Grenze International Journal of Engineering and Technology, June Issue

Secure Storage of Data using Hybrid Cryptography

Sneha Samuel[1] and Dr. Archana Gupta[2]
[1-2]K.J. Somaiya College of Engineering, Computer Engineering Department, Mumbai, India
sneha.samuel@somaiya.edu, archana.gupta@somaiya.edu

***Abstract*—In today's interconnected world, technology has become an indispensable part of our daily lives. Despite modern advances, the escalating threat of Cyber Crimes underscores the vulnerabilities in the very devices we've come to depend on. This reality prompts us to explore the significance of Cyber Security - understanding what it entails, why it is paramount, and what knowledge is essential. Organizations have three critical tools at their disposal to ensure strong Cyber Security: Authentication, Encryption, and Authorization. Encryption stands out as a foundational layer providing a robust first layer protection for data and enhancing Cyber resilience. So the motivation of this project is to provide an insight into the process of Encryption-Decryption System employing a Hybrid Cryptosystem for the textual data and Symmetric Cryptography for the binary data of different file formats which introduces an extra yet essential layer of shield to the data. Additionally, it also guarantees Confidentiality and fosters trust among users regarding security of their data.**

***Index Terms*— Cyber Security, Hybrid Cryptography, Symmetric Cryptography, Encryption.**

I. INTRODUCTION

All of us live a life having a heavy reliance on the internet as with digital revolution the concept of ‘personal computer’ or ‘home computer’ came into existence which has the capacity to store information. Technology made us dependent on it for nearly everything we do and hence internet is a major part of our everyday lives. Most businesses as well as government agencies, rely on it for everything from record storage to operations. As far as individuals are concerned, smartphones and tablets store personal information such as birthdays, card numbers, dates of important events, passwords and user identification codes and other key data that we use frequently.

As information technology continues to advance, the evolution of cyber threats has maintained a parallel trajectory. A Cyber Security threat is a type of threat that targets computer networks, systems, and user data. These threats can come in the form of malware, phishing, and other malicious activity. One single security breach can lead to exposing the personal information of millions of people. These breaches have a strong financial impact on the companies and also loss of the trust of customers. Unfortunately, data breaches are expected to continue to increase. Thus, Cyber Security and its measures comes into the picture to protect their data and customers. Cyber Security is not just about protecting data that is only inside the computer but over any network also comes under Cyber Security.

Authentication, Encryption and Authorization are the initial steps to tackle Cyber Threats and its consequences. Authentication is the process of confirming someone's identity. Encryption is the process of transforming data into something that looks like gibberish using a secret. This secret can also be used to reverse the process, which is called Decryption. Authorization is the act of giving someone official permission to do something.

Grenze ID: 01.GIJET.10.2.634

This project provides a strong Encryption-Decryption system which provides confidentiality to users data which is either in textual format or binary data for file formats like .pdf, .csv, .jpeg/jpg, .mp4. The power of data Encryption is that it prevents malicious or negligent parties from reading sensitive data. Even when the attacker gets access to an environment and exfiltrates the data or snoops on data while in transit, if the data is encrypted the attacker can't access it. The data is therefore rendered useless. By prioritizing security at its core, this project endeavors to instill trust and confidence in users, ensuring that their sensitive information remains shielded against potential threats and vulnerabilities.

II. Related Work

In 'Text Encryption: Hybrid Cryptographic Method using Vigenere and Hill Ciphers' [1], a combination of Hill Cipher and Vigenere Cipher was demonstrated by Hamza Touil et al. For Encryption, elimination of all spaces and tabulations existing between words or letters is done first. Then in the next phase, the text is split into blocks of size 'n' and apply the Hill Cipher. Then Vigenere Cipher is applied on the Cipher text obtained from Hill Cipher. For Decryption the reverse process is followed. The novelty of this hybrid algorithm is that it regroups Streaming and block ciphers.

In 'A Novel Hybrid Multikey Cryptography Technique for Video Communication' [2], Youcef Fouzar et al. describes the software implementation of video encryption and decryption during online video streaming on Android. It uses a hybrid approach of ECC (Elliptic Curve Cryptography) and RSA (Rivest, Shamie, Adleman) algorithms. Because it's a streaming video application, there is need for dynamic key generation and multikey generation. The RSA is used for encrypting the Video id which becomes the key for the next set of chunks of data. The method derives the key from the ECC equation, i.e., $y2 = x3 + ax + b$ and ECC is used for generating encrypted video chunks. All information, including the username, password, public key, and device information like the MAC (Media Access Control) address, is retrieved and stored in the sender's database.

In 'Security Improvement of Cloud Data using Hybrid Cryptography and Steganography' [3], Mustafa Abbas et al. utilizes Hybrid Cryptography, Steganography and Compression on the data stored in the cloud. First the data's array is divided into odd and even data based on its indexes. The Odd indexed data is encrypted using AES (Advanced Encryption Standard) Algorithm of 256 key size and Even Data Array is encrypted using RSA Algorithm. The AES Key is generated from Random Number Generator and for RSA the Public Key is used for encryption. Then, LZW (Lampel-Ziv-Welch) Compression Algorithm compresses the encrypted data. The compressed, encrypted data is hidden into a Cover Image using LSB (Least Significant Bit) Steganography. The reverse process is followed for Decryption.

In 'Signature Image Hiding in Color Image Using Steganography and Cryptography based on Digital Signature Concepts' [4], data transmission using the concept of Cryptography, Steganography and Digital Signature is demonstrated by Sabyasachi Pramanik et al. Authentication and Non Repudiation is achieved using the concept of Digital Signature where the data is encrypted using the sender's private key and it is decrypted by the receiver using the sender's public key. Asymmetric Cryptographic Algorithm RSA is used for Encryption-Decryption and Steganography is obtained through LSB Algorithm on the blue and red color of the pixel. The sender encrypts the data using his private key and that data is then hidden into a cover image using LSB Steganography at the blue and red color of the pixel. The reverse process is followed for Decryption.

In 'Design of Hybrid Cryptography System based on Vigenere Cipher and Polybius Cipher' [5], a new hybrid security cipher was introduced by Shivam Vatshayan et al. by combining Polybius Cipher and Vigenere Cipher. This hybrid encryption cipher provides greater security as compared to classic ciphers. First a random key is chosen as the key for the Vigenere Cipher. The plaintext is encrypted to cipher text using the Vigenere Cipher key. Further, the obtained cipher text from Vigenere Cipher is used as the input for polybius cipher and it is further encrypted to obtain the second cipher text. For Decryption, the reverse process is followed.

In 'A survey on Symmetric and Asymmetric Key based Image Encryption' [6], Sanjay Kumar et al. talks about how Images have become a part of Digital Communication, Multimedia Applications. At the same time, the need of security while transferring images is tremendously increased. Further they provide a general comparison between symmetric and asymmetric encryption and different algorithms of each type. Among the Symmetric Encryption Algorithms – DES (Data Encryption Standard), AES, Blowfish, RC4 (Rivest Cipher 4), IDEA (International Data Encryption Algorithm) and CRT (Chinese Remainder Theorem) are discussed. Among the Asymmetric Encryption Algorithms – RSA, ECC and El Gamal are discussed.

In 'Combined Cryptography and Steganography for Enhanced Security in Suboptimal Images' [7], S. Joseph Gladwin and Pasumarthi Gowthami combines the features of steganography and cryptography techniques by embedding a crypto text/image into an image. This combination of both steganography and cryptography results

in increased authority and ownership of the data for sub-optimal media applications. The original message is encrypted using Hill cipher. Further, ECC is combined with Hill cipher to add more complexity. After encryption, the encrypted values are embedded in the red and blue pixels values of the base image using the LSB approach. The reverse process is followed for Decryption.

In 'A New Approach for Security in Cloud Data Storage for IOT Applications Using Hybrid Cryptography Technique' [8], a hybrid cryptography system is proposed by Anuj Kumar et al. to provide better security on the data which is stored on cloud storage. The proposed approach uses RSA algorithm and DES algorithm and provides a hybrid of the two algorithms to provide more security on the data before storing it on cloud. Initially RSA (Rivest Shamir Adelman) is applied on the original data. Then on the output of RSA Encryption, DES (Data Encryption Standard) is applied. While downloading the data from cloud storage the Cipher Text is first decrypted using DES algorithm which generate the Cipher Text. The Cipher Text is then provided to RSA algorithm for decryption which generate the plain text back to the user.

'Secure framework for IoT technology based on RSA and DNA (Deoxyribonucleic Acid) cryptography'[9], Mona Elamir et al. talks about the security of medical images and medical diagnostic reports used in the exchange of data between sensors, software, and other E - technologies used to save data over the cloud to block unauthorized data transmission access. Here the medical images and medical reports have been encrypted using an RSA algorithm and then encode the encrypted image into DNA format using encoding rules. For Decryption, the reverse sequence is applied starting with separating mixed DNA strands into two strands by dividing the ratio (p/q). And then applying RSA Algorithm to restore the original data.

In 'Efficient Combination of RSA Cryptography, Lossy, and Lossless Compression Steganography Techniques to Hide Data' [10] Osama AbdelWahab et al. proposes compression of data prior to sending it to the internet which helps in minimizing the time and the cost. Here encryption is done using RSA Algorithm, then it is compressed using Lossless Data Compression Method of Huffman Encoding and then that data is hidden using LSB Steganography. The reverse process is followed for decryption. 'Implementation and Performance Analysis of Hybrid Cryptographic Schemes applied in Cloud Computing Environment [11] Sherief Murad and Kamel Rahouma talks about a comparative study for two-tier versus three-tier hybrid cryptographic models applied to secure data on the cloud. A performance analysis was conducted in terms of encryption time, decryption time, average throughput, and efficiency using relatively larger data files. According to the experimental results, the superiority of the AES hybrid model among the other algorithms in terms of performance was observed. Also, it was found that the two-tier hybrid cryptographic model is more efficient than the three-tier model, but the latter provides more security.

'A Novel Approach of Symmetric Key Cryptography' [12] Sanjeev Kumar et al. presents a novel symmetric cryptography technique based on Caesar cipher symmetric cryptography technique to transform the original text/message into secret text/message. In this technique, the sender transmits hash code instead of symmetric key. The same key is used for Decryption of Cipher Text into Original Message also. The proposed method works for all 256 characters having ASCII (American Standard Code for Information Interchange) value from 0 to 255.

III. PROPOSED WORK

A. Introduction to Proposed System

This application employs cryptography techniques to secure both textual data and binary data. Initially the textual data is encrypted using a Symmetric Encryption Algorithm AES and then further encrypted using Asymmetric Encryption Algorithm RSA to obtain the Ciphertext. During Decryption, the reverse process of Encryption is followed. First Asymmetric Encryption Algorithm RSA is used to convert the Ciphertext and then further Symmetric Encryption Algorithm AES is used to convert it into the original data. Thus, Hybrid cryptography serves as a robust safeguard, fortifying the integrity and confidentiality of sensitive information within the application.

Further, this application also employs Encryption-Decryption of binary data in the form of .jpg/.jpeg, .mp4, .pdf, .csv. For File Encryption-Decryption it uses Symmetric Encryption Algorithm AES as Symmetric Encryption Algorithms is primarily used for bulk data Encryption-Decryption whereas Asymmetric Encryption Algorithms is used for Encryption-Decryption of smaller sizes of data. Thus, using Symmetric encryption we provide a layer of security to our binary data in the form of .jpg/ .jpeg, .mp4, .pdf, .csv.

Apart from Encryption-Decryption, this system will also have Authentication, Logout, Saving the encrypted-decrypted textual data in the relational database and Viewing the data saved in the database functionalities.

B. Block Diagram of Proposed System

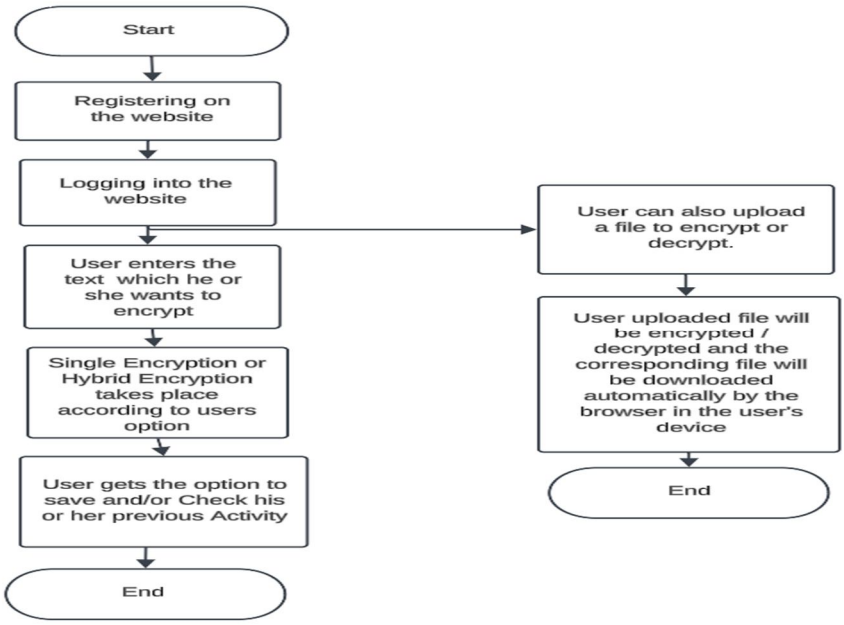


Fig. 1 Block Diagram of the Proposed System

IV. IMPLEMENTATION

A. Authentication

To Authenticate a particular user, he/she needs to first Register and then Login. The user first clicks on the Register button, and whatever details he/she had entered in the form is obtained in the backend. Those Form details are then saved in the database. Before saving the user's password, we create a hash of the password using SHA (Secure Hash Algorithm) -256 and save the hash of the password in the database to prevent malicious actors from accessing the password in case the website is hacked. Also, a check is made whether that user already exists or no using the user's email id.

For Login, the user details are fetched from the database and to verify whether the passwords match for the corresponding user, we create a hash of the user entered password using the SHA-256 and match if the hash of the user entered password and the hash of the password retrieved from the database matches or no. If the passwords match, then the user is directed to Home Page along with a flash notifying about the successful Authentication.

Fig. 2 Registration Form UI

SQL | All Rows Fetched: 8 in 0.024 seconds

FNAME	LNAME	EMAIL	PASSWORD
Sneha	Samuel	ab@gmail.com	a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3
Sneha	Samuel	xyz1@gmail.com	da70dfa4d9f95ac979f921e8e623358236313f334afcd06cddf8a5621cf6a1e9
sneha	oiu	snehasamuel@somaiya.edu	b3a8e0e1f9ab1bfe3a36f231f676f78bb30a519d2b21e6c530c0eee8ebb4a5d0
iuy	tyu	s@gmail.com	86e50149658661312a9e0b35558d84f6c6d3da797f552a9657fe0558ca40cdef
Sneha	Samuel	a@gmail.com	56f4da26ed956730309fa148861lee0f13b0ac95ebb1bc9b5d210e31ff70e79c
qwe	iur	q@gmail.com	cebe3d9d614ba5c19f633566104315854a11353a333bf96f16b5afa0e90abdc4
iuy	oiuy	ty@gmail.com	a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3
poiuyt	jhg	rty@yu.in	610fcca02ba3b30de3a4e372e49bf70cfc042f4b749a66453dd96155d95595b4

Fig. 3 User Details in the Database with hashed password

B. Text Encryption Decryption

On the Home Page, the user enters whatever he/she would want to encrypt. For the implementation of Single Encryption, we create the Secret Key and IV (Initialization Vector) Parameter for AES and then encrypt/decrypt using the same secret key and IV. When the Single Encryption button is clicked by the user, the API (Application Programming Interface) for Single Encryption is hit and along with it the message inputted by the user in the textbox is sent to the function implementing the API as a parameter. This is done using XMLHttpRequest after which the message is encrypted and then returned back on the Home Page.

For Hybrid Encryption we first use AES and then we use RSA. For Hybrid Decryption, the reverse process is followed. Private and Public Keys for RSA is generated which will be used during the Encryption-Decryption process. When the Hybrid Encryption button is clicked by the user on the Home Page, the API for Hybrid Encryption is hit and along with it the message inputted by the user in the textbox is sent to the function as a parameter implementing the API using XMLHttpRequest after which the message is encrypted and then returned back to the Home Page.

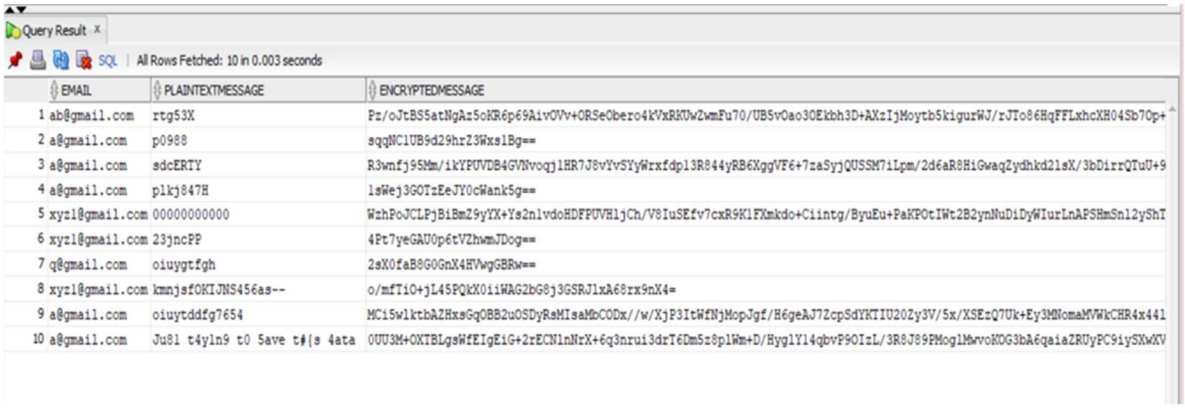
The same process is followed when the Single Decryption button and Hybrid Decryption button is hit.

Fig. 4 Hybrid Encryption on the Home Page

Fig. 5 Hybrid Decryption on the Home Page

C. Storage of Encrypted and Decrypted Data

The user has the option to save his/her Encryption-Decryption activity. When the user clicks on the save button, the API for saving the current data into the database is hit along with the data in the current activity in JSON String format and its corresponding user's email id is sent as a parameter to the backend using XMLHttpRequest. Using the received email id, all the activities that is saved in the database for this particular email id is fetched and shown in a tabular format to the user on the Activity Page. If a particular user has not saved any of his/her Encryption-Decryption activities then a message saying that 'Oops! You don't have any activity yet! Start saving your activity and they will appear here' will be displayed.


Query Result

All Rows Fetched: 10 in 0.003 seconds

	EMAIL	PLAINTEXTMESSAGE	ENCRYPTEDMESSAGE
1	ab@gmail.com	rtg53X	Pz/oJtBS5atNgAz5oKR6p69AivOVv+ORSeObero4kVxRKUwZwmFu70/UB5vOao3OEkbh3D+AXzIjMoytb5kigurWJ/rJTo86HqFFLxhcXH04Sb7Op+
2	a@gmail.com	p0988	sqqNC1UB9d29hrZ3WxslBg==
3	a@gmail.com	sdcERTY	R3wnfj95Mm/ikYPUVDB4GVNvoqj1HR7J8vYvSYyWrxfdp13R844yRB6XggVF6+7zaSyjQUSSM7iLpm/2d6aR8HiGwaqZydhkd2lsX/3bDirrQTuU+9
4	a@gmail.com	plkj847H	1sWej3GOTzEeJY0cWank5g==
5	xyz1@gmail.com	00000000000	WzhPoJCLPjBiBmZ9yYX+Ys2n1vdoHDFPUVHljCh/V8IuSEfv7cxR9K1FXmkdo+Ciintg/ByuEu+PaKPOtIWt2B2ynNuDiDyWIurLnAPSHmSnl2yShT
6	xyz1@gmail.com	23jncPP	4Pt7yeGAU0p6tVZhwmJDog==
7	q@gmail.com	oiuygtfgh	2sX0faB8G0GnX4HVwgGBRw==
8	xyz1@gmail.com	kmnjsfOKIJNS456as--	o/mfTiO+jL45PQkX0iiWAG2bG8j3GSRJlxA68rx9nX4=
9	a@gmail.com	oiuytddfg7654	MCi5wlktbAZHxsGqOBB2uOSDyRsMIsaMbCODx//w/XjP3ItWfNjMopJgf/H6geAJ7ZcpSdYKTIU20Zy3V/5x/XSEzQ7Uk+Ey3MNomaMVWkCHR4x441
10	a@gmail.com	Ju81 t4yln9 t0 5ave t#(s 4ata	0UU3M+OXTBLgsWfEIgEiG+2rECNlnNrX+6q3nrui3drT6Dm5z8plWm+D/HyglY14qbvP9OIzL/3R8J89PMoglMwvoKOG3bA6qaiaZRUyPC9iySXwXV

Fig. 6 Encryption Decryption Activities data in the Database

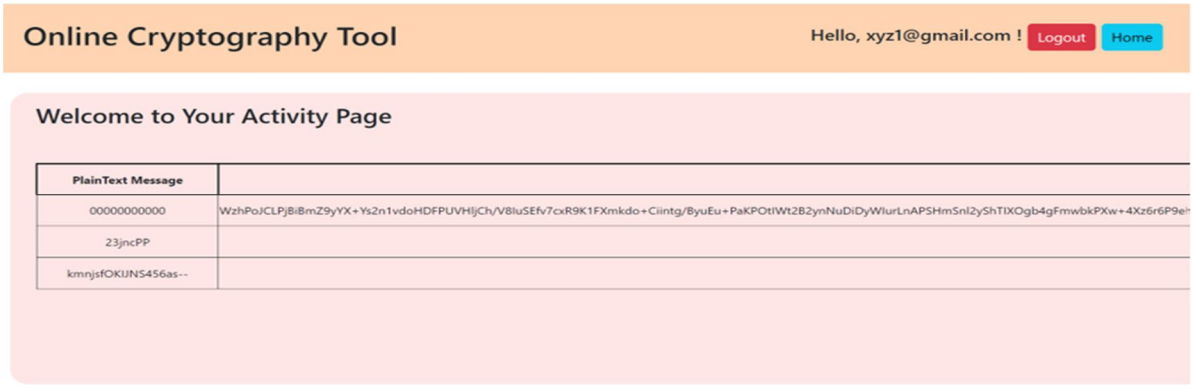


Fig. 7 Activity Page displaying Encryption-Decryption data in tabular format

D. File Encryption Decryption

Apart from text Encryption-Decryption, this application also allows users for binary data in the form of .jpg/.jpeg, .mp4, .csv, .pdf to be encrypted and decrypted using Symmetric Encryption Algorithm AES.
However, unlike for textual data where the encrypted and decrypted format was saved in the database here the Encrypted and Decrypted format of the files won't be saved in the database. Rather, those files will be automatically downloaded onto the user's local device.
As the user uploads the file to encrypt and clicks on submit, the API for File Encryption is hit and the user uploaded file and the type of file is sent to the backend as parameters to the function implementing the Encryption. If the type of the file is not among the ones accepted in this application then a bad request is sent. If the type of the file is among the ones accepted in this application then the file is encrypted using AES and the encrypted output is written to a text file which is then downloaded into user's local device. Similarly for decryption, when the user uploads a file, it is received in the backend after which it is decrypted and then downloaded into the user's local device.

V. RESULTS

To verify the integrity and accuracy of the Encryption-Decryption algorithms, it is imperative that the decrypted output precisely matches the original data. Any variance, no matter how slight, indicates a potential flaw in our

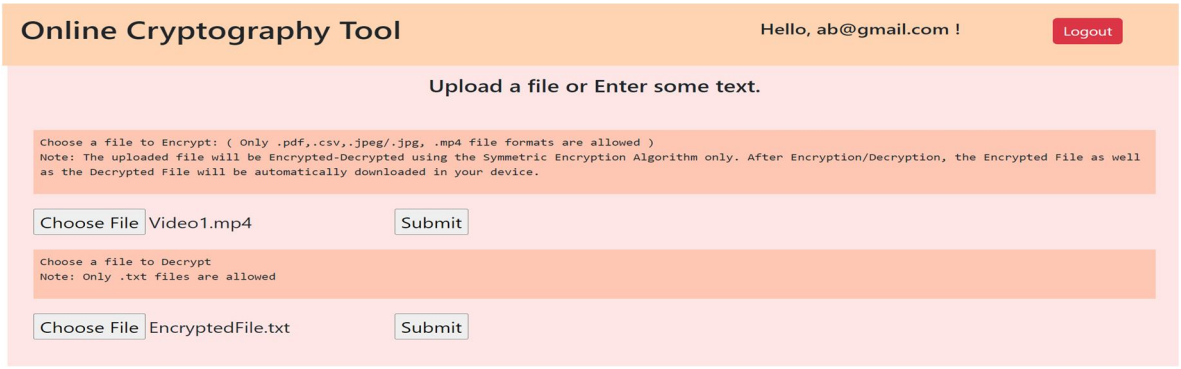


Fig. 8 File Encryption- Decryption on Home Page

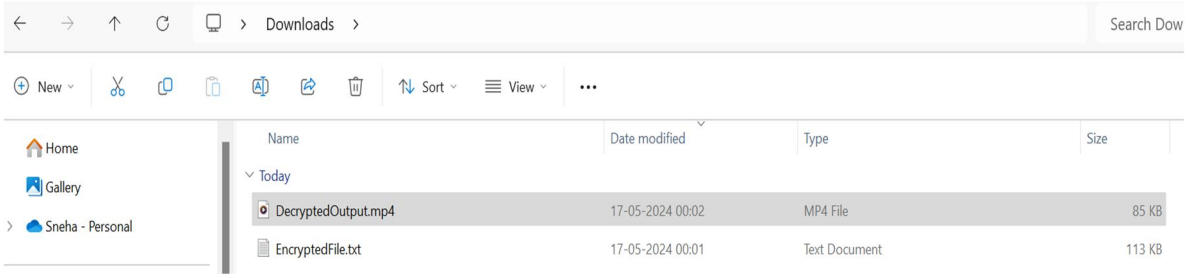


Fig. 9 File Encryption- Decryption Output

Encryption-Decryption process. In case of textual data, we can verify since its in human readable format. But in case of files such as .jpg/.jpeg, .mp4, it's not possible to verify the integrity through human eyes. Thus, comparing the decrypted file with the original file serves as a critical validation step to ensure the reliability of our algorithms.
Below is the table which compares the PDF and CSV original files and its decrypted versions on various metrics.

TABLE I. COMPARISON TABLE FOR PDF AND CSV OUTPUTS

Type of File	**Original File Size**	**Decrypted File Size**	**Content based matching**	**Encrypted File Size**	**Increase in Encrypted File Size**
PDF1.pdf	32KB	32KB	True	42KB	31.25%
PDF2.pdf	140KB	140KB	True	186KB	32.85%
PDF3.pdf	74KB	74KB	True	99KB	33.78%
PDF4.pdf	501KB	501KB	True	667KB	33.13%
PDF5.pdf	351KB	351KB	True	468KB	33.33%
Mean of the Increase in Encryption File Size					32.86%
CSV1.csv	1KB	1KB	True	1KB	0%
CSV2.csv	665KB	665KB	True	887KB	33.38%
CSV3.csv	193KB	193KB	True	257KB	33.16%
CSV4.csv	6KB	6KB	True	8KB	33.33%
CSV5.csv	164KB	164KB	True	218KB	32.92%
Mean of the Increase in Encryption File Size					26.55%

As we can see from the above table, the files remain exactly same content wise after Decryption which verifies the Accuracy of the Hybrid Algorithm. Also, the encrypted file size increased by 33% on an average for PDF files and by 27% on an average for CSV files.

Below is the table which compares the JPG and MP4 original files and its decrypted versions on various metrics.

TABLE II. COMPARISON TABLE FOR JPG AND MP4 OUTPUTS

Type of File	Original File Size	Decrypted File Size	Similarity measure based on tool	Encrypted File Size	Increase in Encrypted File Size
Image1.jpg	1KB	1KB	True	2KB	1%
Image2.jpg	203KB	203KB	True	270KB	33.00%
Image3.jpg	422KB	422KB	True	563KB	33.41%
Image4.jpg	504KB	504KB	True	672KB	33.31%
Image5.jpg	382KB	382KB	True	509KB	33.24%
Mean of the Increase in Encryption File Size					26.79%
Video1.mp4	85KB	85KB	True	113KB	32.94%
Video2.mp4	562KB	562KB	True	749KB	33.27%
Video3.mp4	446KB	446KB	True	594KB	24.91%
Video4.mp4	392KB	392KB	True	523KB	33.41%
Video5.mp4	757KB	757KB	True	1010KB	33.42%
Mean of the Increase in Encryption File Size					31.59%

As we can see from the above table, the files remain exactly equal after Decryption which verifies the Accuracy of the Hybrid Algorithm. Also, the encrypted file size increased by 27% on an average for JPG files and by 32% on an average for MP4 files.

VI. CONCLUSION

Thus, this application offers a robust Encryption-Decryption system integrated with authentication, Text Encryption-Decryption, Database storage, Activity tracking, and File Encryption-Decryption capabilities. This system ensures the confidentiality of user data, adding an essential layer of security. Encrypting data prevents unauthorized access, whether from malicious actors or inadvertent exposure. Even if an attacker gains access to the environment or intercepts data during transmission, the encrypted nature of the data thwarts their efforts. By emphasizing security as a fundamental aspect, this project aims to inspire trust and
provide assurance among users, safeguarding their sensitive information from potential threats and vulnerabilities.

ACKNOWLEDGMENT

The support provided by Computer Engineering Department of K.J. Somaiya College of Engineering, Somaiya Vidyavihar University is greatly appreciated.

REFERENCES

[1] Hamza Touil, Nabil El Akkad, Khalid Satori,"Text encryption: hybrid cryptographic method using vigenere and hill ciphers," 2020 International Conference on Intelligent Systems and Computer Vision, doi: 10.1109/ISCV49265.2020.9204095

[2] Youcef Fouzar, Ahmed Lakhssassi, M. Ramakrishna, "A novel hybrid multikey cryptography technique for video communication," IEEE Access vol.11, pp.15693–15700.

[3] Mustafa Abbas, Suadad Mahdi, Shahad Hussien, "Security improvement of cloud data using hybrid cryptography and Steganography," 2020 International Conference on Computer Science and Software Engineering, doi: 10.1109/CSASE48920.2020.9142072

[4] Sabyasachi Pramanik, Samir Bandyopadhyay, Ramkrishna Ghosh, "Signature image hiding in color image using steganography and cryptography based on digital signature concepts," 2020 2nd International Conference on Innovative Mechanisms for Industry Applications, doi: 10.1109/ICIMIA48430.2020.9074957

[5] Shivam Vatshayan, Raza Abbas Haidri, Jitendra Kumar Verma, "Design of hybrid cryptography system based on vigenere cipher and polybius cipher," 2020 International Conference on Computational Performance Evaluation, doi: 10.1109/ComPE49325.2020.9199997

[6] Sanjay Kumar et al."A survey on Symmetric and Asymmetric Key based Image Encryption," 2nd International Conference on Data, Engineering and Applications, doi: 10.1109/IDEA49133.2020.9170703.

[7] S. Joseph Gladwin, Pasumarthi Lakshmi Gowthami, “Combined Cryptography and Steganography for Enhanced Security in Suboptimal Images”, 2020 International Conference on Artificial Intelligence and Signal Processing, doi: 10.1109/AISP48273.2020.9073306
[8] Anuj Jumar, Vinod Jain, Anupam Yadav, “A New Approach for Security in Cloud Data Storage for IOT Applications Using Hybrid Cryptography Technique,” 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control, doi: 10.1109/PARC49193.2020.236666
[9] Mona Elamir, May Mabrouk, Samir Marzouk, “Secure framework for IoT technology based on RSA and DNA cryptography,” Egyptian Journal of Medical Human Genetics vol. 23, doi: 10.1186/s43042-022-00326-5
[10] Osama AbdelWahab, Aziza Hussien, Hesham Hamed, Hamdy Kelash, Ashraf Khalaf, “Efficient Combination of RSA Cryptography, Lossy, and Lossless Compression Steganography Techniques to Hide Data”,17th International Learning & Technology Conference 2020, vol. 182.
[11] Sherief Murad, Kamel Rahouma, “Implementation and Performance Analysis of Hybrid Cryptographic Schemes applied in Cloud Computing Environment”, 18th International Learning & Technology Conference 2021, doi:10.1016/j.procs.2021.10.070
[12] Sanjeev Kumar, Madhu Gaur, Prem Sharma, Deepkiran Mumjal, “A Novel Approach of Symmetric Key Cryptography” 2021 2nd International Conference on Intelligent Engineering and Management, doi: 10.1109/ICIEM51511.2021.9445343.