International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V70I3P220

Volume 70 Issue 3, 179-184, March 2022

Original Article

Feature Centric Data Augmentation Model-Based Mobile Commerce for Efficient Retail Growth using BlockChain

Rajesh Kumar .M[1], Venkatesh .J[2], Zubair Rahman .A. M. J. Md[3]

[1]*Full Time Ph.D. Research Scholar, Department of Information and Communication Engineering, Al-Ameen Engineering College, Karundevanpalayam, Erode, Tamilnadu. India.*

[2]*Associate Professor, Department of Management Studies, Anna University Regional Campus Coimbatore, Navavoor, Coimbatore, Tamilnadu. India*

[3]*Professor, Department of Information and Communication Engineering, Al-Ameen Engineering College, Karundevanpalayam, Erode, Tamilnadu. India.*

[1]rajeshkumrm@gmail.com, [2]drjvmba@gmail.com, [3]amjzubair@gmail.com

Abstract - *The recent trends in mobile commerce have been well studied and identified several approaches available towards the growth of the retail industry. However, the methods suffer to identify the efficient tool to hike the growth of the retail industry due to the poor management of data and security. Towards improving the performance of the retail industry, and efficient Feature Centric Data Augmentation Model (FCDAM) is presented in this article. The method has been designed for the development of mobile commerce performance and supports effective retail growth. The model adapts feature centric data augmentation techniques in producing efficient data for the user. The method maintains a number of traces of different user purchases and estimates feature centric popularity (FCP), feature centric retail support (FCRS) and feature centric augmentation support (FCAS) values. Using all these values, the model selects different products to the cart of the user at the mobile devices. Using the value of other measures, the value of product support (PS) has been measured to rank the products. Similarly, the augmented and purchase values are maintained using blockchain. Towards data security, the method uses feature centric data encryption and blockchain technique in improving the performance and growth of the retail industry. By incorporating the model, the performance of mobile commerce, as well as retail growth, is improved.*

Keywords - *BlockChain, Data Augmentation, Mobile Commerce, Retail Growth, FCDAM.*

I. INTRODUCTION

The recent development in communication and commercial technologies has opened the gate for their users to access their services through various tools and devices. In this way, the E-commerce systems enable the access of commerce services to purchase and sell or pay to be performed through a number of services. For example, the development in E-commerce has given the name M-commerce which enables the commerce process to be done through mobile devices. The user can visit the commerce website through their mobile phones, and there are M-commerce solutions designed dedicatedly for mobile devices. Using the services available, the user can purchase or sell their product whatever they want. They can visit and analyze the products available in the web forum, and they can purchase through the device they have. Purchasing the product itself is not enough for the system, but there are intelligence can be generated to support the growth of the retail industry.

The customer or the user would have different interests, and the system cannot identify directly. But you can infer the interest of the user by monitoring the product, what they purchase and what they visit. When the system maintains the log of user traces about their purchase and visits, the interest related products can be populated for the user. The mobile device has only limited space on the screen, so it is necessary to choose products to be shown on their display. By placing effective and excellent products, the sale of the product can be improved. However, the growth of the retail industry depends on how the product selection is performed.

Towards the placement of products on display, data augmentation techniques are used. When a user visits a product, it is necessary to populate the related products. But the selection of products from the available set of huge products is more important. The selection of products has been performed in several ways. It has been done according to frequency, popularity, price and so on. If the selection of

products is not effective, then it would affect the performance of the retail industry and growth. The data augmentation techniques help to obtain relevant and effective options to be populated for the users of the retail industry. By doing so, the user would get more interest and would stick to the forum towards purchasing a variety of products.

Like any environment, Mobile commerce is also subject to face variety of challenges in terms of security. The presence of malicious users would involve different threats, which leads to the performance degrade of the entire environment. Also, in terms of user perspective, there are higher chances of stealing the user's money. So, it is necessary to restrict the user from accessing data to which they have no access granted. To perform this, there are a number of approaches available, and each differs with the method of access restriction used, like profile-based, attribute-based, and service-based approaches. Similarly, there are a number of encryption schemes used in maximizing data security and faces a variety of challenges. To handle all these issues, and efficient feature centric data augmentation model is sketched in this article.

II. RELATED WORKS

There exist numerous techniques towards efficient mobile commerce to support the retail industry. This section details a set of approaches related to the problem.

An augmented reality (AR) based approach is presented in [1], which support the mobile environment to produce details of various products according to their purchase. It works in the client-server environment with virtual nature. To encourage the purchase of glasses online, an augmented try-on technology is described for the IoS environment. The method keeps track of user facial information and applies an SVM classifier for classification according to the SIFT feature extracted [2].

An AR model with IoT is described in improving the shopping experience in [3], which supports the purchase of IoT products towards data management, controlling various objects and exchange of information [3]. A DNN-HMM (Deep Neural Network – Hidden Markov Model) based data augmentation technique is presented in [4], which classify the speech according to the Random Forest technique. The method performs classification at multiple levels towards dysarthric speech.

Towards growing access of instant access of situated information, and AR function is presented named MANGO, an Austrian project. The model is developed to support the purchase of groceries, and the model populates a set of products like fruits and vegetables according to the user profile and their interest. The interest of the user has been identified using deep learning techniques [5]. Similarly, the data augmentation problem is approached with a Deep neural network is presented in [6], which works over label information and consider the sparse data. It combines both vocal tract length perturbation (VTLP) and stochastic feature mapping (SFM) schemes with DNN.

The problem of data authentication in the cloud is handled with the AES encryption technique in [7], which restricts the malformed access of data in the cloud. Similarly, a novel secure encryption scheme is presented in [8], which uses multiple coding levels in maintaining the confidence of data with DNA encryption. The method achieves higher data confidentiality by using the AES scheme. A hybrid homomorphic encryption scheme is presented in [9], which works based on the GM approach. The method adds RSA with multiplicate homomorphic. The method achieves higher resistance against various attacks.

The varying size of encryption schemes is presented in [10], which selects the different sizes of encryption techniques like 128, 192 and 256bits according to the size of data. Similarly, in [11], different security schemes of steganography, data encryption standards, compression techniques and data splitting techniques are combined to improve data security.

A Cipher-text Policy Attribute-Based Encryption (CP-ABE) has been presented in [12], which enforce access control on encrypted data in maximizing data confidentiality in the cloud. The method is capable of facing different attacks. To maintain the data security, and data encryption scheme is presented by evaluating the performance of various approaches according to different key sizes being used [13]. The method considers RSA, AES, DES and so on for evaluation. A hybrid encryption scheme is presented to perform data sharing in a cloud environment where the banking data are stored. The method combines AES and Byte Rotation Encryption schemes [14].

A Key-Aggregate Proxy Re-Encryption scheme is sketched in [15], which combine key aggregate and proxy re-encryption schemes. The method uses constant key size for both approaches. Similarly, in [16], a ciphertext retrieval scheme is presented, which index the text using the Porter stemming algorithm and use blowfish to perform data encryption. The authentication is performed with ECC and public key. To handle the security in routing, a multi-layer parameter orient scheme is presented, which uses a User-Controllable Identification scheme and consider only the permitted devices to maintain routing information. A trust-based secure routing protocol (SCORES) is discussed in [18], which consider the energy of nodes and topology of the network in routing. The load balancing is achieved by considering node position and estimating the trust measures to find suitable nodes to perform data routing. An RPL routing scheme is sketched in [19], which maintains a set of keys in the table and consider IoT devices to perform routing. SISLOF approach distributes the keys initially, and

IoT devices are authenticated to involve in data transmission. A crowdsource routing protocol is presented in [20], which uses the result of data analysis and demand analysis to perform efficient routing.

All the methods described above suffer to achieve expected performance in retail market growth and suffer from poor accuracy. This increases the requirement of developing an efficient scheme for the problem.

III. PROPOSED METHOD

The proposed feature centric data augmentation model maintains the traces of products and their metrics like cost, size, quality, grade and so on. The model has been designed to provide service access to mobile users. The method produces product results according to the user query, which has been extended in multiple levels according to the product being purchased and viewed. Also, the method generates the product list using the feature centric data augmentation technique where the product selection on the cart is performed by measuring different feature centric popularity (FCP), feature centric retail support (FCRS) and feature centric augmentation support (FCAS) values. Using all these values, the model selects different products to the cart of the user at the mobile devices. Using the value of other measures, the method computes the value of product support (PS) which has been used in ranking the products. Similarly, the augmented and purchase values are maintained using blockchain, where the method generates blocks by encrypting features according to service and features. The detailed approach is presented in this section.

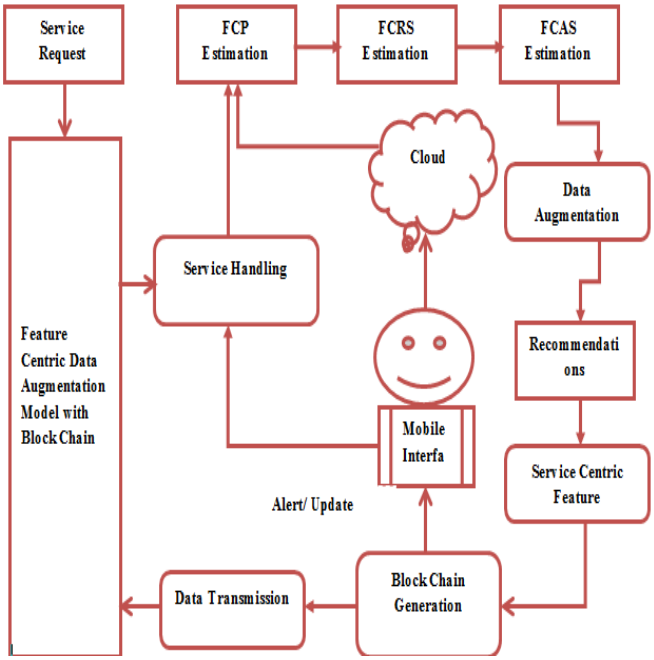

Fig. 1 Architecture of Proposed FCDAM-BC Model

The functional architecture of the proposed FCDAM-BC model has been pictorially represented in Figure 1 and shows the functional components, which are described in detail in this section.

A. Service Handling

The service requests generated by different mobile clients are received by the service handling algorithm. From the service request, the method identifies the service being requested, and according to the service being claimed, the method identifies a set of services and populate them to the user. From the selected service, the method produces a result to the user by accessing the service. Similarly, the result being obtained has been populated by the user. From the set of products generated, the user has been given a set of products as a result. Further, the product selection is enhanced by performing feature centric data augmentation scheme. Again the recommendations are generated according to the product support measured by the data augmentation technique. The recommendations are applied with a data encryption scheme and adapted to the blockchain, and has been transmitted to the mobile user. The mobile user can fetch the blockchain and get the results accordingly.

B. Feature Centric Data Augmentation Technique:

The feature centric data augmentation technique keeps track of a set of products in a product taxonomy. The taxonomy of any product contains different features like colour, flavour, size, price, movement and so on. So, the augmentation technique finds the products from the mobile user's screen and, based on that, the augmentation technique finds a set of related products. For each of the products, the model estimates feature centric popularity (FCP), feature centric retail support (FCRS) and feature centric augmentation support (FCAS) values. The value of FCP is measured based on the popularity of any product, which is being computed according to the frequency of sales. Similarly, the value of FCRS is measured according to the sale of the product being identified according to the number of times it has been purchased by different users. Similarly, the method computes FCAS value according to the variety of products the retail centre has. Using all these values, the method computes the value of product support (PS). Based on the value of PS, the method ranks the products and generates recommendations for the user.

Algorithm:

Given: Product Taxonomy PT, Purchase Trace PuT, Request R

Obtain: Recommendations Rec.

Start

Read PT and PuT, R.

Identify product type requested Ptr.

$$\text{Ptr} = ProductType \in R \quad (1)$$

Find list of products Plist.

$$\text{Plist} = \sum_{i=1}^{size(PT)} PT(i).\text{Type} == \text{Ptr} \quad (2)$$

For each product p

Compute Feature Centric Popularity FCP.

$$FCP = \frac{\sum_{i=1}^{size(PuT)} PuT(i) \in p}{size(PuT)} \quad (3)$$

Compute Feature Centric Retail Support FCRS.

$$FCRS = \frac{\sum_{i=1}^{size(PuT)} PuT(i) \in p \&\& PuT(i).User = U}{size(PuT)} \quad -(4)$$

Compute Feature Centric Augmentation Support FCAS.

$$FCAS = \frac{\sum_{i=1}^{size(PT)} PT(i) == P \&\& PT(i).NPT}{\text{Total No of Product Types}} \quad (5)$$

Compute Product Support $PS = \frac{FCP \times FCRS}{FCAS}$

End

Recommendations = Rank Products according to Product Support.

Stop

The above-discussed algorithm shows how feature centric data augmentation is performed. The method estimates the value of FCAS, FCP and FCRS to measure PS value. Based on the value of PS, the method performs recommendation generation and support the growth of the retail industry.

C. Service-Centric Feature Encryption:

In this stage, the method gets the result of recommendations from the model. From the recommendations, the method performs data encryption based on the service metrics. The model maintains different service taxonomy, and for each taxonomy, the method has the information about the service and scheme with key sets. Using the above information, the method would select a random scheme, key to encode the features or results of the service access. Such encrypted data has been given to the user through blockchain.

Algorithm:

Given: Service Taxonomy ST, Data D, Scheme set Ss, Key Set Ks.

Obtain: Block Chain BC

Start

Read ST, D, Ss, ks.

Generate random no $R = \int_{i=1}^{size(ss)} Random(i, ss)$ (6)

Split Data into R number of Blocks as Db = Split(D, R)

Blockchain BC= generate blockchain with R number of blocks.

For each block b

Random R1 = $\int_{i=1}^{size(ss)} Random(i, ss)$ && Service=S Contained in ST. (7)

Cipher text CT = Data encryption (b,ss(R1),Ks(R1))

Add to block in the chain BC(b)=CT.

BC(Hash) = R1#S

End

Stop

The above-discussed algorithm represents how service-centric feature encryption is performed by choosing the unique key and scheme from the scheme set as well as belongs to the service present in the taxonomy. Generated blockchain has been sent to the user, who can decrypt the data present in the blocks according to the hash code available. The first number is the index of the key and scheme to be used where the service is presented in the last. The decrypted data has been used to improve the performance retail industry.

IV. EXPERIMENT

The proposed Feature Centric Data Augmentation Model with BlockChain (FCDAM-BC) has been implemented and evaluated for its performance. The model has been evaluated for its performance by considering the different number of users in the environment and the number of logs present in the purchase trace.

Table 1. Details of Evaluation

Parameter	Value
Number of Users	**5000**
Number of Products	**500**
Total Records	**1 million**
Tool	**Advanced Java**

The metrics used for the performance evaluation are discussed in Table 1. The novel FCDAM_BC approach has produced higher performance in a variety of parameters and compared with the results of other methods.

Table 2. Analysis of Data Security

	Performance on Data Security		
	100 Users	**205 Users**	**500 Users**
THE	72	74	78
CPABE	76	79	82
Blowfish-ECC	79	83	86
ABBR	82	87	89
FCDAM_BC	87	92	96

The efficiency of methods in achieving higher data security has been measured under the varying users in the environment. In all the cases, the proposed FCDAM-BC approach has produced higher performance in data security than other approaches.

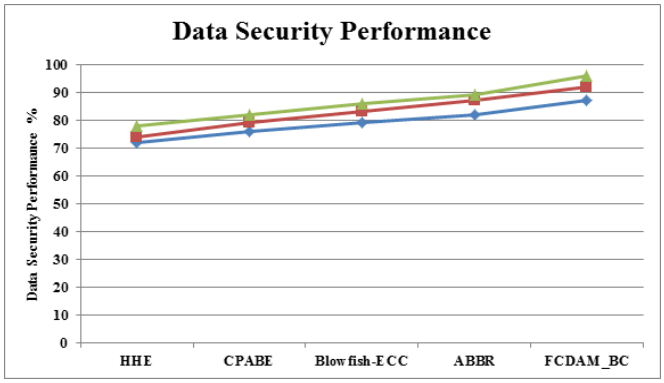

Fig. 2 Performance on data security

The efficacy of data security produced by different algorithms have been measured and compared in Figure 2. The proposed FCDAM-BC model has produced good efficiency in data security than other techniques considered in all the cases.

Table 3. Performance analysis on data augmentation

	Performance on Data Augmentation		
	100 Items	**250 Items**	**500 Items**
SDM	72	74	78
DNN-HMM	74	77	82
VLTP	79	83	86
MANGO	82	87	89
FCDAM-BC	87	92	96

The efficacy of data augmentation produced by different approaches is measured at the constraint of different users in the environment. In each case, the proposed FCDAM-BC has produced higher accuracy and performance than other approaches.

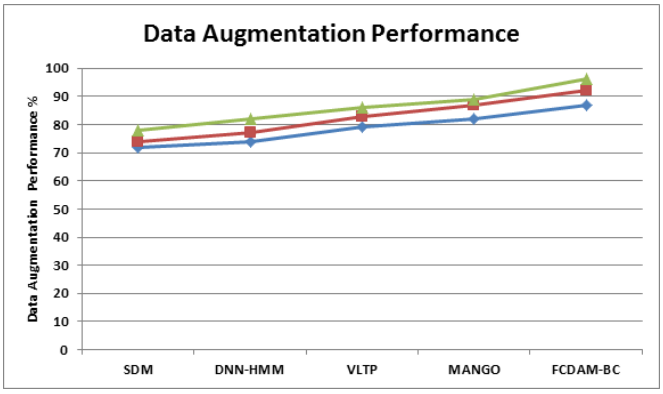

Fig. 3 Performance on data augmentation

The data augmentation performances produced by various approaches are measured at the presence of a different number of items in the basket than the rest of the methods. In each case, the proposed FCDAM-BC has produced maximum performance than any other technique.

Table 4. Performance analysis on throughput

	Performance on Throughput		
	100 Items	**250 Items**	**500 Items**
SDM	67	72	76
DNN-HMM	72	75	79
VLTP	75	79	82
MANGO	78	83	87
FCDAM-BC	87	92	96

The efficacy on throughput has been measured and presented in Table 4. The proposed FCDAM-BC algorithm has achieved a higher throughput ratio than other techniques.

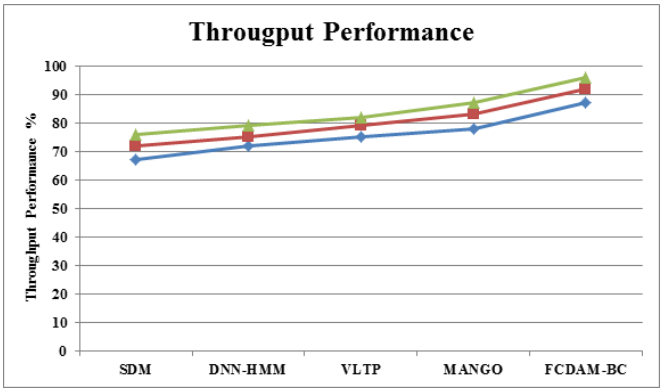

Fig. 4 Performance on throughput

The throughput performance introduced by different algorithms have been measured and presented in Figure 4. The proposed MFDAM-BC algorithm has achieved a higher throughput ratio than other techniques.

V. CONCLUSION

In this paper, an efficient feature centric data augmentation model with blockchain (FCDAM-BC) is presented. The model receives the user request and finds the service being requested. With the service identified, the method fetches the features and applies feature centric data augmentation model, which computes different measures like feature centric popularity (FCP), feature centric retail support (FCRS) and features centric augmentation support (FCAS) values. Using them, a product support value is measured to rank the products and generate a recommendation. Further, the method applies a service-centric feature encryption technique that selects different schemes and keys for different blocks of data according to the service taxonomy. Finally, the blocks generated are added to the blockchain, and the hash code is generated by combining the index of the key or scheme, which is a random number and the service name. The method improves the performance on data security throughput than other methods with higher data augmentation performance.

REFERENCES

[1] Boping Zhang, Augmented virtual reality glasses try-on technology based on iOS platform, EURASIP Journal on Image and Video Processing , (2018).

[2] Dongsik Jo & Gerard, IoT + AR: pervasive and augmented environments for Digi-log shopping experience, Springer, Human-centric Computing and Information Sciences, (2019).

[3] Bhavik Vachchani, Data Augmentation Using Healthy Speech for Dysarthric Speech Recognition, Conference on Interspeech, (2018).

[4] Georg Waitner, MANGO - Mobile Augmented Reality with Functional Eating Guidance and Food Awareness, An Interactive Tool for Speed up the Analysis of UV Images of Stradivari Violins ,425-432.

[5] Xiaodong Cui; Vaibhava Goel; Brian Kingsbury, Data Augmentation for Deep Neural Network Acoustic Modeling: IEEE/ACM Transactions on Audio, Speech, and Language Processing, 23(9) (2015).

[6] N. Surv, Framework for client side AES encryption technique in cloud computing, IEEE (IACC), (2015) 525-528.

[7] N. Mohammed and N. Ibrahim, Implementation of New Secure Encryption Technique for Cloud Computing, IEEE (ICCISTA), (2019) 1-5.

[8] Z. H. Mahmood and M. K. Ibrahim, New Fully Homomorphic Encryption Scheme Based on Multistage Partial Homomorphic Encryption Applied in Cloud Computing, IEEE (AiCIS), (2018) 182-186.

[9] G. Raj, R. C. Kesireddi and S. Gupta, Enhancement of security mechanism for confidential data using AES-128, 192 and 256bit encryption in cloud, IEEE (NGCT), (2015) 374-378.

[10] K. Rani and R. K. Sagar, Enhanced data storage security in cloud environment using encryption, compression and splitting technique, IEEE (TEL-NET), (2017) 1-5.

[11] Y. S. Gunjal, M. S. Gunjal and A. R. Tambe, Hybrid Attribute Based Encryption and Customizable Authorization in Cloud Computing, IEEE (ICACCT), (2018) 187-190.

[12] V. Sreenivas, Performance Evaluation of Encryption Techniques and Uploading of Encrypted Data in Cloud, IEEE (ICCCNT), (2013) 1-6.

[13] P. More, S. Hybrid Encryption Techniques for Secure Sharing of a Sensitive Data for Banking Systems Over Cloud, IEEE (ICACCT), (2018) 93-96.

[14] W. Chen, Efficient Key-Aggregate Proxy Re-Encryption for Secure Data Sharing in Clouds, IEEE (DSC), (2018) 1-4.

[15] S. Mudepalli, V. S. Rao and R. K. Kumar, An Efficient Data Retrieval Approach using Blowfish Encryption on Cloud Ciphertext Retrieval in Cloud Computing, IEEE (ICICCS), (2017) 267-271.

[16] P. L. R. Chze and K. S. Leong, A Secure Multi-Hop Routing for IoT Communication, IEEE (WF-IoT), (2014) 428-432.

[17] G. Hatzivasilis, I. Papaefstathiou and C. Manifavas, SCOTRES: Secure Routing for IoT and CPS, IEEE Internet of Things Journal, 4(6) (2017) 2129-2141.

[18] A. E. Hajjar, G. Roussos and M. Paterson, Secure routing in IoT networks with SISLOF, Global Internet of Things Summit (GIoTS), (2017) 1-6.

[19] Shengli Mao, Crowd Cloud Routing Protocol Based on Opportunistic Computing for Wireless Sensor Networks, EURASIP Journal on Embedded Systems, 2016(1) (2016) 1.

[20] Uma Khemchand Thakur, QoS Aware Cloud-Based Routing Protocol for Security Improvement of Hybrid Wireless Network, Machine Learning Research, 4(1) (2019) 21-26.