IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.11569

Online Transaction System Using Cryptography

Lucky Chaudhary[1], Noor Ahmad[2] Prakhar Mishra[3], Rayyan Manzar Ansari[4]

Student, Department of Computer Science and Engineering, Inderprastha Engineering College,

Ghaziabad, 201010, UP, India

INTRODUCTION

Information security can be summarized as a set of information, steps, procedures and strategies that are used to prevent and monitor illegal access, troubleshooting, revelation, disturbance and adjustment of computer network sources.

Increasing the privacy, reliability and eligibility of the work, it requires a lot of work to strengthen the existing methods from practicing to break them and to improve upon a new way that are resistant to most types of attacks if not all.

Accordingly, it was proven that encoding is one of the most reliable strategies used to secure information since ancient times. In the days of the Romans who used similar methods to enable protection on their valuable information and documents.

Data encoding is the process of converting the form of data into certain symbols through the use of meaningless codes. The process of encoding and decoding completely depends on a single key which is known as same key cryptography. In this process, the same key is used for both encryption and decryption processes. It requires a secure channel between sender and receiver to transfer the secret key. Double cipher modes are dealt with by a symmetric algorithm: block ciphers and stream ciphers.

The block cipher operates on fixed-length groups of named blocks, without transformation specified by a symmetric key. A constant size is controlled by a set of block ciphers. It consists of several identical rounds of processing in which each round, an interchange is performed on one half of the information, followed by a permutation that joins the two halves.

The original key becomes larger, so multi-label keys are used for each round. A symmetric key cryptography indicates cryptographic algorithm that requires two separate keys: the first of which is private (hidden) while the other is public. Although they are not the same, but they are mathematically related. The public key is used to encode the plain text, whereas the private (hidden) key is used to decode the cipher text**.**

GAP ANALYSIS

The main drawback of the existing system is that it fails to prevent the hacking of the user and storing data in an image using steganography which increases the memory in the very first place. The newly planned system thus overcome this drawback by not only encrypting the user details but also storing these details in a hash code (cipher text) has a very significant plus over cryptography which is that the intended secret message to be transmitted over a network does not garner any attention to itself as an item of examination.

Thus, the system carries out the transaction using this hash code making hacking of details much more difficult there by adding an additional level of security as compared to the existing system. Along with fraud prevention the system also focuses on fraud detection by carrying out the data mining on the server side in order to determine any king of change in user spending pattern and transaction location further safeguarding the online banking procedure.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

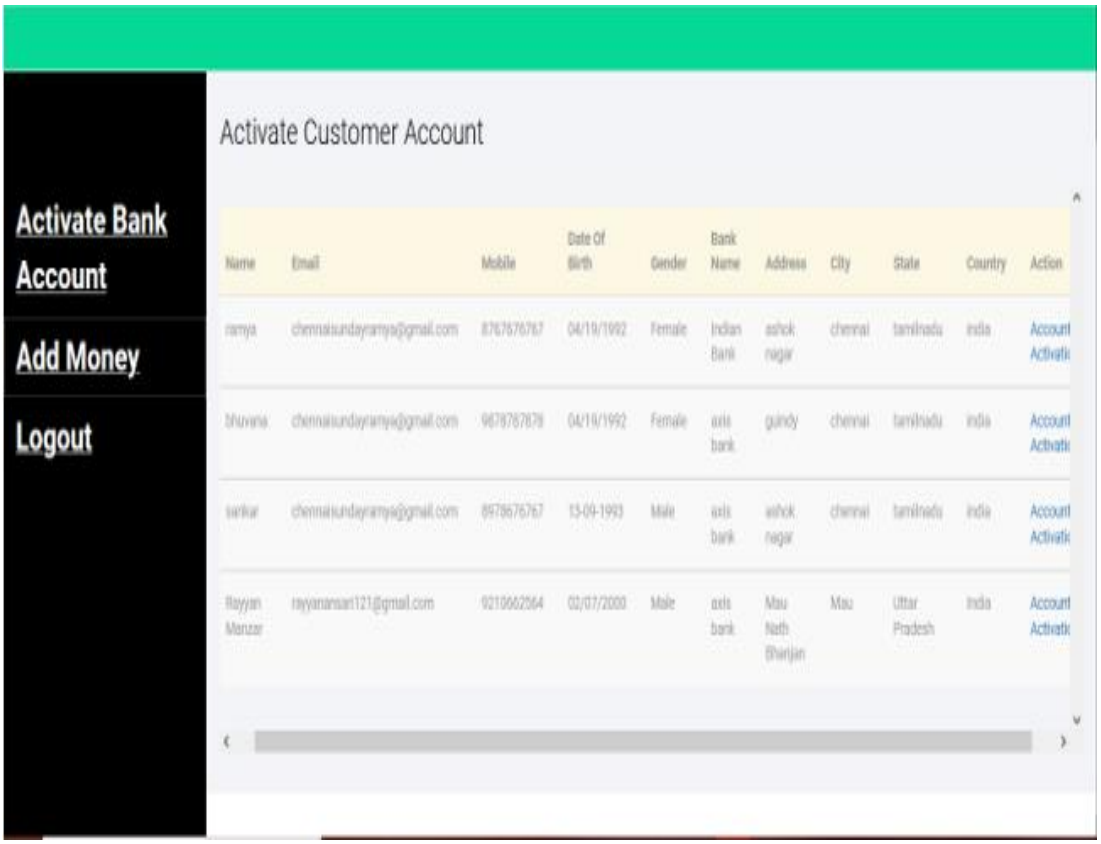
International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.11569

IMPLEMENTATION

Admin Page: -



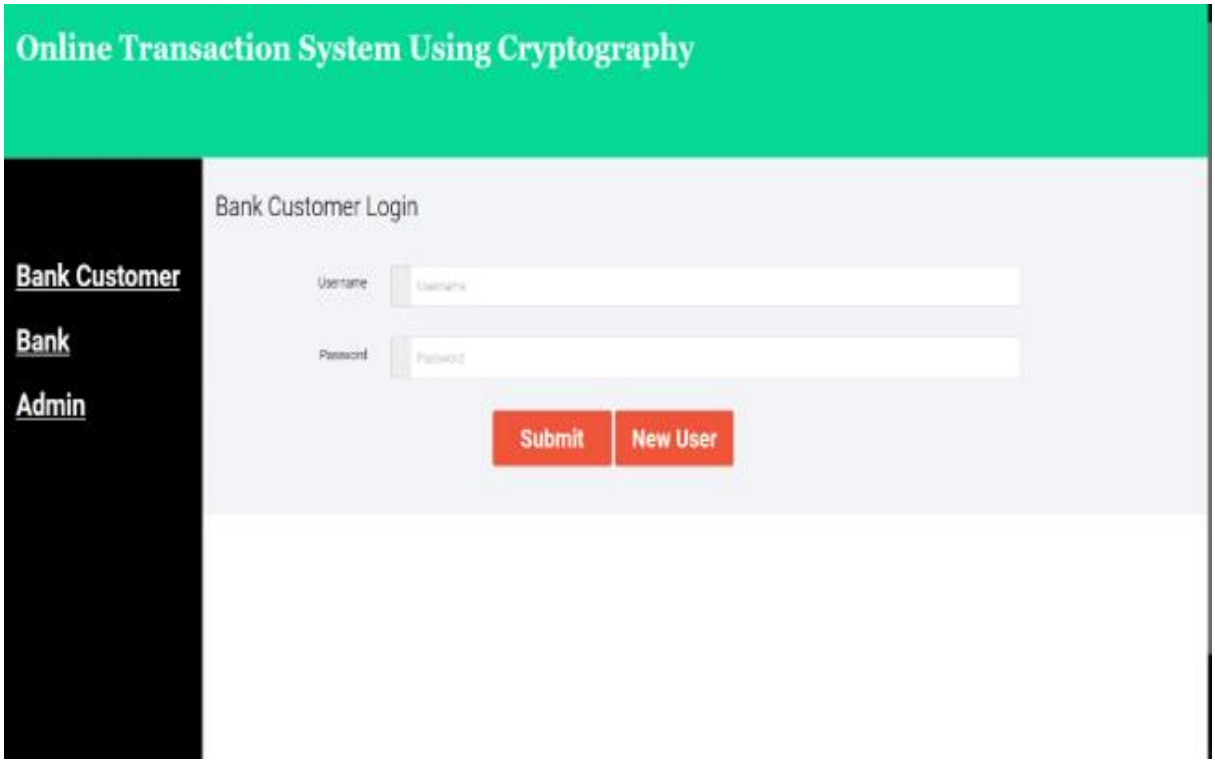
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.11569

Customer Login Page: -



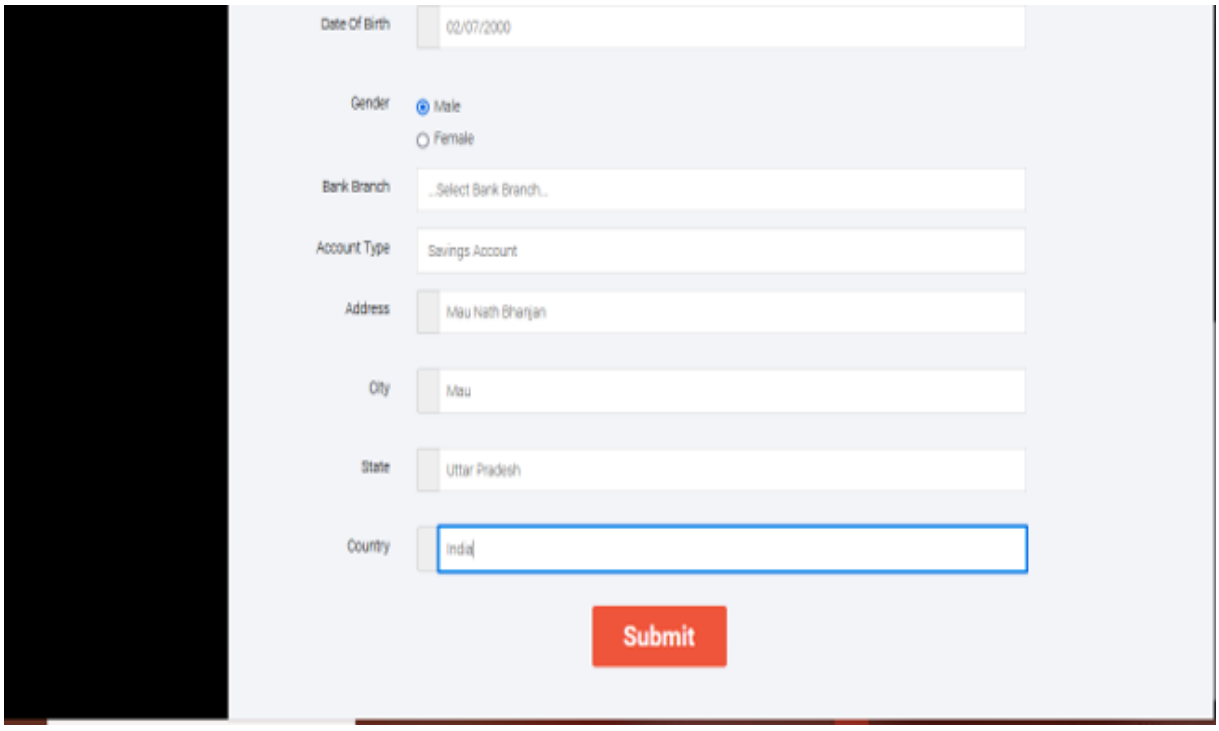
Customer Registration Page: -

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

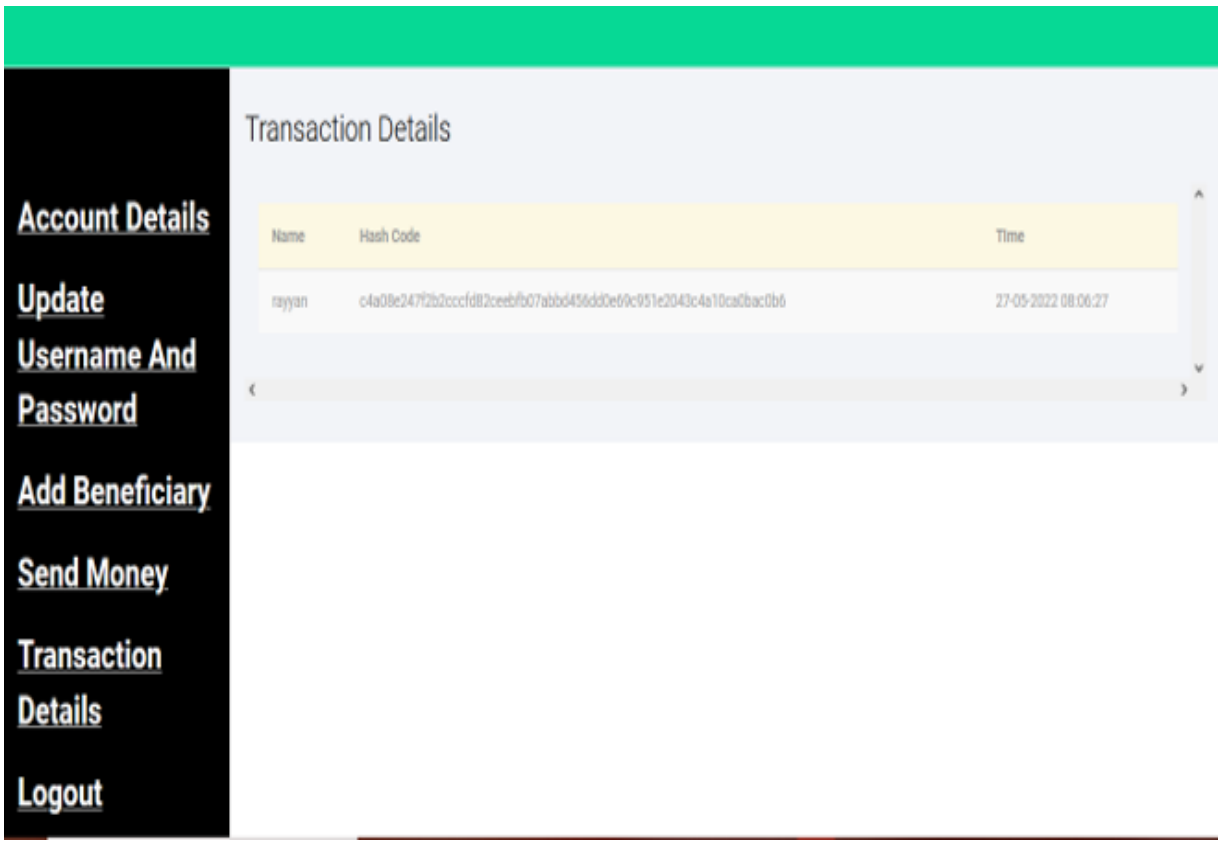
International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.11569



Transaction Details: -



IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.11569

CONCLUSION

This paper presents a survey of the most important cryptography algorithms to date. These are cryptographic algorithms well studied and analysed to help enhance the performance of current cryptographic methods. The result shows techniques that are useful for real-time encryption. All encryption methods have proven that their advantages and shocks and has proven to be suitable for various applications. comparison between symmetric and asymmetric algorithms show that symmetric algorithms are faster than their asymmetric counterparts. Through the last and in the result of study and comparison, we find that the most reliable algorithm is AES in terms of speed encryption, decoding complexity, key length, structure and flexibility.