International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

Bargain Based System Using Encrypted Chatting Application

N Devindran[1], Varun Aggarwal[2], Yashwant Kumar Singh[3], Ritu Dewan[4]

[1,2,3] *Student, Department of MCA, Sharda University, Greater Noida, Uttar Pradesh, India*
[4] *Asst. Professor, Department of Computer Science and Engineering, Sharda University, Uttar Pradesh, India*

Abstract - *The growth of the internet has led to the development of today's data-centric world where information can be exchanged from one part of the world to another with the click of a button. The most commonly used communication device is the mobile phone, with the ability of a portable computer. A large number of chatting applications have been developed that help people to communicate. The information typed inside these chatting applications must pass through the public infrastructure to reach the destination which is its most vulnerable phase of data transfer. A malicious hacker can gain access to messages or alter the messages thus compromising the data security. To maintain data integrity and confidentiality data encryption is used. Data encryption is used which convert our messages into encrypted form so that only people with the secret key can read them. This paper offers a study over the implementation of encryption techniques on Bargaining System which interacts between user and the seller to purchase the product by bargaining rate of the product. The system implements AES 128 bit key standard algorithm to encrypt the chatting application.*

Key Words: Encryption, Bargain, Confidentiality, Security, Cryptography, Chat application

1. INTRODUCTION

Cryptography is the technique that provides a safe way for applications to communicate over the internet where there are many adversaries present. In today's data-centric world chatting applications have become an indispensable tool. Any kind of information can be shared with only a click of a button using the power of the internet. Therefore, a chatting application needs to have a strong encryption method to prevent hackers from gaining access to the data, moreover, the penalty for encryption and decryption should be minimum. The proposed application used the AES 128 bit key algorithm for End to End Encryption for online Bargain system. The web application software developed is to provide e-commerce services to customers to shop the product online. In addition to that, the user can also initiate a chatting module to do bargaining. The online Bargaining System is a web application that implements the use of encryption to secure the chat between the seller and the customer. By this, end-user can easily bargain the product price with encrypted chat application with more secure and convenient

LITERATURE SURVEY

Ekta Agrawal et al. (2017) [1] This paper assists the use of the 8-bit code value of the alphabet and performs some simple calculations like logical NOT and simple binary division to produce the symmetric technique, which emphasizes improving the conventional method of encryption by using a substitution cipher. Substitution techniques have used the alphabet for ciphertext. In this symmetric algorithm, the plain text is initially converted into the corresponding ASCII code value of each alphabet. It uses various symmetric key algorithms, i.e., DES, RC2, RC4, and IDEA, which represent algorithms in detail and then propose a new symmetric key algorithm for encryption and decryption. This method is used for Short message communication can be sent securely using encryption techniques. The proposed approach is based on the number of characters in the message, and simple calculations and operations are performed to minimize the execution time.

Kuldeep Chouhan et al. (2013) [2] The imposed paper focuses on implementing an appropriate encryption technique in the chat area interface (CAI). A chaotic was chosen because it sends a short message and secure chat message. In this system, it is found that chat encryption prevents a message from an unauthorized person to view or modify a message. CAI has become more secure and reliable with the implementation of chaotic encryption. It executes SEC provided an opportunity to use the software design skills to build a secure chat server utilizing public-key encryption to send secure chat messages across the internet. It implements a new structural design for encrypting databases in networks, demonstrating what security features should be implemented to achieve a highly secured chat through a standalone system that can be efficiently implemented on any legacy system.

A. H. Ali et al. (2017) [3] The scope of the project is to secure chatting applications with end-to-end encryption for smartphones running on the Android operating system. It uses public-key cryptography techniques. The system generated the key pair and exchanged it to produce the shared key using the Elliptic Curve Diffie Hellman Key Exchange (ECDH), an asymmetric algorithm used to encrypt data. The application allows users to communicate via text messages, voice messages, and images. For text message encryption, the AES standard algorithm with a 128-bit key is used for security. The generated key (160 bits) was reduced to 128 bits in length by selecting the first 128 bits to be used by the AES algorithm. The proposed secure chatting

application provides confidentiality, privacy, and integrity. Users can be assured that others, including the service provider, will not able to read their messages. The exchanged data shared is only stored on the server, and nothing is stored in the physical memory of the phone. The AES standard is the algorithm used to encrypt text messages to provide greater security, and the RC4 algorithm is used to encrypt the phone's voice and image messages because it is one of the fastest encryption techniques for encrypting large amounts of data.

Shubhankar Chaudhary et al. (2020) [4] This system uses the RSA cryptosystem, which proposed a secure messaging transmission system that uses RSA encryption to provide a communication channel between the Client/Server environment. This research uses client/server architecture to secure client-to-client communication without allowing the server to decrypt the message. Here, The first layer of encryption is used between clients and the server, followed by a second layer of encryption between chat room clients. The RSA calculation has been used since its inception and serves as the foundation for a large number of cutting-edge encryption calculations to use 1024 bit encryption to send the messages.

T. M. Zaw et al. (2019) [5] In this research, the author proposed a technique for achieving confidentiality by using the six types of element-level encryption with AES and ECC encryption. This approach is used to store and retrieve database information in a more reliable manner. With ECC 256-bit key encryption provides confidentiality, authenticity, and availability contains roughly the same degree of protection as a 3072-bit key using RSA. For each element key in the database, the author uses 256-bit AES encryption for rows-level encryption, column-level encryption, and element-level encryption, which provides a good, effective, and efficient method for preventing unauthorized users from accessing the confidential data in the database.

Sridhar C. Iyer et al. (2016) [6] The author has proposed a hybrid technique for video encryption that uses both symmetric and asymmetric algorithms, resulting in a much more stable and fastest way of video encryption. This system split the video file into a different set of frames and apply the algorithm to each frame with symmetric ciphers for both encryption and decryption. ECC 160 bit keys are used in video conversion, while AES 128 bit keys are used for bit conversion. These keys are generated using the Peak Signal-to-Noise Ratio (PSNR), which visually compares grey-level video streams. PSNR is determined using the Mean Square Error (MSE), which illustrates lossless decryption by extracting the AES symmetric key and the ECC private and public keys from a Base64 format text file to generate the QR code to read the video.

2. EXISTING SYSTEM

- The existing shopping platforms where prices and goods are traded and auctioned off. e.g., traders4acause.org
- Customers do not get satisfaction from these types of websites.
- Some websites offer product duplication and other defective items, which discouraging customers from purchasing goods online.
- The system doesn't provide a traditional way of the bargain the product in online mode to negotiate the price of any product.

2.1 DRAWBACKS OF EXISTING SYSTEM

- They don't allow for product modifications, and even small changes are discouraged, and price bargaining isn't taken into account.
- Some e-commerce websites lose customers because they are not able to specify their requirements and needs.
- Difficulties encountered in satisfying consumers and their requirements, as customers may have different opinions on different goods.

3. PROPOSED SYSTEM

- The Proposed System Is To Study Endeavors To Understand Customer Satisfaction In Online Shopping.
- The Major Reason Is To Motivated Customer's Decision Making Process As Well As Inhibitions Of Online Shopping Using "Online Bargaining".
- To Reduce The Cost Of The Product We Make Bargaining Possible In Our Website By Creating A Group Of Consultant Who Will Interacting With Customer 24x7 Delivers At Valid Prices.

3.1 BENEFITS OF PROPOSED SYSTEM

- It reduce the cost of the product we make bargaining possible in our website by creating a group of consultants who will represent our website and can negotiate the prices that will satisfy the customers through chat application.
- Products can be altered or modified according to user's specification by using the command box where the customers can type their requirements.
- As an innovative idea, in our website we have a page called "Design Page" Where the customers can upload their designs. These designs will be selected and implemented by uploading their required product that will be share or given to the designer.
- The chatting system for bargaining the product will be encrypted using AES 128 bit key standard algorithm to encrypt text messages to provide

confidentiality, privacy, and integrity to secure chatting application between the user and seller.

4. METHODOLOGY AND IMPLEMENTATION

4.1 System Tools

Neat beans have been used as a development environment. Java, JSP, HTML was used as programming and scripting languages. The MySql has been used as a database management system. The WAMP and Apache Tomcat servers are used for the localhost. And CSS is used as a scripting method for layout and appearance.

4.2 Architecture of Bargaining Chat system (BCS)

The architecture of BCS is divided into two parts namely the sender and the receiver. The sender first needs to log in with its existing email and password to enter the chat system. If the user is not registered, he/she can create a new account by providing basic information such as name, email, and password for future reference. The user can also select a profile picture. After entering the chatting application the system will provide the list of users currently registered with the system. The user can also view whether they are offline or online. After selecting the person whom the user wants to communicate with, he/she can send a message.

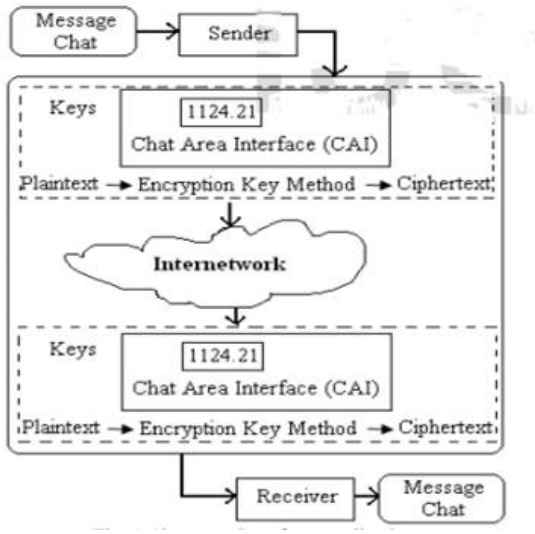

Fig -1 : Chat area interface application

4.3 Public key encryption

Public key encryption or Public key cryptography is a cryptographic technique which uses a pair of keys to implementing encryption and decryption. The algorithm for this kind of encryption is often based on mathematical one-way problems. The public key encrypts the plain text while the private key decrypts the ciphertext. This technique is based upon asymmetric key algorithms in which the public key is different from the private key and only the receiver with the private can decrypt the message, while others cannot. The main advantage of this scheme is that the sender does not have to manually send the symmetric key over an unsecured channel.

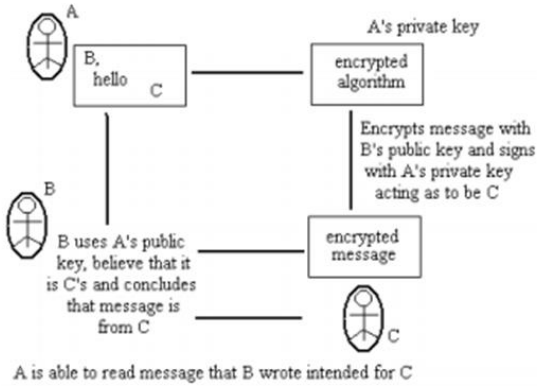

Fig-2 : Secure chat process

4.4 System Architecture

This system uses a centralized database model and there are three types of users: Administrator, User, Seller and it was designed according to requirement and specification.

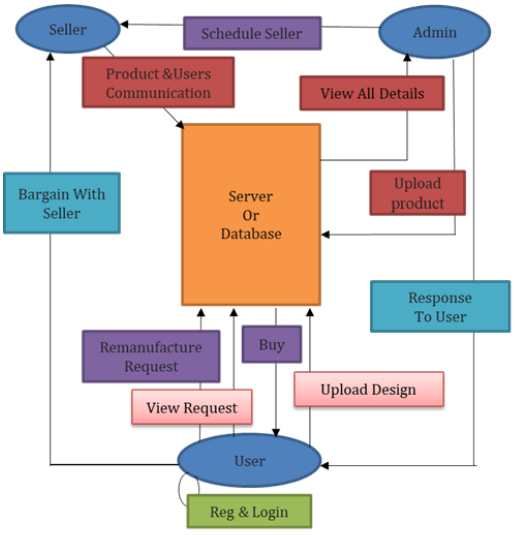

Fig-3 : System architecture

5. CONCLUSIONS

In this paper, we present a new approach for identifying changing consumer demands in the e-commerce industry that are more difficult to satisfy with existing goods, which provide less satisfaction and thus negotiating with consumers. In this user who is registered with his/her can upload their own design and requirements of their needs are being shown to both user and admin. It decreases the cost and time to evaluate their attraction towards the customer

and seller. By this technique, the customer will be fully satisfied by bargaining their required product. It is easy to use and it is less time-consuming. It satisfied the customer to buy a product with their own requirements to negotiate through bargain. The customer can upload their own design and it is placed in the marketplace. Customers can bargain by chatting with the seller. The chat list of user and seller have been encrypted with authorization by using cryptography techniques such as AES which uses asymmetric cryptography that can be used to authenticate the sender and receiver with both agreeing on a key from symmetric encryption.

REFERENCES

[1] E. Agrawal and P. R. Pal, "A Secure and Fast Approach for Encryption and Decryption of Message Communication," International Journal of Engineering Science and Computing (IJESC), vol. 7, no. 5, pp. 11481-11485, May 2017.

[2] K. Chouhan and S.Ravi, "Public Key Encryption Techniques Provide Extreme Secure Chat Environment," International Journal of Scientific & Engineering Research, vol. 4, no. 6, pp. 510-516, June 2013.

[3] A. H. Ali and A. M. Sagheer, "Design of Secure Chatting Application with End to End Encryption for Android Platform," Iraqi Journal for Computers and Informatics (IJCI), vol. 43, no. 1, pp. 22-27, 2017.

[4] S. Chaudhary, S. Dabas, V. Singh and M. S. Raj, "Cryptochat Encryption Messaging Application," International Research Journal of Engineering and Technology (IRJET), vol. 7, no. 5, pp. 2785-2788, May 2020.

[5] T. M. Zaw, M. Thant and S. V. Bezzateev, "Database Security with AES Encryption, Elliptic Curve Encryption and Signature," in 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), St. Petersburg, Russia, 2019.

[6] S. C. Iyer, R. Sedamkar and S. Gupta, "A novel idea of video encryption using hybrid cryptographic techniques," in 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2016.