International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Access Control and Privacy Preserving Dynamic Online Marketing Services System

AFRIN FATHIMA K A[1], JAYA N[2], RAJSREE ROY[3]

[1,2,3] Dept. of Computer Science and Engineering & Dhaanish Ahmed College of Engineering, Chennai

---

Abstract - Web based business has started to significantly impact upon the vehicle industry. The way through which individuals approach buying automobile items is of extraordinary concern. Often the clients need to travel far distances to receive automobile items and it isn't guaranteed to get the right quality. Our venture intends to help merchants as well as clients for trading vehicle items over utilizing a mechanized methodology. The site will direct the merchants to get into new production methods, analyze current market pace of various items, the complete deal and the acquired benefit from the sold items. The site constructs a stage for vendors to guarantee more noteworthy benefit through end client correspondence. The site will go about as a secure method for performing product-showcasing. This application will act as a way for the vendors to sell their items the nation over with some essential information about how to utilize the site. This undertaking permits seeing different items accessible and empowers clients to buy wanted items immediately by online installment.

***Key Words*:** Business, Vehicle, Merchant, Client.

I. INTRODUCTION

The vehicle spare parts business was designed with selling and buying organisations in mind. This system handles dealer, customer, product, sales order, and purchase order management. The trader is given a platform to automate record-keeping. This project's goal is to create a software application that will lessen the amount of manual effort required to manage orders, customers, dealers, and inventories. The goal of this project is to assist the administrator in running his business. Customer information can be kept in the database by the admin. There is no need to enter the customer's information again when he returns the next time. It is selectable from a list showing all customers.

II. EXISTING SYSTEM

The possibility that B2B internet business would profoundly change the way firms to carry on with work. B2B web based business commercial centres are on-line spaces were numerous purchasers and dealers can meet up in one exchanging local area and acquire adequate data to arrive at conclusions about whether to trade. Without examination of receipt or buy or client input, proprietor couldn't create their gain, rebate for the client, and so on. On the off chance that there is no a particularly sort of supporting configuration not accessible, proprietor couldn't tweak their administrations with clients.

Technique: Sequential Adjusting Algorithm

Disadvantage: It requires long investment to handle the information with less proficiency.

III. PROPOSED SYSTEM

E-market place offers customer responsibilities to the owner by giving feedback, purchase, and so on. However, owner run the business among the several competitions, user side reviews will help to upgrade their business service. Based on the user's feedback or owner wishes can change their product prices. These changes will reflect user view price list. By customizing product attributes, owners can get regular customers visits.

Technique: Naïve Bayes Algorithm, DES Algorithm

Advantage: It gives the valid solution with less time based on the data. We can be ready to compute the variables of information's.

IV. SYSTEM ARCHITECTURE

The system architect establishes the basic structure of the system, we proposed Naïve Bayes and DES algorithm in order to protect the privacy. Through the theoretical safety analysis and experimental evaluation the feasibility of our schemes has been validated, which is really a powerful supplement to existing data storage scheme.

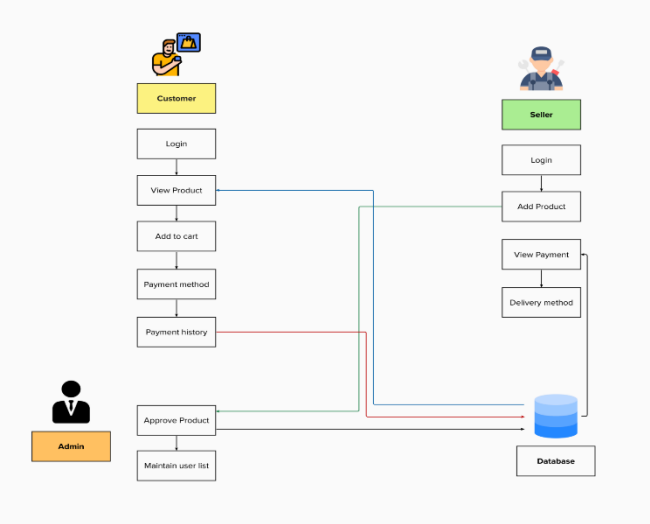

Fig -1: System Architecture

V. FUNCTIONAL DIAGRAM

1. **Application Server:** The application server hosts the B2B web application connecting the seller, customer and admin.
2. **Application Database:** The application database stores the application data such as- seller inventory, customer orders and admin data.
3. **Data Access Layer:** The data access layer handles the communication between the application server and the application database. It also ensures secure and reliable data access.
4. **Authentication:** This component ensures that only authorized users can access the application. It handles user authentication and authorization.
5. **Admin Panel:** The admin panel is the interface that the admin uses to manage the application. It handles seller management, order management and dispute resolution.
6. **Seller Panel:** The seller panel handles inventory management, receiving payments and product dispatch.
7. **Privacy Preserving Component:** This component protects the sensitive information including personal data and payment details using DES encryption. It ensures that access to the application data is controlled.

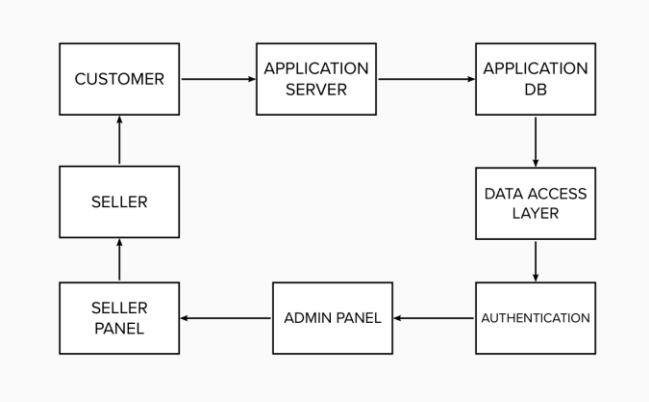

Fig -2: Functional Diagram

VI. SYSTEM IMPLEMENTATION

Data Encryption Standard is referred to as DES. It is possible to break the DES algorithm using certain equipment. A 56-bit key is used by the DES algorithm. The DES creates a block of 64-bit cypher text from a block of 64-bit plain text using this key. There are multiple phases in the DES process, and each step is referred to as a round. The number of rounds changes depending on what size key is being used. For instance, a 128-bit key needs 10 rounds, a 192-bit key needs 12, and so forth.

MODES OF OPERATION

1. Each 64-bit block in the Electronic Codebook (ECB) is separately encrypted and decrypted.

2. Cypher Block Chaining (CBC): Using an Initialization Vector (IV), each 64-bit block in CBC is dependent on the one before it.

3. Cypher Feedback (CFB): This technique uses the previous cypher text as input for the encryption process, which generates pseudorandom output that is then XORed with plain text to create the following cypher text unit.

4. Output Feedback (OFB): Similar to CFB, but with the prior DES encryption technique as the input.

5. Counter (CTR): A counter that has been encrypted is XORed with each plaintext block. The next block causes the counter to be increased.

STEPS OF DES:

1. Key Generation: A 64-bit encryption key is used to encrypt the data. However, the key is too large to be used directly in the encryption process, so it is first processed through a series of transformations to create 16 round keys of 48 bits each.

2. Initial Permutation: The input block of plaintext is rearranged according to a fixed permutation table.

3. Feistel Rounds: DES uses a Feistel network, which consists of a series of rounds that each operate on half of the input block using a different round key. Each round consists of four steps: expansion, substitution, permutation, and key mixing.

- Expansion: The right half of the block is expanded from 32 bits to 48 bits using a fixed permutation table.
- Substitution: The expanded half is divided into eight 6-bit chunks, each of which is substituted using a different S-box, which replaces the 6 bits with 4 bits according to a table.
- Permutation: The resulting 32-bit output from the substitution step is rearranged according to a fixed permutation table.
- Key Mixing: The resulting 32-bit output from the permutation step is XORed with the left half of the block, which is then swapped with the right half to begin the next round.

4. Final Permutation: After the Feistel rounds are complete, the left and right halves of the block are swapped one last time, and the output is rearranged according to a final fixed permutation table.

5. Output: The resulting block of cipher text is produced.

STEPS FOR ENCRYPTION:

The processes for data encryption entail a number of steps. It's them,

1. Split the plain text's 64 bits into two equally sized halves by permuting them.
2. Several rounds of operations will be performed on these 32-bit data pieces.
3. Use an XOR operation between the 48-bit compressed key and the extended right plain text.
4. S-box substitution is the next step once the resulting output is sent.

5. Next, combine the output with the left plain text using the XOR function, and then save the result in the right plain text.
6. Keep the left plain text copy of the first right plain text.
7. The following rounds of processes are issued for both the LPT and RPT halves.
8. Swap the data in the LPT and RPT at the conclusion of the previous round.
9. Use the inverse permutation process in the last step to obtain the cypher text.

STEPS FOR DECRYPTION:

The procedures for data decryption include the following steps:

1. The sequence of the 16 48-bit keys is reversed, making key 16 becoming key 1 and so on.
2. The cypher text is subjected to the encryption processes.

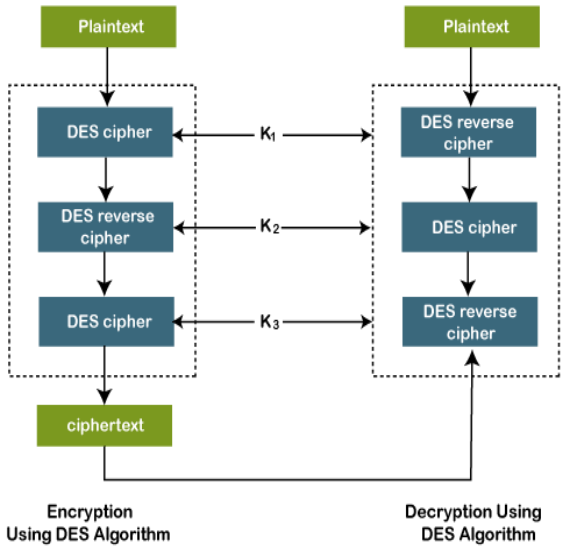

Fig -3: Encryption and Decryption in DES

APPLICATIONS:

1. It is used in random number generation.
2. It is deployed when not-so-strong encryption is needed.
3. It is used to develop a new form of DES, called Triple DES (using a 168-bit key formed using three keys).

NAÏVE BAYES ALOGORITHM:

1. Naive Bayes algorithm is a popular machine learning algorithm that is widely used in various applications including online B2B web apps. Its role in such apps is to perform classification tasks, where it is used to predict the likelihood of a given input belonging to a particular class or category.

2. The B2B web application receives input data (X) from the user or from some other source. This input data is then passed to the Naive Bayes classification model, which uses probabilistic calculations to predict the likelihood of the input belonging to a particular class or category.

3. Based on the predicted class (Y), the web application takes some action or produces some output. For example, if the input data is an email message and the Naive Bayes model predicts that it is spam, the web app can move it to the spam folder or mark it as spam.

4. Overall, the Naive Bayes algorithm plays a critical role in helping the online B2B web app automate decision-making processes and provide personalized experiences for users based on their input data.

5. Naive Bayes algorithm can be used in a B2B web application for access control and privacy preservation. In this example, we will be using Java, JSP, and Servlets to implement the algorithm for a web application that sells vehicle spare parts. The application has three user roles: customer, admin, and seller. The goal is to use Naive Bayes to predict the user role based on their login credentials.

Here are the steps for implementing Naive Bayes algorithm in this web application:

Data Collection: Collect data on the login credentials of each user in the system. For this example, we will be collecting data on the username, password, and role of each user.

Data Preprocessing: Preprocess the data by converting the login credentials into numerical values that can be used by the Naive Bayes algorithm. For example, we can assign a numerical value of 1 to the customer role, 2 to the admin role, and 3 to the seller role.

Training the Model: Train the Naive Bayes model using the preprocessed data. The model will use the login credentials to predict the role of each user.

Dashboard Pages: The algorithm is also implemented in the dashboard pages for customers, admin and sellers, where users can perform various actions such as querying the database for available spare parts.

Query Module: The algorithm is also applied in the module where users can search for spare parts based on their requirements. Depending on their role, they may have access to different types of queries.

Integration with Web Application: Integrate the Naive Bayes model with the web application by creating a Servlet that will handle the login requests. The Servlet will receive the username and password from the user, preprocess the data, and pass it to the Naive Bayes model. The model will predict the role of the user, and the Servlet will redirect the user to the appropriate page based on their role.

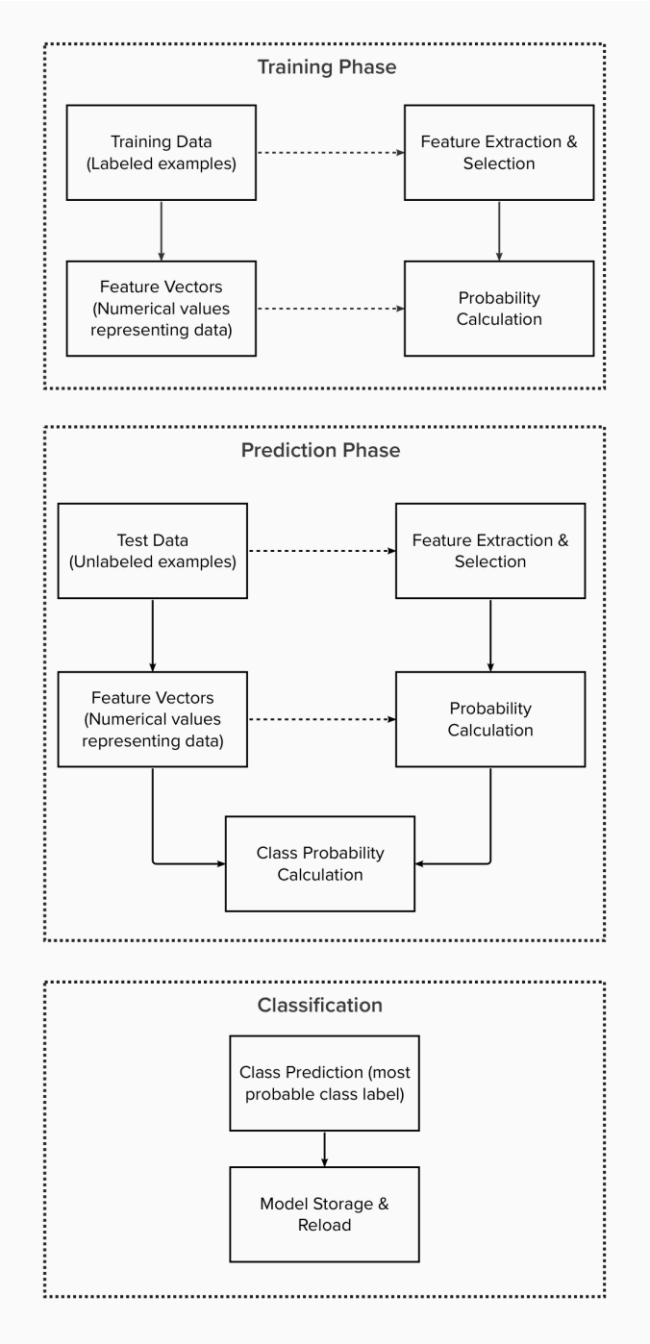

Fig -4: Naïve Bayes algorithm

ADVANTAGE OF NAÏVE BAYES ALGORITHM:

The following are some of the benefits of the Naive Bayes classifier:

1. It is simple and easy to implement.
2. It doesn't require as much training data.
3. It handles both continuous and discrete data.
4. It is highly scalable with the number of predictors and data points.
5. It is fast and can be used to make real-time predictions

VII. MODULES

The system module is categorized into three sub-modules namely,

- ✓ Module 1: Seller
  - ➢ Registration
  - ➢ Login
  - ➢ Add product
  - ➢ View Order
- ✓ Module 2: Customer
  - ➢ Registration
  - ➢ Login
  - ➢ View Product
  - ➢ Add to Cart
- ✓ Module 3: Admin
  - ➢ Seller Approval
  - ➢ Product Approval
  - ➢ Maintain User List
  - ➢ Reporting And Analysis

VIII. CONCLUSION

- E-Commerce has become an increasingly important source of competitive advantage for B2B companies.
- It enables them not only to decrease transactional costs and offer wide range of additional services, but also to enhance efficiency in collaboration with their customers and suppliers.
- Thus, the objective of this paper is to explore how industrial companies use B2B E-Commerce, how it enables their services and what are the main advantages.
- In the context of continuous increase of the services role in B2B markets and rapid development of information technologies, the paper turns high practical and theoretical importance for business environment.
- As it represents a review and summarizes a broad background on the topic, it could be chosen as a basis for further research on different strategies in B2B markets and analysis of the role of E-Commerce.
- The paper can also support companies in decision making on E-Commerce investments.

IX. FUTURE ENHANCEMENT

1. **Integration with IoT Devices:** One potential enhancement would be to integrate the application with IoT (Internet of Things) devices, such as sensors and trackers installed in vehicles, to provide real-time information on the status of the vehicle's parts. This could help customers make informed decisions about purchasing replacement parts and could also help sellers identify potential issues with their inventory.
2. **Integration with Social Media:** The application could be integrated with social media platforms to allow customers to share their purchases with friends and family. This could help promote the application and increase brand awareness.
3. **Blockchain Integration:** Blockchain technology could be integrated into the application to provide enhanced security

and transparency for transactions. This could help prevent fraud and increase trust between buyers and sellers.

X. REFERENCES

[1]. X. Liu, R. Ding, R. Lu, and B. Qin, "Privacy-preserving outsourced calculation on floating point numbers," IEEE Trans. Inf. Forensics Secur., vol. 11,no.11, pp.2513-2527, Nov 2016.

[2].V. C. Hu, T. Grance, D. F. Ferraiolo, and D.R. Kuhn, "An access control scheme for big data processing," in Proc. Int. Conf. Collaborative Comput.: Netw.Appl. Worksharing, 2014, pp. 1-7.

[3]. S.P. Koutsch, "Reference analysis of main concepts of relationship marketing", Vestrik St. Petersburg University, 4(32), 2003 pp.3-25.

[4]. D. Feeny, "Making business sense of the E-Opportunity", MIT Sloan Management Review , 42(2), 2001, pp.41-51.

[5]. R. Morgan and S. Hunt, "The commitment -trust theory of relationship marketing" ,Jounal of Marketing, 58, 1994, pp.20-38.

[6]. O. Burkacky, J. Deichmann, and J .P Stein, "Automotive software and electronics" ,vol. 56, no. 9,pp. 10-11, sept. 2019.

[7]. Y. Aviv and A. Pazgal, "Optimal pricing of seasonal products in the presence of forward-looking consumers," *Manuf. Service Oper. Manage.*, vol. 10, no. 3, pp. 339–359, 2008.

[8]. I. Bellos, M. Ferguson, and L. B. Toktay, "The car sharing economy: Interaction of business model choice and product line design," *Manuf. Service Oper. Manage.*, vol. 19, no. 2, pp. 185–201, 2017.

[9]. G. P. Cachon and R. Swinney, "Purchasing, pricing, and quick response in the presence of strategic consumers," *Manage. Sci.*, vol. 55, no. 3, pp. 497–511, 2009.

[10]. C. H. Chiu, H. L. Chan, and T. M. Choi, "Risk minimizing price- rebatereturn contracts in supply chains with ordering and pricing decisions: A multimethodological analysis," *IEEE Trans. Eng. Manage.*, vol. 67, no. 2, pp 466–482, 2020.

[11]. C. T.M., J. Zhang, andY. J. Cai, "Consumer-to-consumer digital- product exchange in the sharing economy system with risk considerations: Will digital-product-developers suffer?," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 50, no. 12, pp. 5049–5057, Dec. 2020.

[12]. R. H. Coase, "Durability and monopoly," *J. Law Econ.*, vol. 15, no. 1, pp. 143–149, 1972.

[13]. Hensssdel and A. Lizzer, "Adverse selection in durable goods markets," *Amer. Econ. Rev.*, vol. 89, no. 5, pp. 1097–1115, 1999.

[14]. I. Hendel and A. Lizzer, "Interfering with secondary markets," *RAND J. Econ.*, vpl. vol. 30, no. 1, pp. 1–21, 1999b.

[15]. S. Benjaafar and M. Hu, "Operations management in the age of the sharing. economy: What is old and what is new?," *Manuf. Service Oper. Manage.*, vol. 22, no. 1, pp. 93–101, 2019.