International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

A Secure Framework for Cloud-Based Storage of E-Commerce Transaction Data using Bitlock Encryption

[1]*Naresh Kumar Reddy Panga and [2]R. Hemnath

[1]Engineering Manager, Virtusa Corporation, New York, NY, USA
[2]Nandha Arts and Science College, Erode, India.

Received 01 Aug 2021, Accepted 25 Aug 2021, Available online 30 Aug 2021, **Vol.11, No.4 (July/Aug 2021)**

Abstract

The e-commerce ecosystem has the secure handling of transaction data in the cloud to ensure that sensitive information of customers is at bay. With the increasing volume of data and growing threats at the cyber level, it remains one of the biggest challenges in ensuring integrity and scalability in data for e-commerce platforms in the modern world. This study develops an efficient secure and scalable framework for handling transaction data related to e-commerce in the cloud using modern encryption techniques and control access mechanisms. The methodology collected data and pre-processing it, followed by BitLocker encryption, role-based access control (RBAC), and cloud storage for storing secured data management. Results prove that encryption time varies linearly with file size from 1000 ms by 2MB to 9000 ms by 20MB, while system load has a powerful effect on latency, raising 120 ms at load 1 to 460 ms at load 7. This research exhibits that there is a possibility to guarantee safe and scalable data storage while also optimizing system performance for cloud-based e-commerce environments.

Keywords: *E-Commerce Transactions, Cloud Storage, Data Security, BitLocker Encryption, Role-Based Access Control (RBAC).*

1. Introduction

Nowadays, with the booming development of e-commerce and the steady increase in online transactions around the globe, securing sensitive transactional data has become the biggest concern [1] [2]. Customers now hand over their personal and financial information along with credit card details and addresses, which, if exposed, can create greater privacy invasion and financial fraud situations [3] [4]. As a result, while businesses are shifting their infrastructure from local organization efforts to cloud computing to achieve better scalability and cost-effectiveness, the need for security concerning cloud transactions becomes more critical [5] [6]. Cloud computing presents unique security challenges resulting from its distributed nature, shared resources, and remote access [7] [8]. In upholding the trust of users, ensuring the confidentiality, integrity, and availability of data during its collection, storage, and retrieval is paramount [9] [10]. Secure management of e-commerce transactions in the cloud creates a perfect environment for preventing unauthorized access as well as cyber threats; as well, it improves compliance with regulations that call on regulations such as GDPR, PCI-DSS, and HIPAA [11] [12].

*Corresponding author's ORCID ID: 0000-0000-0000-0000
DOI: https://doi.org/10.14741/ijcet/v.11.4.10

The framework proposed, therefore, answers the escalating demand for robust security from inception through operational processes with all steps: data lifecycle [13] [14].

Critical e-commerce applications were located in the traditional data centres with very few outside exposures [15] [16]. Now with cloud-based architecture, multiple endpoints have been introduced, making such systems vulnerable to a whole new array of threats such as data breaches, malware attacks, and insider threats [17] [18]. On the flip side, customers expect that these services will be available all the time from anywhere on any device, which demands an underlying system that is always available and secured [19] [20]. A sound security setup protects consumer data, keeps businesses rolling, and bolsters service trustworthiness [21] [22]. Further investments on secure architecture repay themselves over the long term, especially in avoiding costs associated with data breaches and prosecution fines [23] [24]. The varied means are encryption, access control, and monitoring, which will help combat intelligent threats [25] [26]. In light of this, there is currently a need to design a purpose-built framework that integrates cloud-native features together with the best practices in security [27] [28]. The here-under study addresses the tonsure and scalable cloud-based solution to make e-commerce transactions, from beginning to end, secure and hassle-free [29] [30].

There are several existing methods for ensuring secure transactions in the cloud during e-commerce with varying degrees of success [31] [32]. Most of these techniques, such as Advanced Encryption Standard (AES), RSA encryption, etc., are usually carried out by encrypting the data from transmission to storage [33] [34]. Some other measures include access control mechanisms such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), which have been used to limit unauthorized access [35] [36]. Some frameworks also use Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols for securing data while transiting [37] [38]. However, as common procedures, they tend to become very incomplete in terms of end-of-life and very real-time auditing [39] [40]. Firewalls and intrusion detection systems (IDS) typically have a basic network-level security application, but they do not hold up against application-level protection [41] [42]. Most of these forms are in isolation and do not provide a global measure of visibility and control [43] [44]. They are not able to scale accordingly with growing complexities and ever-increasing traffic of an e-commerce cloud platform [45] [46].

The suggested framework tackles the weaknesses that are there in the existing system by proposing integrated and layered security models specific for cloud-based e-commerce environments [47] [48]. It uses BitLocker for the disk-level encryption of data so that even if physical access to the drives is malicious, data at rest is still protected [49] [50]. The framework uses Role-Based Access Control (RBAC) as an access control system against traditional ones to allow dynamic management of user privileges with an emphasis on specific job functions to minimize unauthorized access [51] [52]. Data pre-processing activities are carried out to check, validate, and clean transaction data before encryption; thus, improving data quality and reducing vulnerabilities [53] [54]. It also keeps secured data in cloud-native storage solutions with strictly configured access policies, allowing scalability with security [55] [56]. Real-time monitoring and auditing mechanisms are always present to detect any suspicious activity to maintain day-to-day compliance [57] [58].

The novelty is in end-to-end security workflow proposed for the modern e-commerce managers based on the cloud [59] [60]. It is the only approach, which fosters BitLocker encryption, RBAC, secure storage, and continuous monitoring, into a single holistic framework. Whereas fragmented solutions are meant to safeguard only pre- and post-processing, this one take care of the complete data cycle-from collection and pre-processing to storage and access [61] [62]. It includes disk-level encryption (BitLocker, which is rarely used in cloud-based e-commerce contexts) for an added layer of defences that traditional application-level encryption misses [63] [64]. Further, by very much integrating role-based controls, the system mitigates internal threats and minimizes human error. The solution is scalable and flexible for enterprises from small ones to big. This holistic approach thus builds confidence in e-commerce platforms while setting a precedent for the future cloud security architecture for the industry [65] [66]. The framework not only secures transactional processes but builds a very strong foundation for compliance and growth.

2. Literature Review

[67] This study integrates Artificial Intelligence and Machine Learning in cloud-based CRM systems for predicting customer churn, where Random Forest Classifier has achieved 92.5% accuracy, talking about the strength of ensemble methods. [68] It presents a Cloud-Based Healthcare Risk Prediction and Surgery Monitoring System with the aid of IoT, Cloud computing and Machine Learning that provides 93% accuracy in real-time patient risk prediction, although data security challenges remain. [69] A safe, scalable cloud-based framework for collection of healthcare data was developed using KNN, Salsa 20 encryption and Transport Layer Security with nearly 100% security strength but still performance problems persist as the load of the system increases.

[70] The present paper talks about a hybrid model: LSTM-Attention which has been optimized through Bayesian Optimization for improving disease prediction accuracy and efficiency in cloud-based healthcare systems with an accuracy of 98.5%, reduced execution time, and scalability to support real-time processing. An AI-Blockchain hybrid model is also introduced to enable decentralized authentication and scalable blockchain transactions for smart manufacturing, supported by AI-driven intrusion detection to mitigate security concerns in IIoT systems. [71] This research encompasses a predictive model for hospital readmission born out of transformers and the attention mechanisms lying on cloud infrastructure for real-time processing, achieving accuracy of 88%, as well as good patient outcomes. [72] It introduces a framework for optimising traffic management as well as cloud security in software-defined networks (SDNs) with a set of deep learning models such as Gated Recurrent Units (GRU) to cater to the requirements of traffic classification, abnormality detection, attack prevention, and provide top-notch performance in terms of both accuracy and F1 score. In addition, an Integrated Cloud Software Network Based on Blockchain was developed for secure ISP federation with SDN and Blockchain to provide data security, network management, and resource optimization.

The research proposes a new innovative platform using Convolutional Neural Networks (CNNs) and Autoencoder for intrusion detection and alert correlation in cloud environments with a threat detection rate of 95% and better than traditional methods [73]. This serves as a reference to an integrated security framework for e-commerce applications based entirely on the cloud, using

blockchain, biometrics, encryption, and zero-trust architectures. This framework boasts an accuracy level of 99.50% in the fraud prevention section and 96% in authentication [74]. The Health Fog system represents a breakthrough in deep learning, IoT, fog, and cloud computing that enables the early diagnosis of infectious and cardiovascular diseases, thereby significantly improving outcomes for patients through the efficient processing of data and monitoring in real-time.

[75] Herein, it is proposed to enhance the scalable health care solution by integrating Fog Bus with cloud federation frameworks, solving challenges such as latency, energy consumption, and data management in IoT-based health care systems. Improves the current real-time processing, security, and resource allocation of the system in comparison with traditional systems when it comes to urgent health care situations. This study also investigates the effect of mobile internet access and financial inclusion on the economic development of rural Africa through data-driven analysis assessing how these affect rural economic outcomes particularly in e-commerce.

3. Problem Statement

The proposed framework comes to address some limitations faced by existing solutions for securing e-commerce transactions in the cloud. Some systems rely only on application-level encryption such as AES without being sensitive to disk-level encryption for the protection of their data. Traditional access control mechanisms such as DAC and MAC do not suit dynamic role-based environments due to their rigidity. There is often limited monitoring and auditing, thus preventing timely detection of unauthorized access or suspicious behaviour. sensitive data are often not masked or validated, so low data quality gives room for data exposure. Many existing frameworks are very fragmented and do not provide end-to-end security, leaving gaps in data collection, storage, and access. The proposed framework solves these problems by combining disk encryption using BitLocker with dynamic role-based access control (RBAC), secure cloud storage, data pre-processing, and continuous monitoring.

4. Proposed Methodology

For ensuring an adequate level of protection for the e-commerce transaction data being handled on the cloud, a very systematic multilevel framework has been created as shown in Fig. 1. The very first step starts with Data Acquisition, where transactional details, such as orders and payments, are being gathered or harvested from the e-commerce applications. This data is then passed for Data Pre-processing, a stage to treat issues such as missing values and duplicate entries, thus improving data quality. Afterwards, the cleansed data is encrypted using BitLocker so as to strengthen data protection in a disk-level sense. Access to encrypted data is controlled through an RBAC model, resulting in permissions granted based on user roles. The secured data can then be presented in Cloud Storage for scalable and secure data hosting. Finally, these Performance Metrics are evaluated to judge the efficacy and efficiency of the whole framework. Hence, each block in the diagram brings towards building a robust end-to-end data security mechanism.

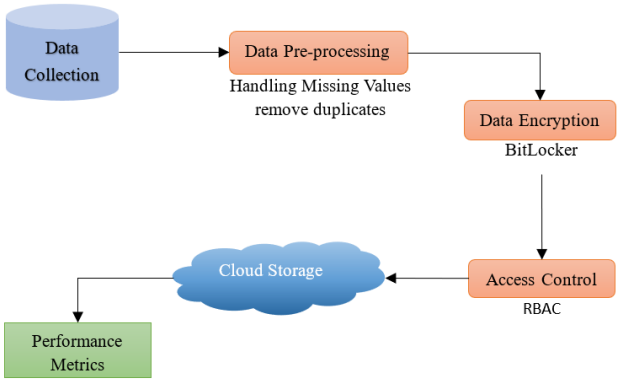

Figure1: Data Processing and Security in Cloud Storage

Data collection

Data collection involves beginning transactions in the way that they were collected from several e-commerce sites. This would comprise any customer details and purchase histories, payment, and shipping records. This is crucial that the accurate and complete data are adhered to in that they would serve as the foundation for further processing and security measures. It avoids any such real-time streaming while focusing on the secure handling of data at batch levels. Data collected would be held temporarily in a secure staging area prior to going through pre-processing. This phase ensures that only relevant and valid transactional records are passed along to the next stage of the framework.

Data Pre-processing

Data pre-processing occupies a very important step in the frame which makes the transactional data more quality, consistent, and secure, which means enriching and protecting the transactional data before it goes to encryption in storage. This includes some steps such as dealing with missing values, eliminating duplicates, and standardizing data formats. Below is a detail explanation of what each step entails.

Handling Missing Values

Incomplete data gives rise to inconsistencies and may affect the correctness of the analysis. One of the most common techniques is:

- *Mean Imputation*

It is nothing but means a replacement of missing values or null values by the mean of the attribute is given in equation (1).

$$x_{\text{new}} = \frac{1}{n}\sum_{i=1}^{n} x_i \quad (1)$$

where x_i are the existing values and x_{new} is the value used for replacement.

- *Mode Imputation:*

Replace missing values with the most often occurring value is given in equation (2).

- *Forward Fill or Backward Fill:*

$$x_t = x_{t-1} \text{ (forward fill) or } x_t = x_{t+1} \text{ (backward fill)} \quad (2)$$

Removing Duplicates

The duplicated records add to the amount of storage that is utilized and lower the efficiency of processing. The duplication of records is detected by defining a unique combination of fields:

If $D(i) = D(j)$ for all key fields, delete $D(j)$
Where $D(i)$ and $D(j)$ are duplicate records.

Data Encryption using BitLocker

BitLocker is a full-disk encryption mechanism developed by Microsoft for protecting data at the volume level against any unauthorized access. In the proposed framework, before the transactional data is sent to cloud storage, we will protect it with BitLocker. BitLocker uses the Advanced Encryption Standard (AES) with a key length of either 128 bits or 256 bits. This is a symmetric-key exchange, wherein the same key is used for both encrypting and decrypting. In an unreadable manner, data so stored in the disk can only be accessed by users or processes with the correct decryption key. The AES basic mathematical operation includes a combination of substitution, permutation, and mixing operations on data blocks, which are 128 bits in size.

The AES encryption process used by BitLocker follows several key steps, mathematically defined as:

1. SubBytes

Each byte of the block is replaced using a predefined S-box as given in equation (3).

$$S(a) = \text{S} - \text{box}[a] \quad (3)$$

2. ShiftRows

Bytes from the block matrix in each row cyclically shift.

3. MixColumns

Each column of the block is mixed using matrix multiplication in Galois Field $GF(2^8)$:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

4. AddRoundKey

The result is XORed with the round key derived from the encryption key is given in equation (4).

$$\text{Block}_{\text{new}} = \text{Block}_{\text{prev}} \oplus \text{RoundKey} \quad (4)$$

Access Control Using Role-Based Access Control (RBAC)

E-commerce transaction data stored in the cloud are encrypted and access control-based by RBAC. In this way, RBAC is used to secure and control access to e-commerce transaction data stored in the cloud while ensuring that the user's job function determines their role. For example, an analyst or auditor's access will be determined by the functions that will be carried out; thus, users in that role may only access information required to carry out work on that task, which minimizes the unauthorized access risk. Least privilege is what drives RBAC and ensures that users only have the least requisite access to carry out their duties. RBAC incorporates four basic components: Users (U), Roles (R), Permissions (P), and Sessions (S). These elements are mathematically related using functions.

- *User-to-Role Assignment:*

$$UA \subseteq U \times R \quad (5)$$

This maps users to roles; for example, if user $u1$ is assigned the role $r1$, then $(u1, r1) \in UA$.

- *Role-to-Permission Assignment:*

$$PA \subseteq R \times P \quad (6)$$

This states what actions each role can perform; for instance, $r1$ has permission $p1$ and permission $p2$ .Therefore, $(r1, p1), (r1, p2) \in PA$.

- *A user session function defines active roles during a login session:*

$$\text{session} : U \rightarrow 2^R \quad (7)$$

Cloud Storage

Cloud storage is used in the proposed framework to securely store the pre-processed and access-controlled encrypted e-commerce transaction data. The data is

uploaded to the cloud storage service that provides scalable, high availability, durability, and fault tolerance. Before the data is sent to the cloud, encryption with BitLocker guarantees that it travels in an unreadable format even in the event of compromised access. Secure transmission protocols are used for transferring data in transit. When stored, access policies and IAM roles are set to ensure that any specific file or object can only be accessed by designated users or systems. Moreover, cloud storage solutions are equipped with versioning, lifecycle policies, and redundancy for better management and recovery of data. The integration of these storage mechanisms underlies the framework, assuring cost-effective, scalable, and long-term security, availability, and integrity of sensitive e-commerce transaction data.

4. Result

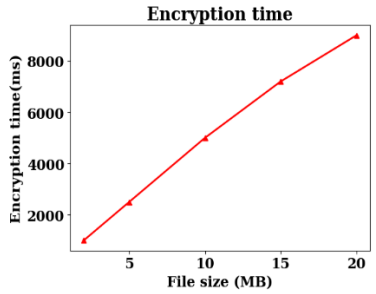

Figure 2: Impact of File Size on Encryption Time

The relationship between file size in megabytes and encryption time in milliseconds is demonstrated in Figure 2. File sizes between 2 and 20 megabytes appeared to induce some steady time increments in encryption from around 1000 ms to about 9000 ms across this range. This would approximately indicate linear growth, showing that larger files require more processing time for encryption. The trend advises that the encryption method used scales with the data volume, which is crucial for performance measurements concerning secure cloud storage systems.

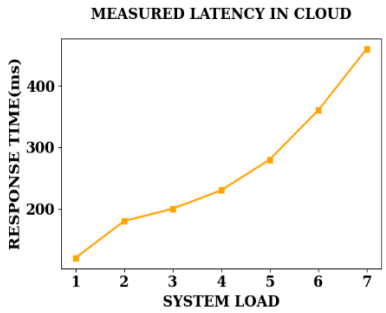

Figure 3: Impact of System Load on Latency

The measured latencies in cloud computing with increasing system loads from 1 to 7 are shown in Figure 3. Steadily, these system response times reach about 120 milliseconds at load 1 and approximately 460 milliseconds at load 7. This constellation of results shows a large variation in performance with increasing load on a system. This trend underscores the need for a cloud infrastructure that supports scalability and optimal responsiveness.

Conclusion

A comprehensive multi-tier security, scalability, and performance optimization framework has been proposed to make handling e-commerce transactional data in the cloud secure and scalable. The data collection and pre-processing followed by encryption using BitLocker, Role-Based Access Control, and cloud storage ensure the confidentiality, integrity, and availability of sensitive transaction data. The analysis shows how encryption time grows linearly with file size, by 1000 ms with 2MB becoming 9000 ms with 20MB while system load increases latency from response time 120 ms with load 1 to 460 ms with load 7. Such observations show that there is an imperative need to work towards optimization in both encryption methodologies and cloud infrastructure for scalable performance. Future improvements could include adopting different encryption algorithms, better real-time data processing, fine-tuned access control mechanisms, and further optimizations on cloud resource management. Multi-cloud, advanced monitoring, and analytics will further improve this framework by extending it in terms of future usability and adaptability in a dynamic e-commerce world.

Reference

[1] Sohaib, O., Naderpour, M., Hussain, W., & Martinez, L. (2019). Cloud computing model selection for e-commerce enterprises using a new 2-tuple fuzzy linguistic decision-making method. Computers & Industrial Engineering, 132, 47-58.

[2] Mohanarangan, V.D (2020). Improving Security Control in Cloud Computing for Healthcare Environments. Journal of Science and Technology, 5(6).

[3] Huang, L., & Abnoosian, K. (2020). A new approach for service migration in cloud-based e-commerce using an optimization algorithm. International Journal of Communication Systems, 33(14), e4457.

[4] Ganesan, T. (2020). Machine learning-driven AI for financial fraud detection in IoT environments. International Journal of HRM and Organizational Behavior, 8(4).

[5] Vijai, C., & Nivetha, P. (2020). E-commerce on cloud: opportunities and challenges. International Journal of Advances in Management, 13(3), 14-21.

[6] Deevi, D. P. (2020). Improving patient data security and privacy in mobile health care: A structure employing WBANs, multi-biometric key creation, and dynamic metadata rebuilding. International Journal of Engineering Research & Science & Technology, 16(4).

[7] Zhang, C., & Rao, W. (2020, February). Impact of cloud computing on agricultural product E-commerce. In IOP Conference Series: Materials Science and Engineering (Vol. 750, No. 1, p. 012210). IOP Publishing.

[8] Mohanarangan, V.D. (2020). Assessing Long-Term Serum Sample Viability for Cardiovascular Risk Prediction in Rheumatoid Arthritis. International Journal of Information Technology & Computer Engineering, 8(2), 2347–3657.

[9] Zhang, M., Yao, Y., Jiang, Y., Li, B., & Tang, C. (2018). Accountable mobile e-commerce scheme in intelligent cloud system transactions. Journal of Ambient Intelligence and Humanized Computing, 9(6), 1889-1899.
[10] Koteswararao, D. (2020). Robust Software Testing for Distributed Systems Using Cloud Infrastructure, Automated Fault Injection, and XML Scenarios. International Journal of Information Technology & Computer Engineering, 8(2), ISSN 2347–3657.
[11] Murali Dhar, M. S., & Manimegalai, R. (2018). A policy-oriented secured service for the e-commerce applications in cloud. Personal and Ubiquitous Computing, 22(5), 911-919.
[12] Rajeswaran, A. (2020). Big Data Analytics and Demand-Information Sharing in ECommerce Supply Chains: Mitigating Manufacturer Encroachment and Channel Conflict. International Journal of Applied Science Engineering and Management, 14(2), ISSN2454-9940
[13] Akinyede, R. O. (2018). Proposed E-Commerce Framework Using Cloud Computing Technology". International Journal of Computer Science Trends and Technology (IJCST), 6(3), 2018.
[14] Alagarsundaram, P. (2020). Analyzing the covariance matrix approach for DDoS HTTP attack detection in cloud environments. International Journal of Information Technology & Computer Engineering, 8(1).
[15] Gupta, S., & Gugulothu, N. (2018). Secure NoSQL for the social networking and e-commerce based bigdata applications deployed in cloud. International Journal of Cloud Applications and Computing (IJCAC), 8(2), 113-129.
[16] Poovendran, A. (2020). Implementing AES Encryption Algorithm to Enhance Data Security in Cloud Computing. International Journal of Information technology & computer engineering, 8(2).
[17] Khrais, L. T. (2020). Role of artificial intelligence in shaping consumer demand in E-commerce. International Journal of Future Internet, 12(12), 226.
[18] Sreekar, P. (2020). Cost-effective Cloud-Based Big Data Mining with K-means Clustering: An Analysis of Gaussian Data. International Journal of Engineering & Science Research, 10(1), 229-249.
[19] Zhang, Y., Abbas, H., & Sun, Y. (2019). Smart e-commerce integration with recommender systems. International Journal of Electronic Markets, 29, 219-220.
[20] Karthikeyan, P. (2020). Real-Time Data Warehousing: Performance Insights of Semi-Stream Joins Using Mongodb. International Journal of Management Research & Review, 10(4), 38-49.
[21] Zhou, Q., Lou, J., & Jiang, Y. (2019). Optimization of energy consumption of green data center in e-commerce. Sustainable Computing: Informatics and Systems, 23, 103-110.
[22] Mohan, R.S. (2020). Data-Driven Insights for Employee Retention: A Predictive Analytics Perspective. International Journal of Management Research & Review, 10(2), 44-59.
[23] Zhou, Q., Zhang, Z., & Wang, Y. (2020). Research on safety management system optimization of B2C e-commerce intelligent logistics information system based on data cube. Journal of Intelligent & Fuzzy Systems, 38(2), 1585-1592.
[24] Sitaraman, S. R. (2020). Optimizing Healthcare Data Streams Using Real-Time Big Data Analytics and AI Techniques. International Journal of Engineering Research and Science & Technology, 16(3), 9-22.
[25] Leung, K. H., Luk, C. C., Choy, K. L., Lam, H. Y., & Lee, C. K. (2019). A B2B flexible pricing decision support system for managing the request for quotation process under e-commerce business environment. International Journal of Production Research, 57(20), 6528-6551.
[26] Panga, N. K. R. (2020). Leveraging heuristic sampling and ensemble learning for enhanced insurance big data classification. International Journal of Financial Management (IJFM), 9(1).
[27] Zhao, X. (2019, April). A study on e-commerce recommender system based on big data. In 2019 IEEE 4th international conference on cloud computing and big data analysis (ICCCBDA) (pp. 222-226). IEEE.
[28] Gudivaka, R. L. (2020). Robotic Process Automation meets Cloud Computing: A Framework for Automated Scheduling in Social Robots. International Journal of Business and General Management (IJBGM), 8(4), 49-62.
[29] Dhanalakshmi, A., Hui, X., Roopini, R., & Supriya, R. (2020). Technological advancements in E-Commerce and customer relationship management. International Journal of Engineering and Management Research (IJEMR), 10(6), 9-20.
[30] Gudivaka, R. K. (2020). Robotic Process Automation Optimization in Cloud Computing Via Two-Tier MAC and LYAPUNOV Techniques. International Journal of Business and General Management (IJBGM), 9(5), 75-92.
[31] Du, X., Liu, B., & Zhang, J. (2019, November). Application of business intelligence based on big data in e-commerce data analysis. In Journal of Physics: Conference Series (Vol. 1395, No. 1, p. 012011). IOP Publishing.
[32] Devi, D. P. (2020). Artificial neural network enhanced real-time simulation of electric traction systems incorporating electro-thermal inverter models and FEA. International Journal of Engineering and Science Research, 10(3), 36-48.
[33] Lingam, Y. K. (2018). The role of Artificial Intelligence (AI) in making accurate stock decisions in E-commerce industry. Int. J. Adv. Res. Ideas Innov. Technol, 4(3), 2281-2286.
[34] Allur, N. S. (2020). Enhanced performance management in mobile networks: A big data framework incorporating DBSCAN speed anomaly detection and CCR efficiency assessment. Journal of Current Science, 8(4).
[35] Leung, K. H., Lee, C. K., & Choy, K. L. (2020). An integrated online pick-to-sort order batching approach for managing frequent arrivals of B2B e-commerce orders under both fixed and variable time-window batching. Advanced Engineering Informatics, 45, 101125.
[36] Deevi, D. P. (2020). Real-time malware detection via adaptive gradient support vector regression combined with LSTM and hidden Markov models. Journal of Science and Technology, 5(4).
[37] Alamdari, P. M., Navimipour, N. J., Hosseinzadeh, M., Safaei, A. A., & Darwesh, A. (2020). A systematic study on the recommender systems in the E-commerce. Ieee Access, 8, 115694-115716.
[38] Dondapati, K. (2020). Integrating neural networks and heuristic methods in test case prioritization: A machine learning perspective. International Journal of Engineering & Science Research, 10(3), 49–56.
[39] Micu, A., Geru, M., Capatina, A., Avram, C., Rusu, R., & Panait, A. A. (2019). Leveraging e-Commerce performance through machine learning algorithms. Ann. Dunarea Jos Univ. Galati, 2, 162-171.
[40] Dondapati, K. (2020). Leveraging backpropagation neural networks and generative adversarial networks to enhance channel state information synthesis in millimeter-wave networks. International Journal of Modern Electronics and Communication Engineering, 8(3), 81-90
[41] Shakya, S. (2019). An efficient security framework for data migration in a cloud computing environment. Journal of Artificial Intelligence, 1(01), 45-53.

[42] Gattupalli, K. (2020). Optimizing 3D printing materials for medical applications using AI, computational tools, and directed energy deposition. International Journal of Modern Electronics and Communication Engineering, 8(3).
[43] Kashurnikov, S. N., Sevalnev, V. V., Truntsevsky, Y. V., Cherepanova, E. V., & Berestneva, O. G. (2019). E-commerce in supply chain management: its introduction and prospects in the light industry. International Journal of Supply Chain Management, 8(4), 727-732.
[44] Allur, N. S. (2020). Big data-driven agricultural supply chain management: Trustworthy scheduling optimization with DSS and MILP techniques. Current Science & Humanities, 8(4), 1–16.
[45] He, W., & Xu, Y. (2018). Cross-border electronic commerce development present situation and the innovation research in China. American Journal of Industrial and Business Management, 8(8), 1825-1842.
[46] Narla, S., Valivarthi, D. T., & Peddi, S. (2020). Cloud computing with artificial intelligence techniques: GWO-DBN hybrid algorithms for enhanced disease prediction in healthcare systems. Current Science & Humanities, 8(1), 14–30.
[47] Jiang, L., Cheng, Y., Yang, L., Li, J., Yan, H., & Wang, X. (2019). A trust-based collaborative filtering algorithm for E-commerce recommendation system. Journal of ambient intelligence and humanized computing, 10, 3023-3034.
[48] Kethu, S. S. (2020). AI and IoT-driven CRM with cloud computing: Intelligent frameworks and empirical models for banking industry applications. International Journal of Modern Electronics and Communication Engineering (IJMECE), 8(1), 54.
[49] Li, M., Shen, L., & Huang, G. Q. (2019). Blockchain-enabled workflow operating system for logistics resources sharing in E-commerce logistics real estate service. Computers & Industrial Engineering, 135, 950-969.
[50] Vasamsetty, C. (2020). Clinical decision support systems and advanced data mining techniques for cardiovascular care: Unveiling patterns and trends. International Journal of Modern Engineering and Computer Science, 8(2).
[51] Lin, H. L., Cho, C. C., Ma, Y. Y., Hu, Y. Q., & Yang, Z. H. (2019). Optimization plan for excess warehouse storage in e-commerce–based plant shops: A case study for Chinese plant industrial. Journal of Business Economics and Management, 20(5), 897-919.
[52] Kadiyala, B. (2020). Multi-swarm adaptive differential evolution and Gaussian walk group search optimization for secured IoT data sharing using supersingular elliptic curve isogeny cryptography, International Journal of Modern Electronics and Communication Engineering,8(3).
[53] Lehrig, S., Sanders, R., Brataas, G., Cecowski, M., Ivanšek, S., & Polutnik, J. (2018). CloudStore—towards scalability, elasticity, and efficiency benchmarking and analysis in Cloud computing. Future Generation Computer Systems, 78, 115-126.
[54] Valivarthi, D. T. (2020). Blockchain-powered AI-based secure HRM data management: Machine learning-driven predictive control and sparse matrix decomposition techniques. Vol 8, Issue 4.
[55] Li, M., Shao, S., Ye, Q., Xu, G., & Huang, G. Q. (2020). Blockchain-enabled logistics finance execution platform for capital-constrained E-commerce retail. Robotics and Computer-Integrated Manufacturing, 65, 101962.
[56] Jadon, R. (2020). Improving AI-driven software solutions with memory-augmented neural networks, hierarchical multi-agent learning, and concept bottleneck models. International Journal of Information Technology and Computer Engineering, 8(2), 13
[57] Kumar, G., Saha, R., Buchanan, W. J., Geetha, G., Thomas, R., Rai, M. K., ... & Alazab, M. (2020). Decentralized accessibility of e-commerce products through blockchain technology. Sustainable Cities and Society, 62, 102361.
[59] Mezni, H., & Abdeljaoued, T. (2018). A cloud services recommendation system based on Fuzzy Formal Concept Analysis. International Journal of Data & Knowledge Engineering, 116, 100-123.
[60] Boyapati, S. (2020). Assessing digital finance as a cloud path for income equality: Evidence from urban and rural economies. International Journal of Modern Electronics and Communication Engineering (IJMECE), 8(3), 122.
[61] Liu, C., Xiao, Y., Javangula, V., Hu, Q., Wang, S., & Cheng, X. (2018). NormaChain: A blockchain-based normalized autonomous transaction settlement system for IoT-based E-commerce. IEEE Internet of Things Journal, 6(3), 4680-4693.
[62] Gaius Yallamelli, A. R. (2020). A cloud-based financial data modeling system using GBDT, ALBERT, and Firefly algorithm optimization for high-dimensional generative topographic mapping. Vol 8, Issue 4, 27.
[63] Brahma, A., & Dutta, R. (2020). Role of social media and e-commerce for business entrepreneurship. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 6(6), 1-18.
[64] Yalla, R. K. M. K., Yallamelli, A. R. G., & Mamidala, V. (2020). Comprehensive approach for mobile data security in cloud computing using RSA algorithm. Journal of Current Science & Humanities, 8(3), 13–33.
[65] Hussein, L. A., Baharudin, A. S., Jayaraman, K., & Kiumarsi, S. H. A. I. A. N. (2019). B2B e-commerce technology factors with mediating effect perceived usefulness in Jordanian manufacturing SMES. Journal of Engineering Science and Technology, 14(1), 411-429.
[66] Samudrala, V. K. (2020). AI-powered anomaly detection for cross-cloud secure data sharing in multi-cloud healthcare networks. Journal of Current Science & Humanities, 8(2), 11–22.
[67] Guan, Z., Wang, N., Fan, X., Liu, X., Wu, L., & Wan, S. (2020). Achieving secure search over encrypted data for e-commerce: a blockchain approach. ACM Transactions on Internet Technology (TOIT), 21(1), 1-17.
[68] Ayyadurai, R. (2020). Smart surveillance methodology: Utilizing machine learning and AI with blockchain for bitcoin transactions. World Journal of Advanced Engineering Technology and Sciences, 1(1), 110–120.
[69] Bui, K. T., Van Vo, L., Nguyen, C. M., Pham, T. V., & Tran, H. C. (2020). A fault detection and diagnosis approach for multi-tier application in cloud computing. Journal of Communications and Networks, 22(5), 399-414.
[70] Chauhan, G. S., & Jadon, R. (2020). AI and ML-powered CAPTCHA and advanced graphical passwords: Integrating the DROP methodology, AES encryption, and neural network-based authentication for enhanced security. World Journal of Advanced Engineering Technology and Sciences, 1(1), 121–132.
[71] Liu, C., Feng, Y., Lin, D., Wu, L., & Guo, M. (2020). Iot based laundry services: an application of big data analytics, intelligent logistics management, and machine learning techniques. International Journal of Production Research, 58(17), 5113-5131.
[72] Narla, S. (2020). Transforming smart environments with multi-tier cloud sensing, big data, and 5G technology. International Journal of Computer Science Engineering Techniques, 5(1), 1-10.
[73] Chen, Y. H. (2020). Intelligent algorithms for cold chain logistics distribution optimization based on big data cloud computing analysis. Journal of Cloud Computing, 9(1), 37.
[74] Alavilli, S. K. (2020). Predicting heart failure with explainable deep learning using advanced temporal convolutional networks. International Journal of Computer Science Engineering Techniques, 5(2).
[75] Asrowardi, I., Putra, S. D., & Subyantoro, E. (2020, February). Designing microservice architectures for scalability and reliability in e-commerce. In Journal of Physics: Conference Series (Vol. 1450, No. 1, p. 012077). IOP Publishing.
[76] Deng, S., Cheng, G., Zhao, H., Gao, H., & Yin, J. (2020). Incentive-driven computation offloading in blockchain-enabled E-commerce. ACM Transactions on Internet Technology (TOIT), 21(1), 1-19.