International Journal of Business, Management and Visuals (IJBMV), ISSN: 3006-2705
Volume 6, Issue 2, July-December, 2023, Available online at: https://ijbmv.com

Encrypted AI for Predictive Maintenance in Industrial IoT

Ohad M

T A University, Israel

ABSTRACT

In the realm of Industrial Internet of Things (IoT), predictive maintenance plays a pivotal role in optimizing operational efficiency and minimizing downtime. However, the sensitive nature of data involved in predictive maintenance poses significant challenges in terms of privacy and security. This abstract explores the integration of encrypted artificial intelligence (AI) techniques to address these challenges effectively. Encrypted AI leverages advanced cryptographic protocols to enable the analysis of sensitive industrial data while preserving its confidentiality. By employing techniques such as homomorphic encryption and secure multi-party computation, encrypted AI allows computations on encrypted data without exposing the raw information to unauthorized parties. This approach facilitates the application of sophisticated machine learning models for predictive maintenance tasks without compromising data privacy.

Key benefits of encrypted AI in predictive maintenance include enhanced security against data breaches and unauthorized access, compliance with stringent data privacy regulations (such as GDPR), and the ability to collaborate securely across distributed IoT environments. Moreover, it enables industrial enterprises to leverage the full potential of AI-driven predictive analytics while maintaining control over their sensitive operational data.
This abstract underscores the transformative potential of encrypted AI in revolutionizing predictive maintenance strategies within Industrial IoT ecosystems, paving the way for more secure, efficient, and privacy-preserving industrial operations in the digital age.

Keywords: Encrypted AI, Predictive Maintenance, Industrial IoT, Data Privacy, Security

INTRODUCTION

In the era of Industrial Internet of Things (IoT), the practice of predictive maintenance stands as a cornerstone for optimizing operational efficiency and minimizing downtime in industrial settings. However, the criticality of data involved in predictive maintenance necessitates robust measures to safeguard privacy and ensure security.

This introduction explores the integration of encrypted artificial intelligence (AI) as a transformative solution to address these challenges effectively. Encrypted AI employs advanced cryptographic techniques to enable the analysis of sensitive industrial data while maintaining its confidentiality.

By utilizing methods such as homomorphic encryption and secure multi-party computation, encrypted AI allows computations on encrypted data without exposing raw information to unauthorized entities. This approach facilitates the application of sophisticated machine learning models for predictive maintenance tasks while preserving data privacy.

This introduction highlights the pivotal role of encrypted AI in revolutionizing predictive maintenance strategies within Industrial IoT environments, offering enhanced security against data breaches, compliance with regulatory frameworks, and the ability to collaborate securely across distributed IoT ecosystems. It sets the stage for exploring how encrypted AI can empower industrial enterprises to harness the full potential of AI-driven predictive analytics while safeguarding sensitive operational data.

LITERATURE REVIEWS

1. **Overview of Predictive Maintenance in Industrial IoT**: Provide a background on the importance of predictive maintenance in industrial settings, emphasizing its role in reducing downtime, optimizing resource allocation, and improving overall operational efficiency.

2. **Challenges of Data Privacy and Security**: Discuss the specific challenges related to data privacy and security in the context of predictive maintenance within Industrial IoT environments. Highlight concerns such as unauthorized access, data breaches, and compliance with privacy regulations (e.g., GDPR).
3. **Introduction to Encrypted AI**: Explain the concept of encrypted AI, including its underlying principles such as homomorphic encryption and secure multi-party computation. Describe how these techniques enable computations on encrypted data while preserving data confidentiality.
4. **Applications of Encrypted AI in Industrial IoT**: Review existing literature on the application of encrypted AI in various industrial sectors, focusing on predictive maintenance tasks. Highlight case studies or examples where encrypted AI has been successfully applied to enhance data privacy and security while enabling effective predictive maintenance strategies.
5. **Benefits and Limitations**: Analyze the benefits of using encrypted AI for predictive maintenance, such as enhanced security, compliance with privacy regulations, and improved trust among stakeholders. Discuss any limitations or challenges associated with implementing encrypted AI in real-world industrial IoT environments.
6. **Comparative Analysis**: Provide a comparative analysis of different approaches to securing sensitive data in predictive maintenance, contrasting traditional methods with encrypted AI techniques. Evaluate the strengths and weaknesses of each approach based on current research findings.
7. **Future Directions and Research Opportunities**: Propose future research directions in the field of encrypted AI for predictive maintenance within Industrial IoT. Identify potential areas for innovation, such as improving computational efficiency, scalability, or integrating additional security measures.

By synthesizing these points, your literature review can provide a comprehensive overview of current research and insights into the role of encrypted AI in advancing predictive maintenance practices while addressing data privacy and security concerns in Industrial IoT environments.

THEORETICAL FRAMEWORK

1. **Predictive Maintenance in Industrial IoT**: Begin by defining predictive maintenance and its significance in industrial IoT contexts. Discuss the traditional approaches to predictive maintenance and their limitations in terms of data security and privacy.
2. **Data Privacy and Security Challenges**: Explore the specific challenges related to data privacy and security in industrial IoT environments, including concerns about data breaches, unauthorized access, and regulatory compliance (e.g., GDPR).
3. **Introduction to Encrypted AI**: Provide a theoretical overview of encrypted AI techniques, such as homomorphic encryption and secure multi-party computation. Explain how these cryptographic methods enable computations on encrypted data while preserving data confidentiality and integrity.
4. **Theoretical Foundations of AI and Machine Learning**: Discuss foundational concepts of AI and machine learning relevant to predictive maintenance, such as supervised learning algorithms, anomaly detection, and predictive modeling. Emphasize the need for robust data analysis techniques while maintaining data privacy.
5. **Integration of Encrypted AI in Predictive Maintenance**: Outline how encrypted AI can be integrated into predictive maintenance workflows within industrial IoT environments. Discuss theoretical frameworks for deploying encrypted AI models for tasks like fault detection, anomaly prediction, and condition monitoring.
6. **Benefits of Encrypted AI**: Explore theoretical benefits of using encrypted AI for predictive maintenance, such as enhanced data security, compliance with privacy regulations, and improved trust among stakeholders. Discuss theoretical scenarios where encrypted AI could provide superior performance compared to traditional approaches.
7. **Theoretical Framework for Implementation**: Propose a theoretical framework for implementing encrypted AI in industrial IoT settings. Include considerations such as computational efficiency, scalability, and integration with existing IoT infrastructure. Discuss theoretical models for evaluating the performance and effectiveness of encrypted AI solutions in real-world applications.
8. **Theoretical Perspectives on Future Directions**: Consider theoretical perspectives on future directions and research opportunities in the field of encrypted AI for predictive maintenance. Identify potential theoretical advancements, such as improving algorithmic efficiency, enhancing data resilience, or exploring novel cryptographic techniques.

By constructing a robust theoretical framework encompassing these elements, you can provide a comprehensive basis for understanding the theoretical underpinnings and potential applications of encrypted AI in enhancing predictive maintenance practices within industrial IoT environments while addressing data security and privacy concerns.

RESEARCH PROCESS

1. **Research Objectives and Hypotheses**: Clearly define the research objectives and hypotheses. Outline the specific goals of the study, such as evaluating the effectiveness of encrypted AI in predictive maintenance tasks while ensuring data privacy and security.
2. **Selection of Industrial IoT Environment**: Describe the industrial IoT environment or setting where the research will be conducted. Specify the type of industry (e.g., manufacturing, energy, transportation) and the specific equipment or systems involved in predictive maintenance.
3. **Data Collection and Preparation**: Detail the process of collecting relevant data for the study. Discuss the types of data sources (e.g., sensor data, maintenance logs) and methods for acquiring and preparing the data for analysis. Address data anonymization or pseudonymization procedures to protect sensitive information.
4. **Implementation of Encrypted AI Techniques**: Explain how encrypted AI techniques, such as homomorphic encryption or secure multi-party computation, will be implemented in the experimental setup. Outline the theoretical framework for deploying these techniques to perform predictive maintenance tasks while preserving data privacy.
5. **Experimental Design**: Specify the experimental design, including the selection of AI models or algorithms for predictive maintenance (e.g., machine learning classifiers, anomaly detection methods). Detail how encrypted AI will be integrated into the predictive maintenance workflow and compare it with traditional, non-encrypted approaches.
6. **Evaluation Metrics**: Define the metrics and criteria used to evaluate the performance of the encrypted AI approach. Consider metrics such as accuracy, precision, recall, and computational overhead. Discuss theoretical models for assessing the effectiveness and efficiency of encrypted AI solutions compared to traditional methods.
7. **Ethical Considerations**: Address ethical considerations related to data privacy, security, and compliance with regulatory frameworks (e.g., GDPR). Discuss theoretical frameworks for ensuring ethical conduct throughout the research process, including obtaining informed consent and protecting participants' rights.
8. **Data Analysis and Interpretation**: Outline the methods for analyzing the experimental results and interpreting findings. Discuss theoretical frameworks for comparing the performance and security aspects of encrypted AI versus non-encrypted approaches in predictive maintenance tasks.
9. **Discussion and Implications**: Provide theoretical perspectives on the implications of the research findings for industrial IoT applications. Discuss theoretical implications for advancing data privacy and security in predictive maintenance practices using encrypted AI.
10. **Future Research Directions**: Propose theoretical perspectives on future research directions and potential advancements in the field of encrypted AI for predictive maintenance. Identify theoretical opportunities for improving algorithmic efficiency, scalability, and practical implementation of encrypted AI techniques in industrial IoT environments.

By outlining these components, you can construct a comprehensive theoretical framework for conducting research or setting up experiments to investigate the application of encrypted AI in predictive maintenance within industrial IoT contexts.

COMPARATIVE ANALYSIS

Aspect	**Traditional Approaches**	**Encrypted AI Approaches**
Data Privacy	Relies on data anonymization and access controls.	Uses advanced encryption techniques (e.g., homomorphic encryption, secure multi-party computation) to perform computations on encrypted data without exposing raw information.
Security	Vulnerable to data breaches and unauthorized access.	Enhances security by protecting data at rest and in transit with strong cryptographic protocols. Enables secure data analysis and computation while preserving confidentiality.
Compliance	May require additional measures to comply with regulations (e.g., GDPR).	Facilitates compliance with stringent data privacy regulations (e.g., GDPR) by ensuring that sensitive data remains encrypted during processing.
Computational Overhead	Generally lower computational overhead.	Introduces higher computational overhead due to encryption and decryption processes. Requires efficient implementation to minimize impact on performance.
Performance	Offers standard performance in	Performance may be impacted by encryption-related

	data analysis tasks.	computations, but advancements in algorithms and hardware are addressing this challenge.
Data Utilization	Uses raw data for analysis, potentially risking exposure.	Operates on encrypted data, preserving data confidentiality while enabling meaningful analysis and predictive maintenance tasks.
Implementation Complexity	Relatively straightforward to implement.	Requires expertise in cryptography and specialized frameworks for implementing encrypted AI techniques.
Trust and Transparency	Relies on organizational controls and data governance.	Enhances trust through transparent use of cryptographic methods and adherence to privacy-preserving principles. Ensures transparency in data handling and processing.
Scalability	Generally scalable depending on infrastructure.	Scalability may be challenged by the computational demands of encrypted AI techniques, but advancements are improving scalability.
Cost Considerations	Lower initial costs for implementation and maintenance.	Higher initial costs due to specialized expertise and potential computational resources. Long-term benefits include enhanced security and compliance.

This table provides a comparative overview of how traditional approaches to predictive maintenance in industrial IoT environments contrast with the use of encrypted AI techniques. It highlights key aspects such as data privacy, security, compliance, performance, implementation complexity, and scalability, illustrating the trade-offs and benefits of adopting encrypted AI for enhancing data privacy and security in predictive maintenance practices.

RESULTS & ANALYSIS

1. **Data Collection and Preparation**
    - Describe the dataset used, including types of data (e.g., sensor readings, maintenance logs), sources, and size.
    - Explain any preprocessing steps undertaken, such as data cleaning, normalization, and anonymization/pseudonymization procedures to ensure data privacy.
2. **Implementation of Encrypted AI**
    - Detail the implementation of encrypted AI techniques (e.g., homomorphic encryption, secure multi-party computation) in the predictive maintenance workflow.
    - Discuss the integration of encrypted AI models/algorithms for tasks such as fault detection, anomaly prediction, and condition monitoring.
3. **Evaluation Metrics**
    - Present the metrics used to evaluate the performance of the encrypted AI approach, such as accuracy, precision, recall, and computational overhead.
    - Compare these metrics with those obtained from traditional, non-encrypted approaches to highlight differences in performance and computational impact.
4. **Performance Evaluation**
    - Analyze the performance of the encrypted AI models/algorithms in predictive maintenance tasks.
    - Discuss any observed improvements or challenges in terms of predictive accuracy, detection of anomalies, and overall efficiency compared to traditional methods.
5. **Security and Privacy Analysis**
    - Evaluate the effectiveness of encrypted AI in enhancing data security and privacy protection.
    - Discuss how encrypted AI mitigates risks associated with data breaches and unauthorized access, ensuring compliance with regulatory frameworks (e.g., GDPR).
6. **Computational Overhead**
    - Assess the computational overhead introduced by encrypted AI techniques.
    - Discuss strategies employed to optimize performance and reduce computational costs while maintaining data privacy and security.
7. **Discussion of Findings**
    - Interpret the results in the context of theoretical frameworks and existing literature on encrypted AI for predictive maintenance.
    - Highlight theoretical implications of the findings for industrial IoT applications, including implications for data privacy, security, and operational efficiency.

8. **Limitations and Challenges**
    - Identify limitations encountered during the study, such as constraints related to dataset availability, computational resources, or implementation complexity.
    - Discuss theoretical challenges and areas for improvement in deploying encrypted AI for predictive maintenance in real-world industrial IoT environments.
9. **Future Directions**
    - Propose theoretical perspectives on future research directions and potential advancements in the field.
    - Identify theoretical opportunities for enhancing algorithmic efficiency, scalability, and practical implementation of encrypted AI techniques in industrial IoT settings.
10. **Conclusion**
    - Summarize the theoretical contributions and practical implications of the study's findings.
    - Reinforce the theoretical importance of encrypted AI for advancing predictive maintenance practices while safeguarding data privacy and security in industrial IoT environments.

By structuring your results and analysis in this manner, you can provide a comprehensive theoretical framework for understanding the impact and effectiveness of encrypted AI in predictive maintenance within industrial IoT contexts.

SIGNIFICANCE OF THE TOPIC

The significance of "Encrypted AI for Predictive Maintenance in Industrial IoT" lies in its potential to address critical challenges and unlock opportunities in industrial operations. Here are key points highlighting its importance:

1. **Enhanced Data Security**: Industrial IoT environments generate vast amounts of sensitive data from machinery and systems. Protecting this data against cyber threats, data breaches, and unauthorized access is paramount. Encrypted AI offers a robust solution by enabling secure data analysis and predictive maintenance while preserving data confidentiality through advanced cryptographic techniques.
2. **Compliance with Data Privacy Regulations**: Regulations like GDPR impose strict requirements on data handling and privacy protection. Encrypted AI ensures compliance by allowing organizations to perform predictive maintenance tasks on encrypted data, thereby mitigating risks of non-compliance and potential legal repercussions.
3. **Optimized Operational Efficiency**: Predictive maintenance powered by AI can significantly reduce downtime, optimize resource allocation, and extend the lifespan of industrial equipment. By integrating encrypted AI, organizations can achieve these benefits while maintaining control over sensitive operational data, ensuring continuous operations and efficiency improvements.
4. **Trust and Transparency**: Implementing encrypted AI fosters trust among stakeholders, including employees, customers, and regulatory bodies. It demonstrates a commitment to data privacy and security, enhancing organizational reputation and minimizing risks associated with data misuse or unauthorized access.
5. **Innovation in Industrial IoT**: Encrypted AI represents a frontier in innovation within the industrial IoT landscape. It encourages the adoption of advanced technologies while addressing inherent challenges related to data privacy and security, paving the way for more sophisticated and resilient industrial IoT ecosystems.
6. **Long-term Cost Savings**: While initial implementation of encrypted AI may involve investment in specialized expertise and infrastructure, the long-term benefits outweigh the costs. Enhanced security and operational efficiency contribute to reduced maintenance costs, increased productivity, and sustainable business growth.
7. **Scalability and Future-proofing**: As industrial IoT continues to expand, scalability becomes crucial. Encrypted AI solutions are designed to scale with growing data volumes and evolving cybersecurity threats, providing a future-proof framework for sustainable development and technological advancement.

In summary, the significance of "Encrypted AI for Predictive Maintenance in Industrial IoT" lies in its ability to integrate cutting-edge technology with stringent data privacy requirements, thereby enhancing operational resilience, regulatory compliance, and overall competitiveness in industrial sectors. By embracing encrypted AI, organizations can unlock new opportunities for innovation and sustainable growth while safeguarding critical industrial data.

LIMITATIONS & DRAWBACKS

While "Encrypted AI for Predictive Maintenance in Industrial IoT" offers significant advantages, it also faces several limitations and drawbacks that merit consideration:

1. **Computational Overhead**: Implementing encrypted AI introduces additional computational complexity and overhead. Encryption and decryption processes can increase latency and resource consumption, potentially impacting real-time predictive maintenance tasks and overall system performance.
2. **Complexity of Implementation**: Integrating encrypted AI requires specialized expertise in cryptography and AI technologies. The complexity of implementation may pose challenges in terms of deployment, maintenance, and integration with existing industrial IoT infrastructure.
3. **Trade-offs in Performance**: Despite advancements, encrypted AI may not always match the performance of non-encrypted AI approaches. The need for computations on encrypted data can limit the types of AI models and algorithms that can be effectively deployed, potentially compromising predictive accuracy and efficiency.
4. **Data Accessibility and Usability**: Encrypted data is inherently less accessible and usable for analysis compared to plaintext data. Analyzing encrypted data may require specific tools and frameworks, limiting the flexibility and agility of data-driven decision-making processes in industrial environments.
5. **Scalability Concerns**: Scaling encrypted AI solutions across large-scale industrial IoT deployments can be challenging. Managing encrypted data streams, ensuring consistent performance across distributed systems, and maintaining data integrity at scale require robust infrastructure and planning.
6. **Cost Considerations**: Initial investment in encrypted AI technologies, including infrastructure, software, and expertise, can be substantial. Organizations must weigh these upfront costs against long-term benefits such as enhanced security and regulatory compliance.
7. **Integration with Legacy Systems**: Many industrial IoT environments operate using legacy systems that may not readily support encrypted AI technologies. Retrofitting existing systems to accommodate encrypted data processing and analysis may require significant effort and resources.
8. **Regulatory and Compliance Issues**: While encrypted AI enhances data privacy, it also introduces complexities related to regulatory compliance. Organizations must navigate compliance requirements such as data localization laws and industry-specific regulations while leveraging encrypted AI for predictive maintenance.
9. **Risk of Misconfiguration or Vulnerabilities**: Improper implementation or configuration of encrypted AI systems can introduce security vulnerabilities or errors that compromise data privacy and operational integrity. Regular audits and robust security protocols are essential to mitigate these risks.
10. **User Acceptance and Adoption**: Encrypted AI may face resistance or skepticism from stakeholders accustomed to traditional, non-encrypted approaches. Educating and gaining acceptance among users, management, and regulatory bodies about the benefits and safeguards of encrypted AI is crucial for successful adoption.

Addressing these limitations requires careful planning, strategic investment in technology and expertise, and continuous evaluation of encrypted AI solutions in real-world industrial IoT environments. Despite these challenges, overcoming them can lead to significant improvements in data security, privacy protection, and operational efficiency within industrial settings.

CONCLUSION

"Encrypted AI for Predictive Maintenance in Industrial IoT" represents a transformative approach to balancing data privacy and operational efficiency in industrial settings. Throughout this exploration, several key insights and implications have emerged:

1. **Enhanced Data Privacy and Security**: By leveraging advanced cryptographic techniques like homomorphic encryption and secure multi-party computation, encrypted AI ensures that sensitive industrial data remains confidential during predictive maintenance operations. This not only mitigates risks of data breaches and unauthorized access but also facilitates compliance with stringent data privacy regulations.
2. **Operational Efficiency and Reliability**: Integrating encrypted AI into predictive maintenance workflows enables industrial enterprises to optimize operational efficiency, reduce downtime, and extend the lifespan of critical equipment. These improvements translate into significant cost savings and enhanced operational reliability.
3. **Challenges and Considerations**: However, the adoption of encrypted AI is not without challenges. Organizations must navigate complexities related to computational overhead, implementation costs, and integration with existing systems. Addressing these challenges requires strategic planning, investment in technology infrastructure, and ongoing evaluation of performance metrics.
4. **Future Directions**: Looking ahead, further research and development are needed to enhance the scalability, usability, and performance of encrypted AI solutions in industrial IoT environments. Innovations in algorithmic efficiency, hardware acceleration, and interoperability with legacy systems will play pivotal roles in advancing the adoption and effectiveness of encrypted AI for predictive maintenance.

5. **Strategic Implications**: Embracing encrypted AI not only strengthens data security practices but also fosters trust among stakeholders and enhances organizational resilience in an increasingly digitized and interconnected industrial landscape. By prioritizing data privacy alongside operational excellence, industrial enterprises can position themselves competitively while safeguarding sensitive information.

In conclusion, "Encrypted AI for Predictive Maintenance in Industrial IoT" represents a theoretical framework and practical pathway towards achieving sustainable innovation and secure data-driven decision-making in industrial operations. By overcoming challenges, embracing technological advancements, and adhering to ethical principles, organizations can harness the full potential of encrypted AI to drive value, efficiency, and trust in the industrial IoT ecosystem.

REFERENCES

[1]. Acar, A. (2020). Industrial Internet of Things (IIoT) and artificial intelligence for predictive maintenance and remote monitoring in manufacturing. In Proceedings of the 3rd International Conference on Electrical, Communication and Computer Engineering (ICECCE) (pp. 1-6).

[2]. Jatin Vaghela, A Comparative Study of NoSQL Database Performance in Big Data Analytics. (2017). International Journal of Open Publication and Exploration, ISSN: 3006-2853, 5(2), 40-45. https://ijope.com/index.php/home/article/view/110

[3]. Akinyelu, A., & Uzoma, O. (2020). Security and privacy concerns in industrial Internet of Things (IIoT) environment: A review. Journal of Information Security and Applications, 50, 102421.

[4]. Al-Makhadmeh, Z. M., & Karray, F. (2021). A comprehensive review on homomorphic encryption. Journal of King Saud University - Computer and Information Sciences.

[5]. Goswami, Maloy Jyoti. "Challenges and Solutions in Integrating AI with Multi-Cloud Architectures." International Journal of Enhanced Research in Management & Computer Applications ISSN: 2319-7471, Vol. 10 Issue 10, October, 2021.

[6]. Bera, S., & Venkatasubramanian, N. (2019). Secure and privacy-preserving predictive maintenance of IoT systems using blockchain and federated learning. In Proceedings of the 2019 IEEE International Conference on Big Data (pp. 5045-5052).

[7]. Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the Internet of Things. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing (pp. 13-16).

[8]. Anand R. Mehta, Srikarthick Vijayakumar. (2018). Unveiling the Tapestry of Machine Learning: From Basics to Advanced Applications. International Journal of New Media Studies: International Peer Reviewed Scholarly Indexed Journal, 5(1), 5–11. Retrieved from https://ijnms.com/index.php/ijnms/article/view/180

[9]. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Zeitzoff, T. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv preprint arXiv:1802.07228.

[10]. Buchmann, N., Döttling, N., Herold, G., Rupp, A., & Zimmermann, J. (2017). Secure two-party computation for privacy-preserving predictive analytics. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 1877-1894).

[11]. Neha Yadav, Vivek Singh, “Probabilistic Modeling of Workload Patterns for Capacity Planning in Data Center Environments” (2022). International Journal of Business Management and Visuals, ISSN: 3006-2705, 5(1), 42-48. https://ijbmv.com/index.php/home/article/view/73

[12]. Chaki, R., & Hasan, R. (2020). Secure and energy efficient data analytics in cloud-assisted industrial IoT environment. Journal of Ambient Intelligence and Humanized Computing, 11(6), 2319-2332.

[13]. Chen, L., & Zhao, H. (2021). A novel privacy-preserving predictive maintenance framework for industrial IoT based on edge computing. Journal of Ambient Intelligence and Humanized Computing, 12(5), 5583-5596.

[14]. Choi, B. J., Lee, J. H., Kim, M. H., & Lee, J. J. (2020). Real-time anomaly detection in smart manufacturing using a deep-learning approach with encrypted data. Journal of Manufacturing Systems, 54, 239-249.

[15]. Bharath Kumar. (2022). AI Implementation for Predictive Maintenance in Software Releases. International Journal of Research and Review Techniques, 1(1), 37–42. Retrieved from https://ijrrt.com/index.php/ijrrt/article/view/175

[16]. Dua, A., & Singh, D. (2020). A comparative study on predictive maintenance techniques for industrial IoT. International Journal of Intelligent Systems Technologies and Applications, 19(1), 47-65.

[17]. El-Hajj, M., & Chehab, A. (2020). A survey of predictive maintenance: Key insights and contributions. IEEE Access, 8, 18016-18063.

[18]. Gharibi, W., Sakurai, K., & Kanai, Y. (2020). Privacy-preserving prediction for IoT-based systems: A survey. IEEE Access, 8, 93993-94011.

[19]. Sravan Kumar Pala. (2016). Credit Risk Modeling with Big Data Analytics: Regulatory Compliance and Data Analytics in Credit Risk Modeling. (2016). International Journal of Transcontinental Discoveries, ISSN: 3006-628X, 3(1), 33-39.

[20]. Goswami, Maloy Jyoti. "Study on Implementing AI for Predictive Maintenance in Software Releases." International Journal of Research Radicals in Multidisciplinary Fields, ISSN: 2960-043X 1.2 (2022): 93-99.

[21]. Gilad-Bachrach, R., Dowlin, N., Laine, K., Lauter, K., Naehrig, M., & Wernsing, J. (2016). Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy. In Proceedings of the 33rd International Conference on Machine Learning (pp. 201-210).

[22]. Li, Y., & Da Xu, L. (2021). Privacy-preserving deep learning for edge computing in industrial IoT. IEEE Transactions on Industrial Informatics, 17(6), 4140-4149.

[23]. Sravan Kumar Pala, Investigating Fraud Detection in Insurance Claims using Data Science, International Journal of Enhanced Research in Science, Technology & Engineering ISSN: 2319-7463, Vol. 11 Issue 3, March-2022.

[24]. Lopez, J., Fernandez, D., Marcano, A., Mora, F., & Monzo, C. (2019). Survey of predictive maintenance and condition monitoring techniques based on industrial IoT. Sensors, 19(11), 2483.

[25]. Luo, S., Gao, F., & Wang, H. (2018). Homomorphic encryption-based secure big data storage and computation in Industrial Internet of Things. Journal of Network and Computer Applications, 112, 22-31.

[26]. Kuldeep Sharma, Ashok Kumar, “Innovative 3D-Printed Tools Revolutionizing Composite Non-destructive Testing Manufacturing”, International Journal of Science and Research (IJSR), ISSN: 2319-7064 (2022). Available at: https://www.ijsr.net/archive/v12i11/SR231115222845.pdf

[27]. Mohassel, P., & Zhang, Y. (2017). SecureML: A system for scalable privacy-preserving machine learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 1223-1238).

[28]. Samir, K. C., Park, Y., & Kim, J. H. (2019). A survey on fog computing for the Internet of Things. Journal of Supercomputing, 75(3), 1296-1310.