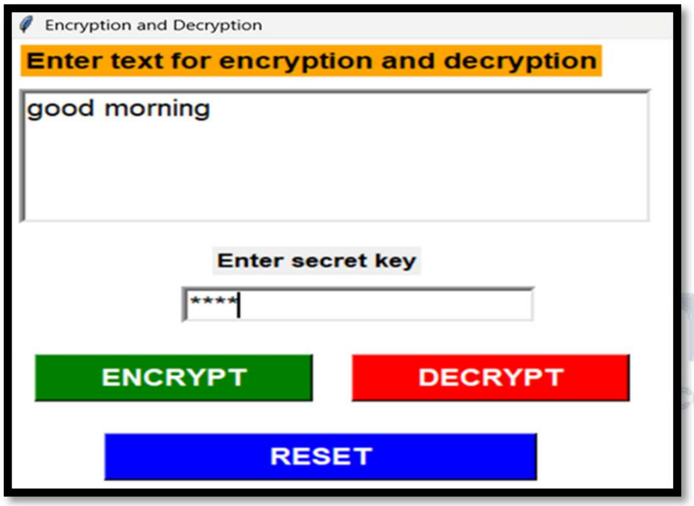

Encryption and Decryption
Enter text for encryption and decryption
Enter secret key
ENCRYPT
DECRYPT
RESET

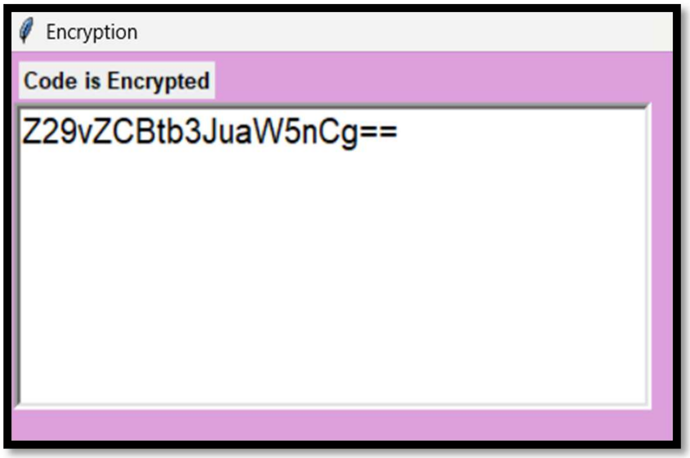
Fig 4: Encryption window


Encryption and Decryption
Enter text for encryption and decryption
Enter secret key
ENCRYPT
DECRYPT
RESET

good morning

****

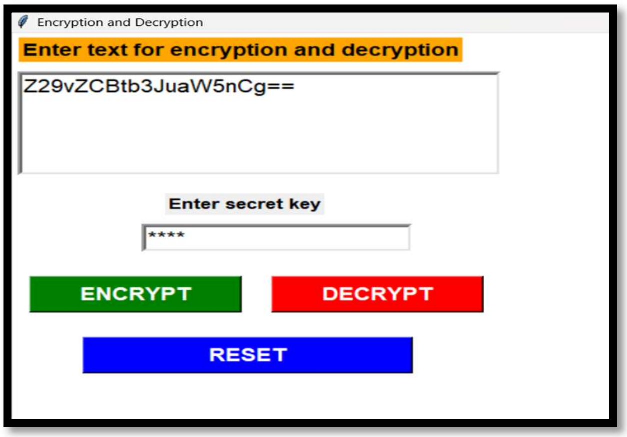
Fig 5: enter the text and key



Code is Encrypted

Z29vZCBtb3JuaW5nCg==

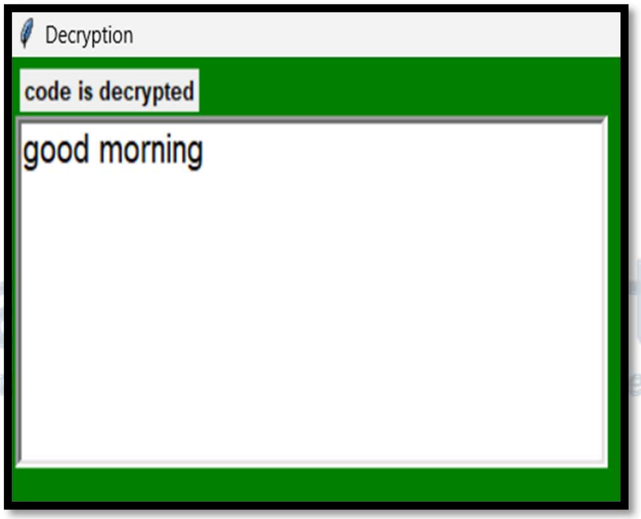
Fig.6: encrypted text


Encryption and Decryption
Enter text for encryption and decryption
Enter secret key
ENCRYPT
DECRYPT
RESET

Z29vZCBtb3JuaW5nCg==

****

Fig.7: enter the text and key



code is decrypted

good morning

Fig 8:decrypted text

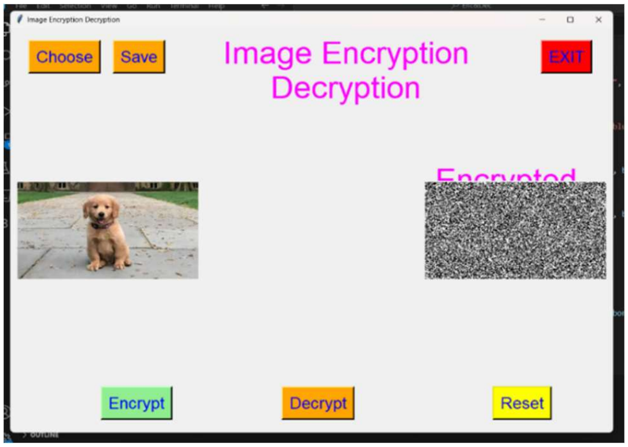


Fig 9: encrypted image

ISSN [Online]: 2583-2654

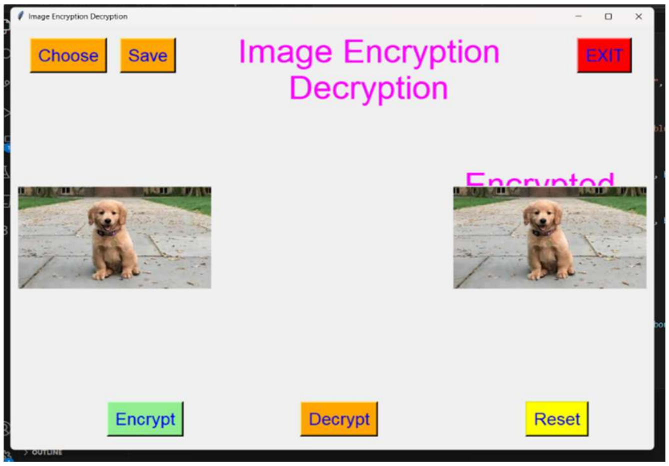


Fig 10: original image after decryption

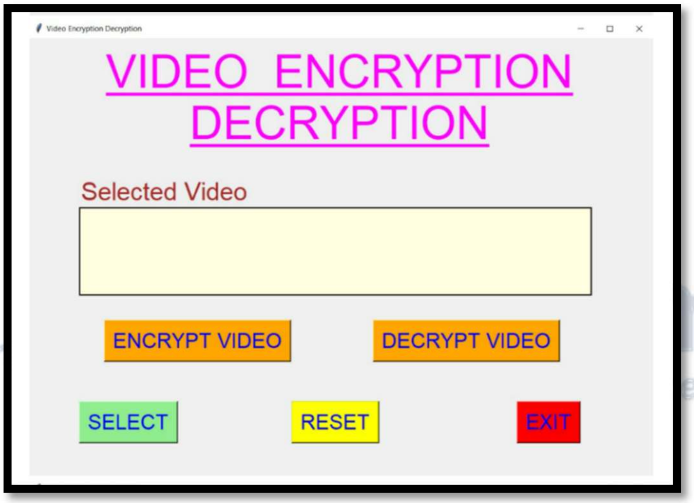


Fig 11:select the video for encryption

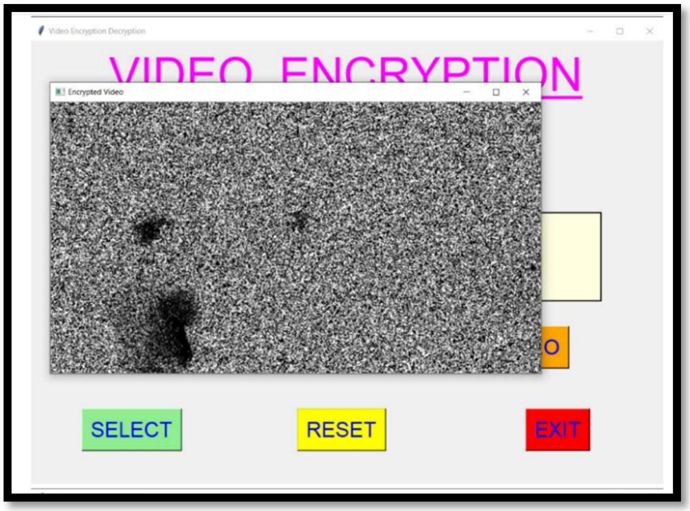
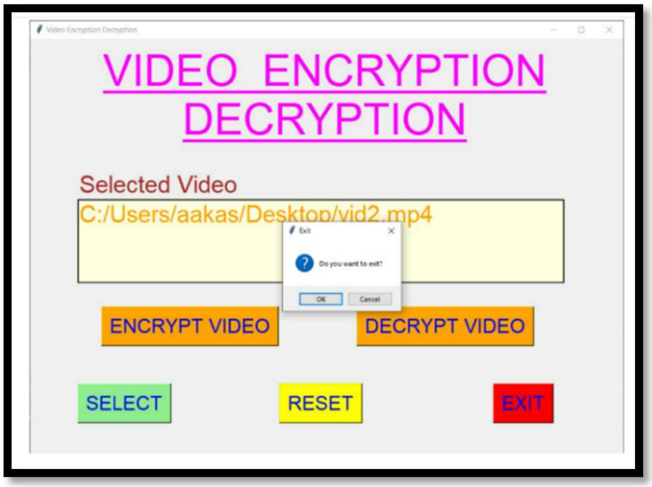


Fig 12: encrypted video



C:/Users/aakas/Desktop/vid2.mp4

Do you want to exit?

Fig 13: click decrypt to obtain the original video

V. CONCLUSION

The project titled “ECC Cryptography for Image and Data Storage on NAS” presents a comprehensive and secure solution for safeguarding sensitive digital content, including text, images, and videos. By integrating Elliptic Curve Cryptography (ECC) with Network-Attached Storage (NAS), the system ensures both data security and accessibility across networked environments. The implementation effectively combines modern cryptographic methods such as AES for symmetric encryption, leveraging ECC for secure key exchange, resulting in a robust hybrid encryption model.Furthermore, the incorporation of visual obfuscation techniques—such as pixelation on encrypted multimedia files—adds an additional layer of privacy, enhancing protection against unauthorized interpretation. The system's frontend, developed using FastAPI, provides a user-friendly interface that simplifies encryption and decryption tasks for diverse file formats, facilitating ease of use without compromising security.Overall, the solution demonstrates high adaptability and is particularly suited for applications across sectors where secure storage and transmission of data are paramount. It significantly contributes to enhancing data confidentiality, integrity, and user accessibility in modern networked storage systems.

VI. FUTURE WORK

Future enhancements to the project "ECC Cryptography for Image and Data Storage on NAS" may focus on optimizing system performance, particularly in the context of large-scale files and real-time encryption processes. Incorporating multi-factor authentication (MFA) can further enhance security by introducing an additional layer of user verification, thereby mitigating unauthorized access risks.Moreover, the exploration of extended hybrid encryption techniques that integrate ECC with other cryptographic algorithms such as RSA or enhanced variants of AES could offer more flexible and resilient security frameworks. Expanding the system to support integration with cloud-based storage platforms would also improve scalability and accessibility, enabling broader adoption across distributed environments.Lastly, continuous updates will be essential to address emerging cryptographic vulnerabilities and to maintain compatibility with evolving technologies. Such proactive adaptation will ensure the system's long-term effectiveness in meeting the dynamic security demands of modern data management infrastructures.

REFERENCES

[1] G. Ye, "A block image encryption algorithm based on wave transmission and chaotic systems," Nonlinear Dynamics, vol. 75, no. 3, pp. 417–427, Feb. 2014.

[2] A. S. Rajput and M. Sharma, "A novel image encryption and authentication scheme using chaotic maps," in Advances in Intelligent Informatics, Cham, Switzerland: Springer, 2015, pp. 277–286.

[3] Y. Luo, L. Cao, S. Qiu, H. Lin, J. Harkin, and J. Liu, "A chaotic map control-based and plain-image-related cryptosystem," Nonlinear Dynamics, vol. 83, no. 4, pp. 2293–2310, Mar. 2016.

[4] L. D. Singh and K. M. Singh, "Image encryption using elliptic curve cryptography," Procedia Computer Science, vol. 54, pp. 472–481, 2015.

[5] D. S. Laiphrakpam and M. S. Khumanthem, "Medical image encryption based on improved ElGamal encryption technique," Optik, vol. 147, pp. 88–102, Oct. 2017.

[6] L. Xu, X. Gou, Z. Li, and J. Li, "A novel chaotic image encryption algorithm using block scrambling and dynamic index-based diffusion," Optics and Lasers in Engineering, vol. 91, pp. 41–52, Apr. 2017.

[7] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," Signal Processing, vol. 141, pp. 109–124, Dec. 2017.

[8] S. Sun, "Chaotic image encryption scheme using two-by-two deoxyribonucleic acid complementary rules," Optical Engineering, vol. 56, no. 11, Art. no. 116117, 2017.

[9] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," Optics and Lasers in Engineering, vol. 88, pp. 197–213, Jan. 2017.

[10] S. Amina and F. K. Mohamed, "An efficient and secure chaotic cipher algorithm for image content preservation," Communications in Nonlinear Science and Numerical Simulation, vol. 60, pp. 12–32, Jul. 2018.