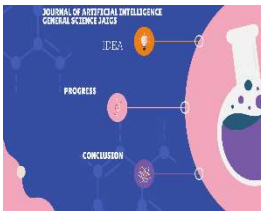
Vol.3,Issue 01, March 2024
Journal of Artificial Intelligence General Science JAIGS



Protecting Data Access Liabilities in Cloud Computing

Muhammad Umair

Marketing Analyst, Ortak Jewellery - United Kingdom.

*Corresponding Author: Muhammad Umair

ARTICLEINFO
Article History:
Received:
05.03.2024
Accepted:
10.03.2024
Online: 10.04.2024
Keyword:cloud computing, logging, privacy, security, data sharing, information accountability framework.

ABSTRACT

Cloud computing revolutionizes service provision by delivering virtualized services via the internet. The Cloud, a ubiquitous term for this online space, is managed by service providers. However, users engaging with cloud services face concerns regarding data security and privacy, fearing potential misuse by service providers, who may inadvertently expose sensitive data to unauthorized parties. To address this challenge, we introduce a novel framework called the Cloud Information Accountability (CIA) framework, centered on the concept of data liability. Our framework outlines essential requirements and offers guidelines for achieving robust data accountability in cloud environments. Upon data submission by the owner, the service provider gains full access and control over the data, typically governed by traditional access control mechanisms. To enhance transparency and accountability, we propose an algorithm that automates data access logging via JAR files, providing detailed insights into data usage. Our approach aims to bolster trust, mitigate privacy concerns, and fortify security in cloud computing ecosystems.

Introduction

The Cloud Information Accountability (CIA) framework introduced in this study facilitates automated logging and distributed auditing of pertinent access activities conducted by any entity, across any Cloud Service Provider (CSP). The CIA framework comprises two key components: the logger and the log harmonizer. Within this framework, a JAR (Java Archive) file is employed to establish simple access control rules, governing permissions for entry and exit into cloud storage. Consequently, data management within the cloud traverses a sophisticated and dynamic hierarchical service chain, distinct from conventional environments.

To address these challenges, we propose a novel approach, the Cloud Information Accountability (CIA) framework, which supports the concept of data responsibility. We delineate common requirements and offer diverse recommendations to achieve data accountability within cloud environments. For instance, when a user subscribes to a specific cloud service, they typically transmit their data and associated access control policies to the service provider. Subsequently, upon receipt of the data, the CSP is granted access permission rights, such as read, write, and copy, utilizing standard access control mechanisms. Once access rights are granted, the data becomes fully accessible to the service provider.

The CIA framework, as proposed in this study, facilitates automated logging and distributed auditing of relevant access actions across various cloud services through its core components: the logger and log harmonizer. The JAR file encapsulates a set of straightforward access control rules, governing the authorization of cloud servers and potential data stakeholders to access the content. Following successful verification, service providers are granted access to the data as specified within the JAR. Depending on the configurations established during creation, the Java Archive file offers usage control alongside logging capabilities. Each time data is accessed, the JAR generates a corresponding log entry automatically.

Cloud computing heralds a paradigm shift in resource provisioning, offering an on-demand, scalable model for accessing IT services over the internet. In this model, data management is outsourced by the CSP to various entities within the cloud ecosystem, each forwarding applications to subsequent entities, thus forming a chain of service provision.

Literature Review

a) Provenance Management in Curated Databases (Peter Buneman, Adriane P. Chapman, James Cheney)

Curated databases across various fields, including bioinformatics, undergo extensive manual annotation, correction, and data transfer from diverse sources. To assess the integrity and

scientific value of such data, understanding its provenance—comprising creation, attribution, and version history—is crucial. Traditional database systems offer limited support for tracking provenance, particularly when data migrates among databases. This paper explores general techniques for documenting provenance when data is copied between databases. We propose an approach that monitors user actions during browsing of source databases and data copying into a curated database, capturing these actions in a queryable format. An implementation of this approach is presented and evaluated to assess the feasibility of database support for provenance management. Our experiments demonstrate that while a native approach incurs high overhead, simple optimizations can mitigate this to an acceptable level.

b) The Advantages of Elliptic Curve Cryptography for Wireless Security (Kristin Lauter, Microsoft Corporation)

This article provides an overview of elliptic curves and their application in cryptography, with a focus on the performance benefits offered in wireless environments compared to traditional cryptosystems like RSA. Specific applications of elliptic curve cryptography in securing messaging and identity-based encryption are discussed.

c) Identity-Based Encryption from the Weil Pairing (Dan Boneh, And Matt Franklin)

We introduce a fully functional identity-based encryption scheme (IBE), offering chosen ciphertext security in the random oracle model based on an elliptic curve variant of the computational Diffie-Hellman problem. Precise definitions for secure identity-based encryption schemes are provided, along with several applications for such systems.

d) Verifiable Security of Boneh-Franklin Identity-Based Encryption (Gilles Barthe, Federico Olmedo, and Santiago Zanella-Beguelin)

Identity-based encryption (IBE) enables one party to send encrypted messages to another using an arbitrary identity string as the encryption key, simplifying key management in public-key cryptography. While the concept of IBE was introduced by Shamir in 1981, practical scheme construction remained a challenge until Boneh and Franklin proposed a solution in 2001, which leverages pairing-based cryptography. We present a game-based, machine-checked reduction of the security of the Boneh-Franklin IBE scheme to the Bilinear Diffie-Hellman assumption, accompanied by an analysis of its tightness through an exact security bound. Our proof streamlines and elucidates the original Boneh-Franklin proof and is automatically verified using a trusted checker.

Existing System

• Cloud data management entails navigating a complex and dynamically evolving service chain within the cloud environment.

• Traditional environments struggle to effectively accommodate such services.

• Ordinary web frameworks are typically employed for data auditing purposes.

• Standard web services are utilized for handling requests and responses.

a) Disadvantages

• User data lacks adequate security measures such as authentication.

• Implementation requires costly resources.

• Not conducive for small to medium-sized storage users.

b) Proposed System

• We advocate for a contemporary solution called the Cloud Information Accountability (CIA) framework, centered on the concept of data liability.

• The CIA framework ensures end-to-end accountability in a highly decentralized manner.

• A comprehensive security analysis is provided, discussing strengths and reliability, while our robust architecture implements Java Running Environment.

• Apart from generating a class file for authenticating servers or users, another class file produces the appropriate inner JAR, while a third class file validates the JVM's integrity using oblivious hashing.

• A timer mechanism is proposed to restrict access for security purposes.

• Securing the JVM enhances software tamper resistance capabilities to the JAR file, providing integrity and confidentiality.

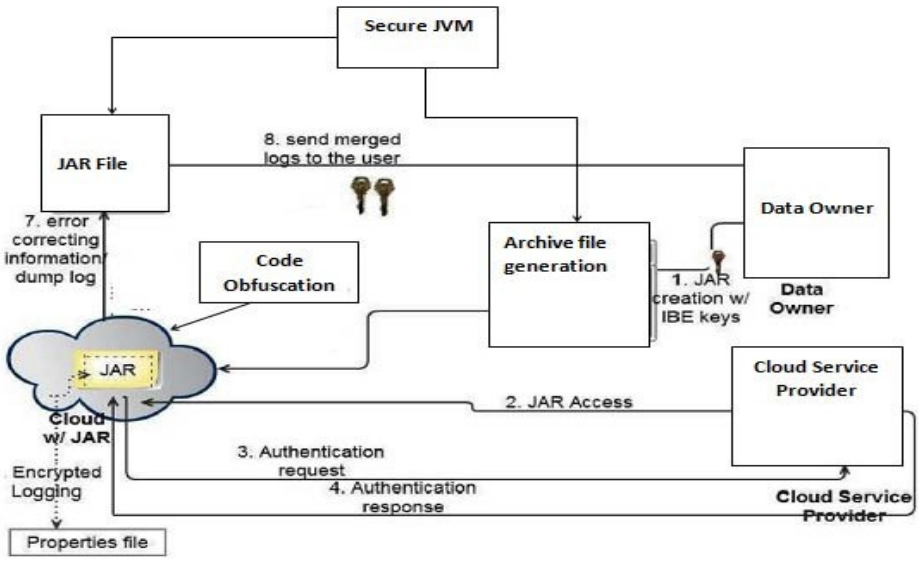
c) Advantages

• The CIA framework excels in maintaining lightweight yet robust accountability, integrating elements of access control, usage control, and authentication.

• This technique effectively mitigates various attacks including man-in-the-middle, dictionary, disassembling, and compromised JVM attacks.

• It is suitable for both limited and extensive storage requirements.

Architecture Diagram



In this manuscript, we propose a robust approach that sequentially incorporates entities in the order of their creation LR = (r1; . . . ; rki). Each entity is encrypted individually and subsequently updated to the log file. Upon read-only requests, the internal JAR decrypts the data, generating a temporary decrypted file. This file is then presented to the entity through a Java application viewer. Suppose it is displayed to a user, they can interact with the data within the Java application, opting out of methods that enable copying using hotkeys such as Print Screen.

a) Mode Setting

To ensure data owners are promptly and accurately informed about their data usage, our distributed logging mechanism is complemented by a unique auditing mechanism. We support two complementary auditing modes:

i) Push mode

ii) Pull mode.

• Push Mode: In this mode, the harmonizer pushes the logs to the data owner (or auditor) in a timely manner. The push action is triggered by either of the following two events: either a certain time period elapses according to the temporal timer inserted as part of the JAR file, or the JAR file exceeds the size stipulated by the content owner at the time of creation.

• Pull Mode: This mode allows auditors to retrieve the logs, providing explicit dynamic data support to ensure the correctness and availability of users' data in the cloud.

a) JAR Generation

The JAR file contains a set of access control policies specifying whether and how the cloud servers, and potentially other interested parties (users, companies), are authorized to access the information. Depending on the configuration settings, the JAR will provide usage control combined with login credentials.

b) Logger Creation

To enable automated logging, we leverage the programming capabilities of the JAR files. User information and related data items are stored in a nested Java JAR file, which serves as the logger component. The outer JAR provides authentication to entities for accessing the data stored in the JAR file. In this scenario, data owners may not be aware of the exact CSPs handling their data. Therefore, authentication is based on the server's functionality. Data owners can grant permissions in user-centric terms, contrary to the usual code-centric security offered by Java, utilizing its Authentication and Authorization Services. Additionally, the outer JAR facilitates the selection of the correct inner JAR based on the identity of the entities requesting the data.

c) Log Record Generation

The logger component generates the log records. Logging occurs with every access to the data in the JAR, allowing data owners to review recent accesses to their own data at any time.

b) Algorithm

The utilization of push-pull strategies proves highly advantageous when dealing with large volumes of data accessed within short timeframes. In such scenarios, if data transmission lacks randomness, the logging file swells in size, leading to increased operational costs such as data copying. Data owners typically favor the push mode, seeking consistent monitoring of data usage over time. Automatic receipt of logs alleviates the burden on data analysts for such owners.

Configurable parameters, including the maximum log size for push-out, are easily set during logger component creation. Conversely, the pull strategy becomes crucial when a data owner suspects misuse of their data, enabling immediate monitoring of content usage. A hybrid strategy, blending the consistent information flow of the push mode with the on-demand convenience of the pull mode, presents a practical solution.

c) Logging Mechanism

- The Logger Structure

- Log Record Generation

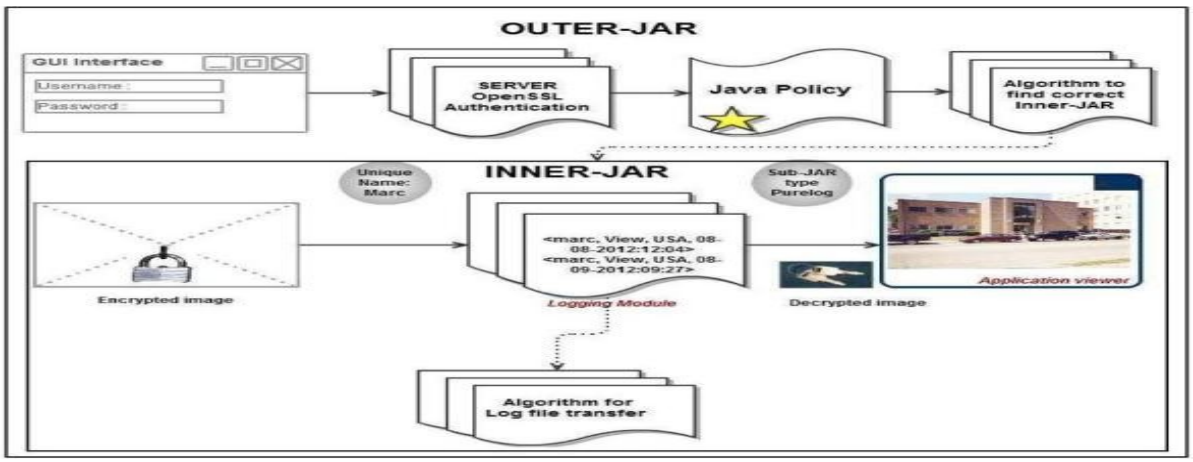
- Dependability of Logs

- Availability of JARs

- Accuracy of Logs

d) The Logger Structure

Automated logging relies on the programming capabilities embedded within the JAR file. A logger component, housed within a nested Java JAR file, contains a user's data items and associated log files.



The outer JAR is responsible for authenticating entities seeking access to the data stored within the JAR file. In scenarios where data owners lack precise knowledge of the CSPs managing the data, authentication is tailored based on server functionality. For instance, a policy might dictate that Server X can retrieve data if it functions as a storage server. Additionally, the outer JAR can enforce data owner parameters, defined as Java policies, which are implemented on the data.

Access permissions within the Java Environment, governed by Java policies, reflect File System Permissions. However, data owners can articulate access permissions in user-centric terms, contrary to Java's typical code-centric security, utilizing its authentication and authorization services. Furthermore, the outer JAR is responsible for selecting the appropriate inner JAR based on the requesting entity's identity.

To facilitate log file retrieval, display enclosed data in a suitable format, and maintain a log file for each encrypted item, each inner JAR stores encrypted data and class files. Two options are supported:

- Pure Log: Records every data access solely for auditing purposes.

- Access Log: Performs logging actions and enforces access control. Denied requests are logged with request time, while granted requests are additionally logged with access information and allowed time period.

These logging methods encourage data owners to implement access conditions proactively (for Access Logs) or reactively (for Pure Logs). For instance, billing services require Pure Logs, while services with service-level agreements restricting access to sensitive information necessitate Access Logs.

To execute these tasks, the inner JAR writes log records using class files. Another class file coordinates with the log harmonizer, while a third encrypted class file facilitates data retrieval or copying from the server. The system never stores secret keys.

Apart from containing one or more inner JARs, the outer JAR includes class files for authenticating servers or users, and another for identifying the correct inner JAR. Additionally, a third class file utilizes oblivious hashing to verify the JVM's validity. Furthermore, a class file manages the Graphical User Interface for user authentication and Java Policy.

e) Log Record Generation

The Logger Component generates log records for any access to the data within the JAR, systematically adding new entries in order of creation LR= (r1; . . . ; rki). Each record ri undergoes encryption individually before being appended to the log file. To ensure the accuracy of log records, access time, locations, and actions are meticulously verified. Access time is determined using the Network Time Protocol (NTP) to prevent manipulation by malicious entities. By leveraging IP addresses, the JAR traces the location of Cloud Service Providers (CSPs) using IP lookup techniques. Advanced methods are employed for precise location determination. Additionally, if a trusted time stamp management infrastructure is available, it can be utilized to record timestamps in the accountability log.

Recording actions on users' data is crucial. The system supports four types of actions: view, download, timed access, and location-based access. Each action is recorded or enforced differently depending on the type of logging module employed:

- View: For entities with read-only permissions, the pure log updates the log record while Access Logs enforce the action using the enclosed access control module. When a read-only access request is made, the inner JAR creates a temporary decrypted file on-the-fly. If accessed by a human user, the Java application viewer reveals the hidden file, enabling the entity to interact with the data. Print screen copying methods are disabled, and data hiding measures are employed to prevent unauthorized access.

- Download: Entities are permitted to save a raw copy of the data without logging access to the copy. With Pure Log, the user's data can be directly downloaded in its original form via a provided link. In the case of Access Logs, the entire JAR file containing the data is provided to the entity for download.

- Timed Access: Access is granted for a limited period, recorded by both the pure log and Access Log. The duration is calculated using the Network Time Protocol, and access is enforced only when combined with view or download access.

- Location-based Access: The pure log records the location of entities, while Access Logs verify the location for each access. Data access is granted only to entities located at locations specified by the data owner.

Dependability of Logs

The integrity of log records is crucial. To ensure this, the JRE within the logger component should remain unaltered. A two-step process is employed to check the integrity of the logger component:

1. The JRE is repaired before the logger is launched to guarantee the integrity of the environment.

2. Hash codes are inserted to detect modifications of the JRE once the logger component is launched, ensuring the original code flow is maintained.

The system must also contend with potential threats such as intruders storing JARs remotely to disrupt the auditing mechanism or gaining control of the JRE running JAR files.

JARs Availability

To safeguard offline JARs from attackers, the Cloud Information Accountability system provides a log harmonizer. This component performs two main tasks: managing JAR copies and recovering corrupted logs. Each log harmonizer maintains copies of logger components holding similar data items, ensuring integrity and availability without compromising user data.

Conclusion:

The system proposes innovative methods for automatically logging all data access in the cloud, accompanied by an auditing mechanism. This mechanism empowers data owners not only to audit their content but also to implement robust backend protection measures. Additionally, a key feature of our approach is its ability to facilitate auditing of copies of data made without the owner's knowledge.

Future Work

In addition to a class file designed for authenticating servers or users, another class file locates the correct inner JAR, while a third class file verifies the JVM's integrity using oblivious hashing techniques.

References:

[1]. Rehan, H. (2024). Revolutionizing America's Cloud Computing the Pivotal Role of AI in Driving Innovation and Security. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 189-208. DOI: https://doi.org/10.60087/jaigs.v2i1.p208

[2]. Rehan, H. (2024). AI-Driven Cloud Security: The Future of Safeguarding Sensitive Data in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 47-66. DOI: https://doi.org/10.60087/jaigs.v1i1.p66

[3]. Islam, M. M. (2024). Exploring Ethical Dimensions in AI: Navigating Bias and Fairness in the Field. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 13-17.**DOI:** https://doi.org/10.60087/jaigs.v1i1.p18

[4]. Khan, M. R. (2024). Advances in Architectures for Deep Learning: A Thorough Examination of Present Trends. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 24-30. **DOI:** https://doi.org/10.60087/jaigs.v1i1.p30

[5]. Shuford, J., & Islam, M. M. (2024). Exploring the Latest Trends in Artificial Intelligence Technology: A Comprehensive Review. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1). **DOI:** https://doi.org/10.60087/jaigs.v2i1.p13

[6]. Islam, M. M. (2024). Exploring the Applications of Artificial Intelligence across Various Industries. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 20-25.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p25

[7]. Akter, S. (2024). Investigating State-of-the-Art Frontiers in Artificial Intelligence: A Synopsis of Trends and Innovations. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 25-30.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p30

[8]. Rana, S. (2024). Exploring the Advancements and Ramifications of Artificial Intelligence. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 30-35.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p35

[9]. Sarker, M. (2024). Revolutionizing Healthcare: The Role of Machine Learning in the Health Sector. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 35-48.

DOI: https://doi.org/10.60087/jaigs.v2i1.p47

[10]. Akter, S. (2024). Harnessing Technology for Environmental Sustainability: Utilizing AI to Tackle Global Ecological Challenges. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 49-57.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p57

[11]. Padmanaban, H. (2024). Revolutionizing Regulatory Reporting through AI/ML: Approaches for Enhanced Compliance and Efficiency. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 57-69.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p69

[12]. Padmanaban, H. (2024). Navigating the Role of Reference Data in Financial Data Analysis: Addressing Challenges and Seizing Opportunities. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 69-78.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p78

[13]. Camacho, N. G. (2024). Unlocking the Potential of AI/ML in DevSecOps: Effective Strategies and Optimal Practices. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 79-89.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p89

[14]. PC, H. P., & Sharma, Y. K. (2024). Developing a Cognitive Learning and Intelligent Data Analysis-Based Framework for Early Disease Detection and Prevention in Younger Adults with Fatigue. *Optimized Predictive Models in Health Care Using Machine Learning*, 273.

[15]. Padmanaban, H. (2024). Quantum Computing and AI in the Cloud. *Journal of Computational Intelligence and Robotics*, *4*(1), 14–32. Retrieved from https://thesciencebrigade.com/jcir/article/view/116

[16]. Sharma, Y. K., & Harish, P. (2018). Critical study of software models used cloud application development. *International Journal of Engineering & Technology, E-ISSN*, 514-518.https://www.researchgate.net/profile/Harish-Padmanaban-2/publication/377572317_Critical_study_of_software_models_used_cloud_application_development/links/65ad55d7ee1e1951fbd79df6/Critical-study-of-software-models-used-cloud-application-development.pdf

[17]. Padmanaban, P. H., & Sharma, Y. K. (2019). Implication of Artificial Intelligence in Software Development Life Cycle: A state of the art review. *vol*, *6*, 93-98.https://www.researchgate.net/profile/Harish-Padmanaban-2/publication/377572222_Implication_of_Artificial_Intelligence_in_Software_Development_Life_Cycle_A_state_of_the_art_review/links/65ad54e5bf5b00662e333553/Implication-of-Artificial-Intelligence-in-Software-Development-Life-Cycle-A-state-of-the-art-review.pdf

[18]. Harish Padmanaban, P. C., & Sharma, Y. K. (2024). Optimizing the Identification and Utilization of Open Parking Spaces Through Advanced Machine Learning. *Advances in Aerial Sensing and Imaging*, 267-294. **https://doi.org/10.1002/9781394175512.ch12**

[19]. PC, H. P., Mohammed, A., & RAHIM, N. A. (2023). *U.S. Patent No. 11,762,755*. Washington, DC: U.S. Patent and Trademark Office.https://patents.google.com/patent/US20230385176A1/en

[20]. Padmanaban, H. (2023). Navigating the intricacies of regulations: Leveraging AI/ML for Accurate Reporting. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(3), 401-412.DOI: https://doi.org/10.60087/jklst.vol2.n3.p412

[21]. PC, H. P. Compare and analysis of existing software development lifecycle models to develop a new model using computational intelligence.https://shodhganga.inflibnet.ac.in/handle/10603/487443

[22]. Latif, M. A., Afshan, N., Mushtaq, Z., Khan, N. A., Irfan, M., Nowakowski, G., ... &Telenyk, S. (2023). Enhanced classification of coffee leaf biotic stress by synergizing feature concatenation and dimensionality reduction. *IEEE Access*.
DOI: https://doi.org/10.1109/ACCESS.2023.3314590

[23]. Irfan, M., Mushtaq, Z., Khan, N. A., Mursal, S. N. F., Rahman, S., Magzoub, M. A., ... & Abbas, G. (2023). A Scalo gram-based CNN ensemble method with density-aware smote oversampling for improving bearing fault diagnosis. *IEEE Access*, *11*, 127783-127799.
DOI: https://doi.org/10.1109/ACCESS.2023.3332243

[24]. Irfan, M., Mushtaq, Z., Khan, N. A., Althobiani, F., Mursal, S. N. F., Rahman, S., ... & Khan, I. (2023). Improving Bearing Fault Identification by Using Novel Hybrid Involution-Convolution Feature Extraction with Adversarial Noise Injection in Conditional GANs. *IEEE Access*.

DOI: https://doi.org/10.1109/ACCESS.2023.3326367

[25]. Rahman, S., Mursal, S. N. F., Latif, M. A., Mushtaq, Z., Irfan, M., & Waqar, A. (2023, November). Enhancing Network Intrusion Detection Using Effective Stacking of Ensemble Classifiers With Multi-Pronged Feature Selection Technique. In *2023 2nd International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETECTE)* (pp. 1-6). IEEE.

DOI: https://doi.org/10.1109/ETECTE59617.2023.10396717

[26]. Latif, M. A., Mushtaq, Z., Arif, S., Rehman, S., Qureshi, M. F., Samee, N. A., ... & Al-masni, M. A. Improving Thyroid Disorder Diagnosis via Ensemble Stacking and Bidirectional Feature Selection.
https://doi.org/10.32604/cmc.2024.047621

[27]. Ara, A., &Mifa, A. F. (2024). INTEGRATING ARTIFICIAL INTELLIGENCE AND BIG DATA IN MOBILE HEALTH: A SYSTEMATIC REVIEW OF INNOVATIONS AND CHALLENGES IN HEALTHCARE SYSTEMS. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *3*(01), 01-16.

DOI: https://doi.org/10.62304/jbedpm.v3i01.70

[28]. Bappy, M. A., & Ahmed, M. (2023). ASSESSMENT OF DATA COLLECTION TECHNIQUES IN MANUFACTURING AND MECHANICAL ENGINEERING THROUGH MACHINE LEARNING MODELS. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *2*(04), 15-26.
DOI: https://doi.org/10.62304/jbedpm.v2i04.67

[29]. Bappy, M. A. (2024). Exploring the Integration of Informed Machine Learning in Engineering Applications: A Comprehensive Review. *American Journal of Science and Learning for Development*, *3*(2), 11-21.
DOI: https://doi.org/10.51699/ajsld.v3i2.3459

[30]. Uddin, M. N., Bappy, M. A., Rab, M. F., Znidi, F., &Morsy, M. (2024). Recent Progress on Synthesis of 3D Graphene, Properties, and Emerging Applications.
DOI: https://doi.org/10.5772/intechopen.114168

[31]. Hossain, M. I., Bappy, M. A., &Sathi, M. A. (2023). WATER QUALITY MODELLING AND ASSESSMENT OF THE BURIGANGA RIVER USING QUAL2K. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *2*(03), 01-11.
DOI: https://doi.org/10.62304/jieet.v2i03.64

[32]. Zhu, M., Zhang, Y., Gong, Y., Xing, K., Yan, X., & Song, J. (2024). Ensemble Methodology: Innovations in Credit Default Prediction Using LightGBM, XGBoost, and LocalEnsemble. *arXiv preprint arXiv:2402.17979*.

https://doi.org/10.48550/arXiv.2402.17979

[33]. Yafei, X., Wu, Y., Song, J., Gong, Y., &Lianga, P. (2024). Generative AI in Industrial Revolution: A Comprehensive Research on Transformations, Challenges, and Future Directions. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *3*(2), 11-20.

DOI: https://doi.org/10.60087/jklst.vol.3n2.p20

[34]. Xu, J., Wang, H., Zhong, Y., Qin, L., & Cheng, Q. (2024). Predict and Optimize Financial Services Risk Using AI-driven Technology. *Academic Journal of Science and Technology*, *10*(1), 299-304.

https://drpress.org/ojs/index.php/ajst/article/view/19205

[35]. Ness, S., Sarker, M., Volkivskyi, M., & Singh, N. (2024). The Legal and Political Implications of AI Bias: An International Comparative Study. *American Journal of Computing and Engineering*, *7*(1), 37-45.
DOI: https://doi.org/10.47672/ajce.1879

[36]. Sarker, M. (2022). Towards Precision Medicine for Cancer Patient Stratification by Classifying Cancer By Using Machine Learning. *Journal of Science & Technology*, *3*(3), 1-30.
DOI: https://doi.org/10.55662/JST.2022.3301

[37]. Manoharan, A., &Sarker, M. REVOLUTIONIZING CYBERSECURITY: UNLEASHING THE POWER OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING FOR NEXT-GENERATION THREAT DETECTION.

DOI :https://www.doi.org/10.56726/IRJMETS32644

[38]. Lee, S., Weerakoon, M., Choi, J., Zhang, M., Wang, D., & Jeon, M. (2022, July). CarM: Hierarchical episodic memory for continual learning. In *Proceedings of the 59th ACM/IEEE Design Automation Conference* (pp. 1147-1152).

https://doi.org/10.1145/3489517.3530587

[39]. Lee, S., Weerakoon, M., Choi, J., Zhang, M., Wang, D., & Jeon, M. (2021). Carousel Memory: Rethinking the Design of Episodic Memory for Continual Learning. *arXiv preprint arXiv:2110.07276*.

https://doi.org/10.48550/arXiv.2110.07276

[40]. Weerakoon, M., Heaton, H., Lee, S., & Mitchell, E. (2024). TopoQual polishes circular consensus sequencing data and accurately predicts quality scores. *bioRxiv*, 2024-02.

doi: https://doi.org/10.1101/2024.02.08.579541

[41]. Pillai, A. S. (2023). Advancements in Natural Language Processing for Automotive Virtual Assistants Enhancing User Experience and Safety. *Journal of Computational Intelligence and Robotics*, *3*(1), 27-36.

https://thesciencebrigade.com/jcir/article/view/161

[42]. Sharma, Y. K., & Harish, P. (2018). Critical study of software models used cloud application development. *International Journal of Engineering & Technology, E-ISSN*, 514-518.

https://scholar.google.com/citations?view_op=view_citation&hl=en&user=Fxv3elcAAAAJ&citation_for_view=Fxv3elcAAAAJ:d1gkVwhDpl0C

[43]. PC, H. P., Mohammed, A., & RAHIM, N. A. (2023). *U.S. Patent No. 11,762,755*. Washington, DC: U.S. Patent and Trademark Office.

https://patents.google.com/patent/US11762755B2/en

[44]. Miah, S., Rahaman, M. H., Saha, S., Khan, M. A. T., Islam, M. A., Islam, M. N., ... & Ahsan, M. H. (2013). Study of the internal structure of electronic components RAM DDR-2 and motherboard of nokia-3120 by using neutron radiography technique. *International Journal of Modern Engineering Research (IJMER)*, *3*(60), 3429-3432

https://shorturl.at/nCJOQ

[45]. Rahaman, M. H., Faruque, S. B., Khan, M. A. T., Miah, S., & Islam, M. A. (2013). Comparison of General Relativity and Brans-Dicke Theory using Gravitomagnetic clock effect. *International Journal of Modern Engineering Research*, *3*, 3517-3520.

https://shorturl.at/hjm37

[46]. Miah, M. H., & Miah, S. (2015). The Investigation of the Effects of Blackberry Dye as a Sensitizer in TiO2 Nano Particle Based Dye Sensitized Solar Cell. *Asian Journal of Applied Sciences*, *3*(4).

https://shorturl.at/iyJQV

[48]. Miah, S., Miah, M. H., Hossain, M. S., & Ahsan, M. H. (2018). Study of the Homogeneity of Glass Fiber Reinforced Polymer Composite by using Neutron Radiography. *Am. J. Constr. Build. Mater*, *2*, 22-28.

https://shorturl.at/joDKZ

[49]. Miah, S., Islam, G. J., Das, S. K., Islam, S., Islam, M., & Islam, K. K. (2019). Internet of Things (IoT) based automatic electrical energy meter billing system. *IOSR Journal of Electronics and Communication Engineering*, *14*(4 (I)), 39-50.

[50]. Nadia, A., Hossain, M. S., Hasan, M. M., Islam, K. Z., & Miah, S. (2021). Quantifying TRM by modified DCQ load flow method. *European Journal of Electrical Engineering*, *23*(2), 157-163.

https://shorturl.at/csuO3

[51]. Miah, S., Raihan, S. R., Sagor, M. M. H., Hasan, M. M., Talukdar, D., Sajib, S., ... & Suaiba, U. (2022). Rooftop Garden and Lighting Automation by the Internet of Things (IoT). *European Journal of Engineering and Technology Research*, *7*(1), 37-43.

DOI: https://doi.org/10.24018/ejeng.2022.7.1.2700

[52]. Prasad, A. B., Singh, S., Miah, S., Singh, A., & Gonzales-Yanac, T. A Comparative Study on Effects of Work Culture on employee satisfaction in Public & Private Sector Bank with special reference to SBI and ICICI Bank.

[53]. Ravichandra, T. (2022). A Study On Women Empowerment Of Self-Help Group With Reference To Indian Context.

https://www.webology.org/data-cms/articles/20220203075142pmwebology%2019%20(1)%20-%2053.pdf

[54]. Kumar, H., Aoudni, Y., Ortiz, G. G. R., Jindal, L., Miah, S., & Tripathi, R. (2022). Light weighted CNN model to detect DDoS attack over distributed scenario. *Security and Communication Networks*, *2022*.

https://doi.org/10.1155/2022/7585457

[55]. Ma, R., Kareem, S. W., Kalra, A., Doewes, R. I., Kumar, P., & Miah, S. (2022). Optimization of electric automation control model based on artificial intelligence algorithm. *Wireless Communications and Mobile Computing*, *2022*.

https://doi.org/10.1155/2022/7762493

[56]. Devi, O. R., Webber, J., Mehbodniya, A., Chaitanya, M., Jawarkar, P. S., Soni, M., & Miah, S. (2022). The Future Development Direction of Cloud-Associated Edge-Computing Security in the Era of 5G as Edge Intelligence. *Scientific Programming*, *2022*.

https://doi.org/10.1155/2022/1473901

[57]. Al Noman, M. A., Zhai, L., Almukhtar, F. H., Rahaman, M. F., Omarov, B., Ray, S., ... & Wang, C. (2023). A computer vision-based lane detection technique using gradient threshold and hue-lightness-saturation value for an autonomous vehicle. *International Journal of Electrical and Computer Engineering*, *13*(1), 347.

https://shorturl.at/ceoyJ

[58]. Patidar, M., Shrivastava, A., Miah, S., Kumar, Y., & Sivaraman, A. K. (2022). An energy efficient high-speed quantum-dot based full adder design and parity gate for nano application. *Materials Today: Proceedings*, *62*, 4880-4890.

https://doi.org/10.1016/j.matpr.2022.03.532

[59]. Gitte, M., Bawaskar, H., Sethi, S., & Shinde, A. (2014). Content based video retrieval system. *International Journal of Research in Engineering and Technology*, *3*(06), 123-129. https://scholar.google.co.in/citations?view_op=view_citation&hl=en&user=XlLBRR4AAAAJ&citation_for_view=XlLBRR4AAAAJ:u5HHmVD_uO8C

[60]. Shivakumar, S. K., & Sethii, S. (2019). *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*. Apress.

https://shorturl.at/bdFQ9

[61]. Sethi, S., & Panda, S. (2024). Transforming Digital Experiences: The Evolution of Digital Experience Platforms (DXPs) from Monoliths to Microservices: A Practical Guide. *Journal of Computer and Communications*, *12*(2), 142-155.

DOI: https://doi.org/10.4236/jcc.2024.122009

[62]. Sethi, S. (2018). Healthcare blockchain leads to transform healthcare industry. *International Journal of Advance Research, Ideas and Innovations in Technology*, *4*(1), 607-608.

[62]. Sethi, S., & Shivakumar, S. K. (2023). DXPs Digital Experience Platforms Transforming Fintech Applications: Revolutionizing Customer Engagement and Financial Services. *International Journal of Advance Research, Ideas and Innovations in Technology*, *9*, 419-423.

[63]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., & Sethii, S. (2019). DXP Security. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 183-200.

DOI https://doi.org/10.1007/978-1-4842-4303-9_6

[64]. Sethi, S., & Panda, S. (2023). The Evolution of Monolithic DXPs to Microservice based DXPs. *Authorea Preprints*.

DOI https://doi.org/10.36227/techrxiv.24328504.v1

[65]. Sethi, S., Panda, S., & Kamuru, R. (2023). Comparative study of middle tier caching solution. *International Journal of Development Research*, *13*(11), 64225-64229.

[66]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., & Sethii, S. (2019). Designing the Integration Layer. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 149-179.

DOI https://doi.org/10.1007/978-1-4842-4303-9_5

[67]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., & Sethii, S. (2019). DXP Performance Optimization. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 235-259.

DOI https://doi.org/10.1007/978-1-4842-4303-9_9

[68]. Shivakumar, S. K., & Sethii, S. (2019). Building Digital Experience Platforms.

https://link.springer.com/book/10.1007/978-1-4842-4303-9

[69]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., & Sethii, S. (2019). Quality Attributes and Sizing of the DXP. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 215-234.

DOI https://doi.org/10.1007/978-1-4842-4303-9_8

[70]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., & Sethii, S. (2019). End to End DXP Case Study. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 299-320.

DOI https://doi.org/10.1007/978-1-4842-4303-9_11

[71]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., & Sethii, S. (2019). Transforming legacy banking applications to banking experience platforms. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 261-295.

DOI https://doi.org/10.1007/978-1-4842-4303-9_10

[72]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., & Sethii, S. (2019). DXP Information Security. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 201-212.

DOI https://doi.org/10.1007/978-1-4842-4303-9_7

[73]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., & Sethii, S. (2019). Introduction to Digital Experience Platforms. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 3-26.

DOI https://doi.org/10.1007/978-1-4842-4303-9_1

[74]. Sethi, S. (2023). Platforms Based Approach and Strategy for Fintech applications. *Authorea Preprints*.

DOI https://doi.org/10.36227/techrxiv.24329533.v1

[75]. Sarkar, M., Puja, A. R., & Chowdhury, F. R. (2024). Optimizing Marketing Strategies with RFM Method and K-Means Clustering-Based AI Customer Segmentation Analysis. *Journal of Business and Management Studies*, *6*(2), 54-60.

[76]. Gazi, M. S. (2024). Optimizing Regional Business Performance: Leveraging Business and Data Analytics in Logistics & Supply Chain Management for USA's Sustainable Growth. *Journal of Business and Management Studies*, *6*(2), 144-152.

[77]. Islam, M. Z., Gurung, N., & Gazi, M. S. (2024). Novel AI-Powered Dynamic Inventory Management Algorithm in the USA: Machine Learning Dimension. *Journal of Economics, Finance and Accounting Studies*, *6*(2), 156-168.