IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 2, March-April 2025

Impact Factor: 8.152

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 2, March-April 2025 ||

DOI:10.15680/IJARETY.2025.1202049

Protecting Government Research Content Using AES-Encrypted QR Code Technology

Gowtham Raju Kongara[1], Mareedu Navya[2], Chikkala Jayanth Sai[3], Gullapudi Varun[4], Matta Asha Jyothi[5]

Assistant Professor, Department of CSE, Eluru College of Engineering & Technology, Eluru, India [1]

B. Tech Student, Department of CSE, Eluru College of Engineering & Technology, Eluru, India[2,3,4,5]

ABSTRACT: Government Exploration is pivotal for public development and profitable growth. still, icing that sensitive exploration content is safe from unauthorized access and cyber pitfalls is a significant challenge. Traditional storehouse styles frequently suffer from data breaches, inefficiencies, and availability issues.

This study introduces an innovative result using AES- translated QR law technology to ameliorate the security and availability of government exploration accoutrements. By applying the AES(Rijndael) encryption algorithm, exploration data is securely converted into ciphertext and also bedded into QR canons. This means that only authorized labor force with the correct decryption key can pierce the original content.

Integrating QR law technology not only enhances data reclamation effectiveness but also boosts data protection, making it a strong and dependable system for securing government exploration records.

KEYWORDS: QR Code, Decryption, Encode and Cryptography.

I. INTRODUCTION

Cryptography could be a strategy to secure communication or trade messages between one client with another client, by scrambling the message to be sent ensured to be secure from meddlers since the message is prepared with a key that's not had by the meddler. Encryption could be a handle of making messages that can be perused (plain content) into irregular messages that cannot be perused (cipher content). By and large, there are two sorts of encryption, specifically symmetric encryption where the decryption key is the same as the encryption key, and topsy-turvy encryption where the decoding key isn't the same as the encryption key. The .NET Remoting makes a reference for a remotable protest accessible for a client application, which at that point instantiates and employments this question as in the event that it were a nearby question. Moreover, the genuine code execution happens at the server-side. An protest is recognized by Actuation URLs and are instantiated by a association to the URL. A audience for the question is made by the remoting runtime when the server registers the channel that's used to put through to this question. At the client side, the framework makes a intermediary that stands-in as a pseudo-instantiation of the protest. As such, the remoting foundation ought to know the open interface of the protest already.

The strategy calls that are made against the protest, counting the personality of the strategy and any parameters passed, are serialized to a byte stream and exchanged over a communication protocol-dependent channel to a beneficiary intermediary question at the server side by composing to the Channel's transport sink. Cipher changes over information in a coded frame called Cipher content and reverse cipher changes over the information back into its unique frame called as the plaintext. The Key extension produces a key plan that's utilized in cipher and reverse cipher strategy and composed of particular number of rounds. Number of rounds is subordinate on the key length. Rijndael calculation indicates three encryptions: 128-bit, 192 bit, 256 bit.

The Number of rounds Nr is based on key length of Nk and words. Nb is steady for all forms. Cryptography is the portion of science which bargains with data security which has gotten to be exceptionally basic . The trade of advanced information in cryptography comes about completely different calculation classified into two cryptographic component: symmetric key in which same key issue for encryption and decoding which are quick and less demanding to actualize than topsy-turvy key calculation

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 2, March-April 2025 ||

DOI:10.15680/IJARETY.2025.1202049

1.1 MOTIVATION:

As digital information exchange becomes more common, safeguarding sensitive data from unauthorized access is vital. Cryptography ensures secure communication by encrypting data, making it unreadable to intruders. The prompt discusses symmetric encryption, where the same key is used for both encryption and decryption, and asymmetric encryption with different keys. It also highlights the Rijndael algorithm (AES), which uses multiple rounds for added security. Symmetric encryption is often preferred for its speed and simplicity. The .NET Remoting example demonstrates how encrypted data is securely transmitted between clients and servers. In an increasingly connected world, cryptography ensures data privacy and integrity during transmission.

1.2 PROBLEM DEFINITION:

The primary challenge is to design a secure system that encrypts sensitive government research data using AES encryption and encodes the encrypted data into QR codes. This system should ensure secure storage, transmission, and controlled access to confidential information, thereby protecting against unauthorized access and data manipulation.

1.3 OBJECTIVE OF THE PROJECT:

The objective of this project is to explore secure communication between clients using encryption techniques in .NET Remoting. We will implement symmetric and asymmetric encryption to protect messages between two clients, ensuring secure data transmission. The project will focus on creating and managing remotable objects that are instantiated by clients through Actuation URLs, with actual execution taking place on the server side. The framework will include a remoting runtime that registers channels for communication and facilitates object instantiation. A proxy object will represent the remote object at the client side, maintaining the integrity of the communication process. The project will demonstrate how cryptographic methods can secure data exchange while leveraging the capabilities of .NET Remoting for distributed systems. Additionally, the system will showcase the use of encryption keys for confidentiality and integrity in remote communication.

II. LITERATURE SURVEY

Dynamic 2D-barcodes for multi-device Web session migration including mobile phones:

This article introduces a novel Web architecture that supports session migration in multi-device Web applications, particularly the case when a user starts a Web session on a computer and wishes to continue on a mobile phone. The proposed solution for transferring the needed session identifiers across devices is to dynamically generate pictures of 2D-barcodes containing a Web address and a session ID in an encoded form. 2D-barcodes are a cheap, fast and robust approach to the problem. They are widely known and used in Japan, and are spreading in other countries. Variations on the topic are covered in the article, including a possible migration from a mobile device to a computer (opposite direction), and between two or more mobile phones (possibly back and forth). The results show that this HCI approach is inexpensive, efficient, and works with most camera-phones on the market; the author does see any other mature technique with such assets**.**

Influencing the Online consumer's behaviour: The web experiences:

We examined the relationships between the determinants that affect consumer's use of food delivery apps. Using an extended flow theory model, we explored consumers' experiences in purchasing delivery food through mobile apps. We distributed a self-administered questionnaire online and used structural equation modelling to test the hypotheses. We found that consumer experience (web and digital) had a significant effect on buying intention behavior. The empirical findings show that consumers' experience has significant effect on buying behavior when using the application. Consumer experience in term of the usability, interactivity and aesthetic of the web positively affects food delivery apps buying intention behavior. Further, this study finds that consumers had experience buying from the website are based on the functionality rather than psychology and content factors. Furthermore, digital experience demonstrates a stronger effect on buying behavior with more experience using the food delivery application. This study is one of the early studies to investigate the role of consumer experience. In addition, we find that in user's first interaction with food delivery apps, web experience (usability, interactivity, aesthetic) and digital experience has a larger impact on their buying intention behaviour.

Bar code reading from images captured by Camera Phones:

Bar codes are being widely used in many fields for applications of great commercial value. By encoding a series of characters or symbols, bar codes are able to both carry explicit information and a database key. Nowadays, The availability of imaging phones provides people a mobile platform for decoding bar code rather than the use of the conventional scanner which is lack of mobility. However, the short-distance capture of bar codes using an imaging

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 2, March-April 2025 ||

DOI:10.15680/IJARETY.2025.1202049

phone inevitably makes bar code images blurred, meanwhile, these images are contaminated heavily with noises. Hence, it is a challenge for automatic bar code reading by imaging phones in such applications. In this paper, research effort on the algorithms of bar code reading by real NOKIA imaging phone products is proposed and EAN-13, a widely used 1-D bar code standard, is taken as an example to show the efficiency of the method. The method, of course, can be extended to other bar code standards without much effort. A wavelet-based bar code area location and knowledge-based bar code character segmentation scheme is applied to extract bar code characters under poor image quality of real conditions. Then the waveforms of the 12 marked divisions are input to the decoding engine, which is called statistical recognition block, and final decoding decision is made. Training of the statistical classifiers is based on the modified GLVQ (generalised learning vector quantization) method and the initial feature extraction is based on LDA (linear discriminant analysis). Training samples are from the database contains over 1,100 bar code images taken by an imaging phone and the sample set is extended by manually shifting (distortion) of the original samples to cover more possibilities of occurrence. Nearly 300 EAN-13 bar code images taken by imaging phone (NOKIA 3650) without micro-lens are tested to prove the effectiveness of the proposed method. The entire symbol recognition rate is 85.62%, which is desirable for the first kick-off - - of the attempt to implement bar code reading applications in the camera phone products. Bar code images taken with micro-lens or optical zoom functionality are also tested and the entire symbol recognition rate is nearly hundred percent

Robust Recognition of 1-D Bar codes using Camera Phones:
In this paper we present an algorithm for the recognition of 1D barcodes using camera phones, which is highly robust regarding the the typical image distortions. We have created a database of barcode images, which covers typical distortions, such as inhomogeneous illumination, reflections, or blurriness due to camera movement. We present results from experiments with over 1,000 images from this database using a Mat lab implementation of our algorithm, as well as experiments on the go, where a Symbian C++ implementation running on a camera phone is used to recognize barcodes in daily life situations. The proposed algorithm shows a close to 100% accuracy in real life situations and yields a very good resolution dependent performance on our database, ranging from 90.5% (640 × 480) up to 99.2% (2592 × 1944). The database is freely available for other researchers.

III. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM :

Within the field of cryptography there exist a few methods for encryption/decryption these strategies can be for the most part classified in to two major bunches Routine and Open key Cryptography, Routine encryption is checked by its utilization of single key for both the method of encryption and decoding though in open key cryptography isolated keys are utilized. Our Proposed strategies to a few degree bargains with a few of the downsides of existing strategies that incorporates utilization of key because it is without actuating any disarray within the essential key .Additionally the key measure of proposed concept may be changes from 4character or 32bits to onwards it can be 64-bits ,128-bits and so on while on the other hand the have illustration of DES, AES and triple-DES, Blow-Fish that have settled key structure[9].The key presents the perspective of instability which may be a positive perspective when it comes to encryption, time complexity is the wonder that depicts the impact within the output cipher content on the off chance that a huge content information are adjusted within the file.
This alter that happens at the yield ought to be adequate in case we need to make a secure calculation. Assessing one calculation as a rule have to be consider time complexity and space complexity, which must be very clear of calculation. The paper proposes can mimic the era of plaintexts and keys that happen actually in presence, and the number of assessing tests don’t witnesses exponential development concurring to the input scale.

3.1.1 DISADVANTAGES OF EXISTING SYSTEM:

Fixed Key Size: Traditional encryption algorithms like DES, AES, and Triple-DES have fixed key sizes, making them less adaptable to varying security requirements.
Key Management Issues: In symmetric key cryptography, managing and securely distributing a single key for both encryption and decryption is challenging.
Predictability in Key Generation: Some traditional encryption methods may lack randomness, making them vulnerable to attacks.
Time Complexity: As the data size increases, the time required for encryption and decryption can become significantly high.
Space Complexity: Some algorithms consume more memory, making them inefficient for resource-constrained environments.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 2, March-April 2025 ||

DOI:10.15680/IJARETY.2025.1202049

Security Concerns: Older encryption methods like DES have been proven weak against brute-force attacks due to their small key size.
Scalability Issues: Existing methods may not efficiently handle large-scale data encryption without performance degradation.

3.2 PROPOSED SYSTEM:

We propose a framework to create a windows application which can offer assistance to secure the government investigate substance record within the government segment. The research division of government collects investigate substance and stores it within the database. Each investigate content is scrambled by utilizing AES Rijndael calculation and is put away as QR code picture within the database. Arbitrary key is produced, and the key is part up utilizing Shamir's calculation. In arrange to see the inquire about substance, at that point Get to key is sent to the individual staff mail for confirmation. Once Get to Key confirm, modify key, extract scrambled from QR code picture decode information utilizing key. This empowers security and security and avoids from third- party get to.

3.2.1 ADVANTAGES OF PROPOSED SYSTEM:

Enhanced Security: The combination of AES Rijndael encryption and QR code storage provides a strong security layer, making unauthorized access difficult.

Key Splitting for Extra Protection: Using **Shamir's Secret Sharing** algorithm ensures that the encryption key is divided into multiple parts, reducing the risk of a single point of failure.

Secure Key Transmission: The **Access Key** is sent to authorized personnel via email for authentication, preventing unauthorized retrieval of sensitive information.

Data Integrity & Confidentiality: Encrypting research content before storing it as a QR code ensures that the data remains secure and unaltered.

Prevention of Third-Party Access: The authentication mechanism prevents unauthorized users from accessing or decrypting the sensitive research data.

Efficient Data Storage & Retrieval: Storing encrypted content in QR codes optimizes storage efficiency and allows easy retrieval while maintaining security.

Scalability & Flexibility: The framework can be adapted for different types of research documents and secure storage applications across various government sectors.

IV. SYSTEM DESIGN

4.1 DATA FLOW DIAGRAM:

1.The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.

2.The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.

3.DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.

4.DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 2, March-April 2025 ||

DOI:10.15680/IJARETY.2025.1202049

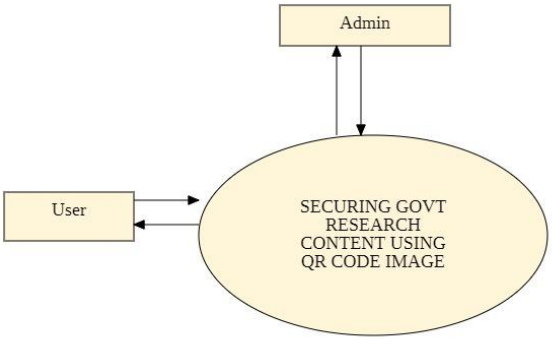

Fig 1: Data Flow Digram

4.2 SYSTEM ARCHITECTURE :

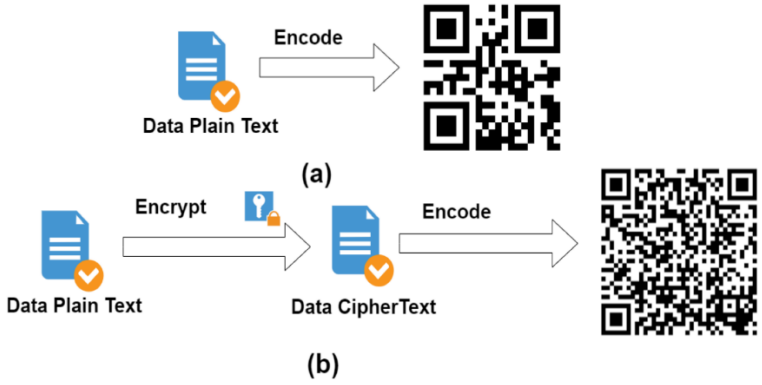

Fig 2: System Architecture

4.3 RIJNDAEL ALGORITHM

The Rijndael algorithm (pronounced as "Rain-dahl") is the symmetric key encryption algorithm that was selected as the Advanced Encryption Standard (AES) by the National Institute of Standards and Technology (NIST) in 2001

What Is Rijndael Algorithm:

- Rijndael is a **block cipher** that encrypts data in **fixed-size blocks of 128 bits**, with **key lengths of 128, 192, or 256 bits**.
- It was developed by two Belgian cryptographers, **Vincent Rijmen** and **Joan Daemen**, which is why the name "Rijndael" comes from their surnames.

Working Of Rijndael Algorithm

The algorithm operates in multiple rounds (10, 12, or 14 rounds) depending on the key size:

Key Size	Number of Rounds
128-bit key	10 rounds
192-bit key	12 rounds
256-bit key	14 rounds

Main Steps in Each Round :

Each round consists of four major steps:

1. Sub Bytes (Substitution Layer):

- Each byte in the block is replaced using an S-box (Substitution box).
- The S-box is a fixed 16x16 matrix used for non-linear substitution, making the algorithm resistant to attacks like differential and linear cryptanalysis.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 2, March-April 2025 ||

DOI:10.15680/IJARETY.2025.1202049

2. ShiftRows (Permutation Layer):
   - The rows of the state matrix are shifted to the left by different offsets.
   - Row 0 remains unchanged.
   - Row 1 shifts left by 1 byte.
   - Row 2 shifts left by 2 bytes.
   - Row 3 shifts left by 3 bytes.

3. Mix Columns (Mixing Layer):
   - Each column of the state matrix is transformed using matrix multiplication over a finite Galois field (GF(2^8)).
   - It provides diffusion, meaning changes in one byte affect all other bytes.
   - Add Round Key (Key Mixing Layer):
   - The current state matrix is XORed with a round key derived from the original key using a key expansion algorithm.

V. RESULTS

The following figures present the sequence of screenshots of the results.

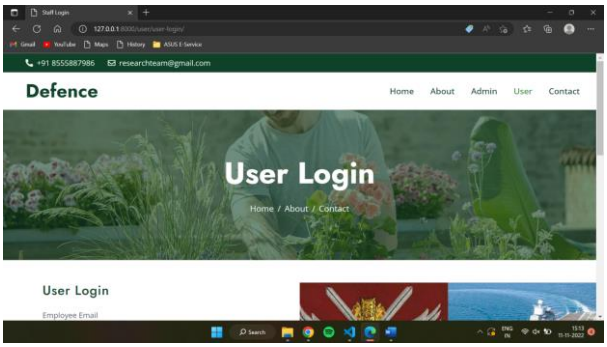

Fig 3a: Login page

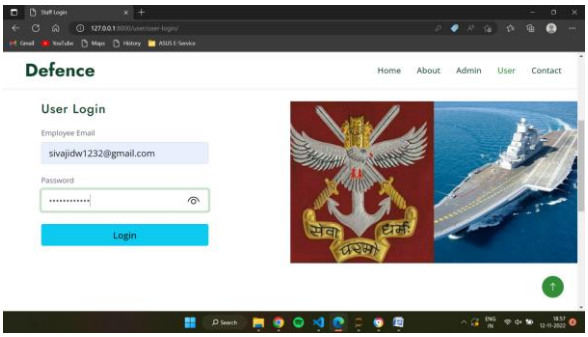

Fig 3b: User Login

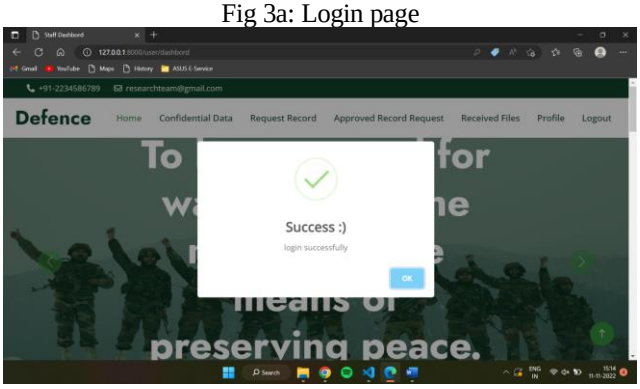

Fig 3c: Login Success

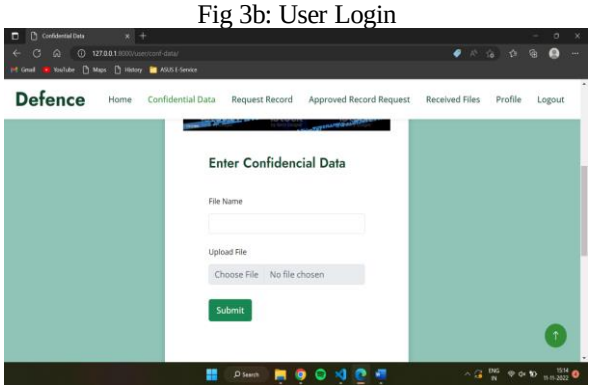

Fig 3d: Enter confidential data

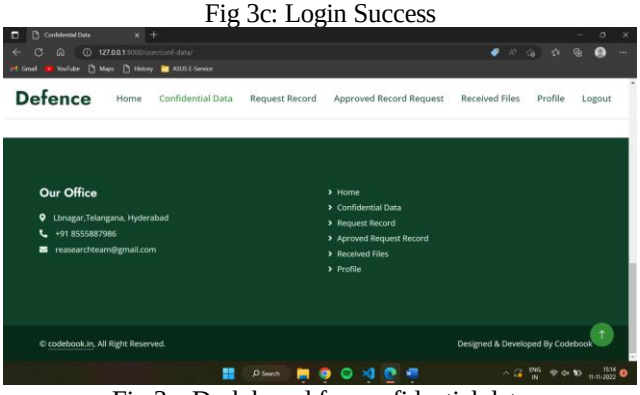

Fig 3e: Dash board for confidential data

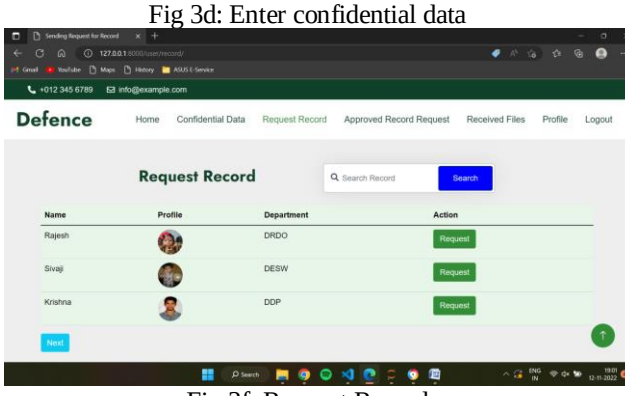

Fig 3f: Request Record

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 2, March-April 2025 ||

DOI:10.15680/IJARETY.2025.1202049

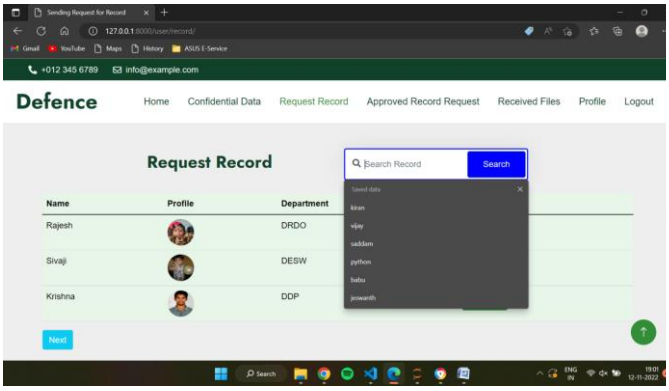

Fig 3g: Request Record Cont.

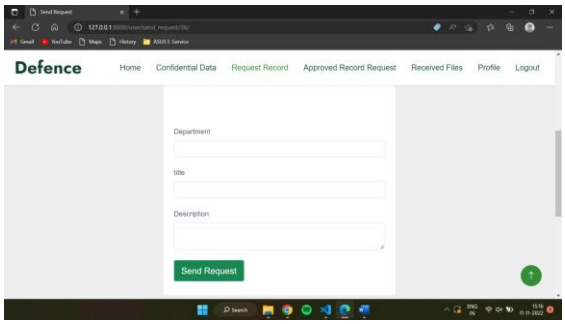

Fig 3h: Send request

Fig 3i: Send request dash board

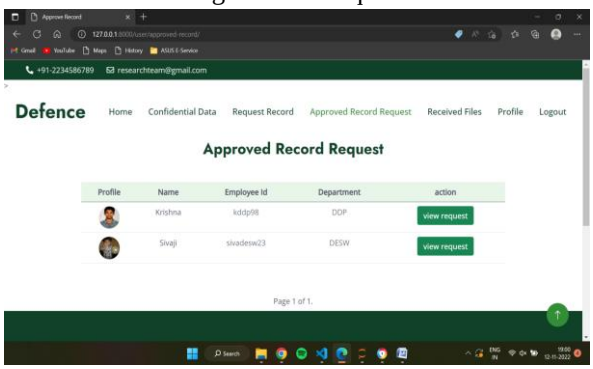

Fig 3j: Request Approved

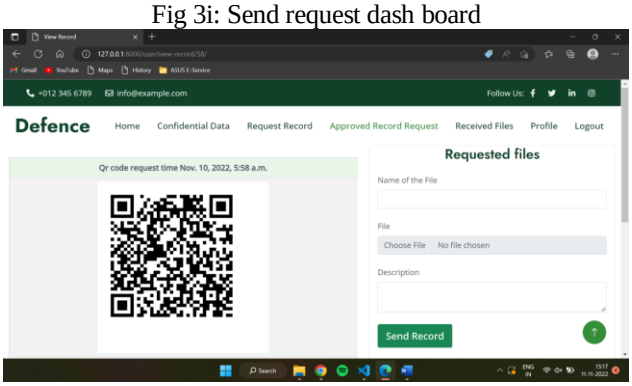

Fig 3k: QR Scan

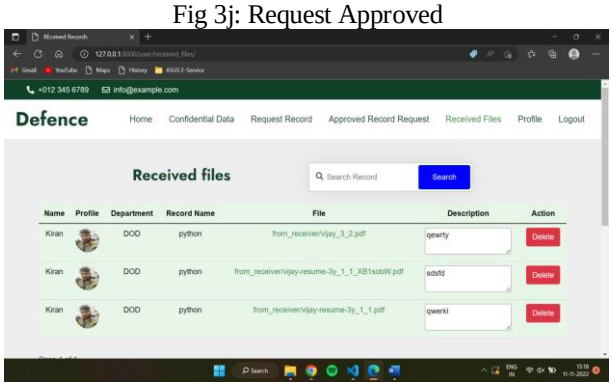

Fig 3l: Received Files

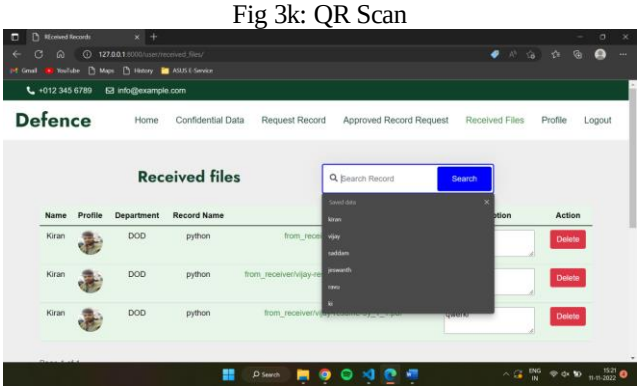

Fig 3m: Received Files Cont..

Fig 3n: Verification

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 2, March-April 2025 ||

DOI:10.15680/IJARETY.2025.1202049

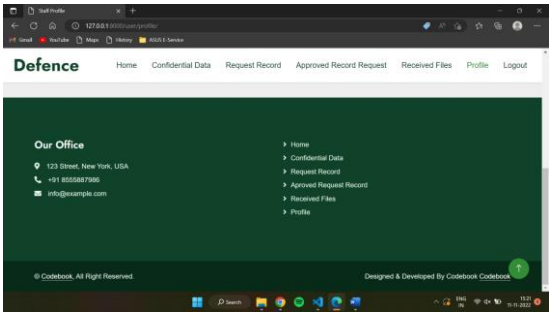

Fig 3o: Verification Dashboard

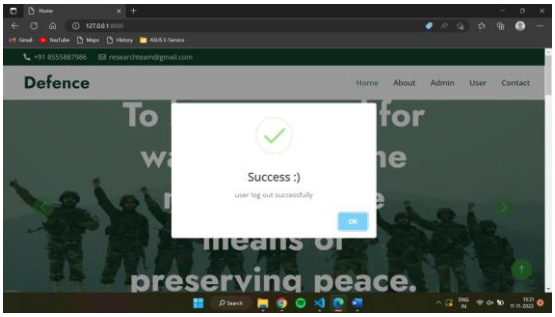

Fig 3p: Verification Succuss

VI. CONCLUSIONS AND FUTURE WORK

6.1 CONCLUSIONS

From now on Government segment may be a imperative portion of the nation's economy. Assurance of government investigate substance from all sorts of dangers is basic not as it were for commerce progression but too for supporting the economy of the country as a entirety. With the digitization of conventional records, government substances experience troublesome issues, such as government capacity and access. Research division spend significant time questioning the desired information when getting to Government inquire about substance subtle elements, but the gotten information are not essentially rectify, and get to is some of the time limited. Too the premise, this think about proposes a inquire about substance which utilize ciphertext-based encryption to guarantee information secrecy and get to control of record subtle elements. The inquire about head may scramble the put away data for achieving get to control and keeping information secure. From now on AES Rijndael calculation is utilized for encryption. This guarantees security for the data and empowers Security.

6.2 FUTURE WORK

Future work for this project aims to enhance security, accessibility, and scalability by integrating advanced technologies. One key improvement is the incorporation of blockchain technology to create a tamper-proof logging system that ensures transparency and prevents unauthorized modifications to access records. Additionally, AI-based threat detection can be implemented to analyze user behaviour and detect suspicious activities, helping to prevent potential cyber threats in real time. To improve data accessibility while maintaining security, cloud-based encrypted storage can be introduced, allowing government personnel to securely store and retrieve encrypted QR codes from remote locations without compromising confidentiality.

Moreover, developing a dedicated mobile application will enable authorized users to scan, retrieve, and decrypt research content conveniently using their smartphones while ensuring end-to-end encryption. To further strengthen authentication mechanisms, biometric security features, such as fingerprint scanning or facial recognition, can be integrated to prevent unauthorized access and eliminate reliance on passwords alone. As technology evolves, post-quantum cryptography should also be explored to future-proof the encryption system against quantum computing threats, ensuring long-term data security.

An automated key recovery system can also be introduced to securely restore lost or corrupted encryption keys without exposing sensitive information. Additionally, the system should be expanded for large-scale deployment across multiple government agencies, enabling a unified, high-security research content management system. These enhancements will significantly improve the system's reliability, making it a robust, future-ready solution for protecting sensitive government research content while ensuring efficient accessibility for authorized personnel.

REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, "The secure data informatics based on data encryption.," IEEE vol. A247, pp. 529–551, April 2016

[2] Alexandre Alapetite, "Dynamic 2D-barcodes for multi-device Web session migration including mobile phones", ACM Digital Library, Springer-Verlag London, UK , Volume 14 Issue 1, January 2010.

[3] Constantinides, E., (2004), "Influencing the Online consumer's behaviour: The web experiences", Internet Research, vol.14, no.2, pp.111-126.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 2, March-April 2025 ||

DOI:10.15680/IJARETY.2025.1202049

[4] Thirunagalingam, A., & Whig, P. (2025). Emotional AI Integrating Human Feelings in Machine Learning. In Humanizing Technology With Emotional Intelligence (pp. 19-32). IGI Global Scientific Publishing.
[5] Gagandeep Nagra, R .Gopal, "A study of Factors Affecting on Online Shopping Behaviour of Consumer", International journey of scientific and research publications, Volume3, issue 6, June 2013.
[6] Mobile technology, Applications and System, 2005 International Conference on Bar code reading from images captured by Camera Phones.
[7] International Standard ISO/IEC 18004 (2000). Automatic Identification and data capture techniques-Bar code symbology-QR Code, Switzerland. .
[8] S. Wachenfeld, S.Terlunen, and X.Jiang, "Robust Recognition of 1-D Bar codes using Camera Phones", Proc. Int'l Conf. Pattern Recognition, pp. 1-4, 2008.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com