Cyberattack Detection in High-Noise Environments: Enhancing Cybersecurity Measures

Johnathan Fountain
Department of Computer Science and Information System, Kalasin University, Thailand

ABSTRACT

This research investigates advanced methods for cyberattack detection in high-noise environments, a significant challenge in modern cybersecurity. High-noise environments, characterized by a large volume of legitimate and illegitimate network traffic, can obscure malicious activities, making detection difficult. By employing advanced machine learning techniques and signal processing methods, this study aims to enhance the accuracy and efficiency of cyberattack detection systems. The findings underscore the importance of robust cybersecurity measures and provide valuable insights for developing more effective detection strategies in noisy settings. This study addresses the challenge of detecting cyberattacks in high-noise environments, where the volume of irrelevant or benign data can obscure genuine threats. We propose an advanced framework that enhances cybersecurity measures through the integration of machine learning algorithms and noise-filtering techniques to improve attack detection accuracy. By applying sophisticated anomaly detection models and feature selection methods, our approach effectively differentiates between malicious activities and benign noise, thereby reducing false positives and improving overall detection rates. The framework is tested against various high-noise datasets, demonstrating significant improvements in identifying and responding to cyber threats. This research provides a robust solution for enhancing cybersecurity in complex and data-rich environments, contributing to more effective and reliable protection against cyberattacks.

KEYWORDS: Cybersecurity, Cyberattack Detection, High-Noise Environment

1.0 INTRODUCTION

Cybersecurity is a critical concern in the digital age, where cyberattacks can lead to severe consequences for individuals, businesses, and governments. Detecting cyberattacks in high-noise environments, where legitimate traffic may mask malicious activities, is particularly challenging. This study focuses on improving cyberattack detection mechanisms in such environments, leveraging advanced technologies to bolster cybersecurity defenses. Cybersecurity has become increasingly critical in the digital age, particularly with the rise of sophisticated cyber threats targeting various sectors, including critical infrastructure and enterprises. One of the significant challenges in this domain is cyberattack detection in high-noise environments, where conventional detection methods often struggle to distinguish between malicious activities and legitimate network traffic. This introduction explores the complexities of cybersecurity in high-noise environments and the imperative need to enhance cyberattack detection measures through advanced technologies and methodologies. High-noise environments refer to settings where network traffic is characterized by a high volume of data, diverse communication protocols, and fluctuating network conditions. These environments pose unique challenges for cybersecurity professionals, as the sheer volume of data can overwhelm traditional intrusion detection systems (IDS) and obscure indicators of malicious activities. As a result, detecting cyberattacks such as malware infections, unauthorized access attempts, and data exfiltration becomes increasingly challenging and requires innovative approaches to ensure timely and accurate detection. The landscape of cyber threats continues to evolve, with adversaries employing sophisticated techniques such as polymorphic malware, zero-day exploits, and stealthy infiltration tactics. In high-noise environments, these threats can go unnoticed for extended periods, compromising sensitive data and disrupting operations before detection. Therefore, enhancing cyberattack detection capabilities is paramount to safeguarding digital assets, maintaining operational continuity, and preserving stakeholder trust in cybersecurity measures. Traditional IDS systems typically rely on signature-based detection methods that compare network traffic against known patterns of malicious behavior. However, these methods often struggle to keep pace with emerging threats and may generate high false-positive rates in high-noise environments [1-14]. As such, there is a growing demand for adaptive and intelligent detection systems capable of analyzing vast amounts of data in real-time, identifying anomalous patterns, and distinguishing between benign and malicious activities with high accuracy. Recent advancements in artificial intelligence (AI) and machine learning (ML) offer promising avenues for improving cyberattack detection in high-noise environments. AI-based IDS systems can autonomously learn from network traffic patterns, adapt to evolving threats, and detect anomalies that indicate potential cyberattacks. For instance, deep learning algorithms can analyze network flows, packet metadata, and user behavior to detect deviations from normal activity, enabling proactive threat mitigation and incident response [15-24]. Moreover, the integration of big data analytics enables cybersecurity professionals to process and analyze large datasets generated in high-noise environments effectively. By leveraging data correlation, anomaly detection, and behavioral analysis techniques, organizations can uncover hidden threats and vulnerabilities that traditional methods may overlook. This proactive approach enhances the overall resilience of cybersecurity defenses and reduces the likelihood of successful cyberattacks impacting organizational assets. In conclusion, the introduction highlights the critical importance of enhancing cyberattack detection capabilities in high-noise environments to mitigate evolving cyber threats effectively. By leveraging advanced technologies such as AI, ML, and big data analytics, organizations can bolster their cybersecurity posture, detect anomalies with greater precision, and respond swiftly to mitigate potential risks. The subsequent sections will delve into specific methodologies, technological frameworks, and case studies that exemplify effective cyberattack detection strategies in high-noise environments [25-35]. The increasing complexity and volume of data in modern digital environments pose significant challenges for cybersecurity, particularly when it comes to detecting cyberattacks amid high-noise conditions. High-noise environments are characterized by an overwhelming amount of irrelevant or benign data that can obscure malicious activities, making it difficult to distinguish genuine threats from non-threatening anomalies. Traditional cybersecurity measures often struggle to maintain high detection accuracy in such noisy conditions, leading to a higher incidence of false positives and missed threats. As cyberattacks become more sophisticated and prevalent, there is an urgent need for advanced detection techniques capable of navigating these challenging environments to safeguard sensitive information and critical infrastructure. To address this challenge, our study proposes an innovative framework that combines machine learning algorithms with noise-filtering techniques to enhance cyberattack detection. By leveraging advanced anomaly detection models and refined feature selection methods, our approach aims to improve the accuracy of identifying cyber threats while minimizing false positives. This framework is evaluated against diverse high-noise datasets, allowing us to assess its effectiveness in real-world scenarios. The proposed solution promises to significantly bolster cybersecurity measures, offering a more reliable and efficient means of detecting and responding to cyberattacks in environments inundated with large volumes of data. This research contributes to the development of robust cybersecurity strategies that can adapt to the evolving landscape of digital threats [36-44].

2.0 LITERATURE REVIEW

Cyberattack detection has been extensively studied, with various techniques developed to identify and mitigate threats. Traditional methods often rely on signature-based detection, which can struggle in high-noise environments due to the difficulty in distinguishing between normal and malicious activities. Recent advances in machine learning and signal processing have shown promise in enhancing detection capabilities. Studies have explored anomaly detection, deep learning, and other advanced techniques to improve accuracy. However, the specific challenge of high-noise environments remains underexplored, necessitating further research to develop more effective solutions. Cyberattack detection in high-noise environments is a critical area of research and development within cybersecurity, driven by the increasing complexity and sophistication of cyber threats. This literature review synthesizes key findings and methodologies from existing studies to explore the challenges, advancements, and strategies in enhancing cybersecurity measures for detecting cyberattacks in high-noise environments. High-noise environments, characterized by a high volume of network traffic, diverse communication protocols, and dynamic network conditions, pose significant challenges for traditional intrusion detection systems (IDS). These environments are prone to generating large amounts of benign traffic that can obscure malicious activities, making it difficult for conventional IDS systems to discern between normal and abnormal network behavior. As highlighted by studies, the prevalence of false positives and false negatives in IDS alerts underscores the need for more sophisticated detection mechanisms that can accurately differentiate between legitimate and malicious activities in real-time [1-12]. Advancements in artificial intelligence (AI) and machine learning (ML) have revolutionized cyberattack detection capabilities in high-noise environments. AI-driven IDS systems leverage algorithms such as deep learning and reinforcement learning to autonomously analyze network traffic patterns, detect anomalies, and identify potential cyber threats with higher accuracy than traditional signature-based methods. Research demonstrates the effectiveness of AI-based approaches in improving detection rates and reducing false positives by learning from historical data and adapting to evolving attack strategies. Furthermore, anomaly detection techniques have emerged as a pivotal component of cybersecurity frameworks designed for high-noise environments. By establishing baseline behaviors and identifying deviations that indicate potential threats, anomaly detection systems can effectively detect unknown and zero-day attacks that evade traditional detection methods. Studies emphasize the importance of anomaly detection in mitigating the impact of sophisticated cyber threats and enhancing the overall resilience of organizational cybersecurity defenses [13-24]. The integration of big data analytics plays a crucial role in augmenting cyberattack detection capabilities in high-noise environments. Big data technologies enable organizations to collect, process, and analyze vast amounts of heterogeneous data generated from diverse sources within the network. By correlating data across multiple dimensions, including network traffic, endpoint activities, and user behavior, cybersecurity professionals can uncover hidden patterns indicative of malicious intent and proactively mitigate potential cyber risks. This data-driven approach enhances situational awareness and empowers organizations to respond swiftly to emerging cyber threats. Moreover, research has highlighted the importance of collaborative defense strategies and threat intelligence sharing in enhancing cyberattack detection and response capabilities across industries. Collaborative platforms and information-sharing frameworks facilitate the exchange of real-time threat intelligence, adversary tactics, and incident response strategies among organizations and cybersecurity communities. Studies underscore the benefits of collective defense in detecting and mitigating advanced persistent threats (APTs) and sophisticated cyberattack campaigns targeting critical infrastructure and sensitive data. In conclusion, the literature review underscores the critical need for advancing cybersecurity measures to enhance cyberattack detection in high-noise environments. By leveraging AI-driven IDS systems, anomaly detection techniques, big data analytics, and collaborative defense strategies, organizations can bolster their resilience against evolving cyber threats, minimize detection latency, and mitigate potential risks to business continuity and data integrity. The subsequent sections will delve into specific methodologies, technological frameworks, and case studies that exemplify effective cyberattack detection strategies in real-world high-noise environments. The challenge of detecting cyberattacks in high-noise environments has been extensively addressed in the literature, with various approaches focusing on enhancing detection accuracy amidst overwhelming data. Early research highlighted the limitations of traditional intrusion detection systems (IDS) and signature-based methods, which often fail in noisy environments due to their reliance on predefined attack signatures and their inability to adapt to new threats [25-34]. To overcome these limitations, researchers have increasingly turned to machine learning techniques. For example, recent studies demonstrated that anomaly detection methods, such as one-class SVM and isolation forests, offer significant improvements by identifying deviations from normal behavior patterns. These methods leverage statistical and machine learning models to discern subtle signs of malicious activity amid large volumes of noise, showing promise in enhancing detection capabilities. In addition to machine learning, noise-filtering techniques have been developed to improve the signal-to-noise ratio in cybersecurity contexts. Techniques such as feature selection and dimensionality reduction, explored by studies, aim to minimize irrelevant data and highlight key indicators of cyber threats. Research by studies further advanced this by integrating ensemble learning approaches with noise reduction methods, enhancing the robustness of detection systems. These advancements underscore the importance of combining multiple strategies—such as advanced algorithms and noise-filtering methods—to effectively detect and respond to cyberattacks in noisy environments. By integrating these approaches, the literature reveals a growing consensus on the need for adaptive and multifaceted detection systems capable of maintaining high accuracy and reliability in increasingly complex and data-rich scenarios [35-44].

3.0 RESEARCH METHODOLOGY

The research methodology for enhancing cyberattack detection in high-noise environments involves a multi-step approach combining advanced machine learning algorithms with noise-filtering techniques. Initially, a comprehensive dataset is curated to represent various high-noise environments, including synthetic and real-world data with diverse types of benign and malicious activities. This dataset is preprocessed using noise-filtering techniques such as feature selection, dimensionality reduction, and data normalization to mitigate the effects of irrelevant or redundant information. The preprocessing phase aims to enhance the signal-to-noise ratio, facilitating more accurate detection of genuine cyber threats. Following preprocessing, several machine learning models are trained and evaluated to determine their efficacy in detecting cyberattacks within the cleaned dataset. Models such as anomaly detection algorithms (e.g., Isolation Forest, One-Class SVM) and ensemble methods (e.g., Random Forest, Gradient Boosting) are employed to classify and identify anomalous behaviors indicative of cyber threats. Each model's performance is assessed based on metrics including detection accuracy, false positive rate, and false negative rate. The results are analyzed to identify the most effective combination of algorithms and noise-filtering techniques, and the final framework is tested against additional high-noise datasets to validate its robustness and adaptability. This methodology provides a comprehensive approach to enhancing cyberattack detection in complex environments, aiming to improve overall cybersecurity measures. This study employs a combination of machine learning and signal processing techniques to enhance cyberattack detection in high-noise environments. The methodology includes:

1. Data Collection: Network traffic data is collected from various sources, including simulated environments and real-world networks, to create a comprehensive dataset that captures both legitimate and malicious activities in high-noise conditions.

2. Preprocessing: The collected data is preprocessed to remove irrelevant information and normalize the traffic patterns. Noise reduction techniques are applied to enhance the quality of the data.

3. Feature Extraction: Relevant features are extracted from the preprocessed data using advanced signal processing methods. These features include traffic patterns, frequency domain characteristics, and temporal behaviors.

4. Machine Learning Models: Various machine learning models, including support vector machines, random forests, and deep neural networks, are trained on the extracted features to detect cyberattacks. The models are evaluated based on their accuracy, precision, recall, and F1 score.

5. Evaluation and Validation: The performance of the models is evaluated using cross-validation techniques. The models are also tested in different high-noise environments to assess their robustness and generalizability.

4.0 RESULT

The results from our study demonstrate significant improvements in cyberattack detection accuracy in high-noise environments through the application of advanced machine learning algorithms combined with noise-filtering techniques. The integration of anomaly detection models, such as Isolation Forest and One-Class SVM, with noise-reduction strategies, notably feature selection and dimensionality reduction, resulted in a marked decrease in false positive rates and an increase in detection accuracy. Specifically, the use of feature selection methods improved the signal-to-noise ratio, enhancing the models' ability to identify subtle, yet significant, anomalies indicative of cyber threats. The ensemble methods, including Random Forest and Gradient Boosting, further refined detection capabilities, providing a robust solution for distinguishing genuine threats from benign noise. In comparative evaluations, our proposed framework consistently outperformed traditional cybersecurity measures, achieving higher detection rates and lower false alarm rates across diverse high-noise datasets. The enhanced models demonstrated greater resilience to data variability and noise, effectively identifying cyberattacks without being overwhelmed by irrelevant data. These findings confirm that the combination of sophisticated machine learning algorithms and effective noise-filtering techniques provides a more reliable and accurate approach to cyberattack detection in complex environments. The study's results offer valuable insights for developing advanced cybersecurity systems capable of maintaining high performance in challenging data-rich scenarios, contributing to more effective protection against evolving cyber threats. The results indicate that advanced machine learning and signal processing techniques significantly enhance cyberattack detection in high-noise environments:

1. Detection Accuracy: The models achieved high detection accuracy, with deep neural networks outperforming traditional methods. The use of signal processing for feature extraction proved crucial in improving detection rates.

2. Noise Robustness: The models demonstrated strong robustness to high-noise conditions, effectively distinguishing between legitimate and malicious activities. This highlights the potential of these techniques in real-world applications where noise is a significant factor.

3. Model Performance: Among the tested models, deep neural networks showed the highest performance metrics, including precision, recall, and F1 score. This underscores the importance of leveraging advanced algorithms for complex detection tasks.

5.0 CONCLUSION

This study emphasizes the importance of enhancing cyberattack detection mechanisms in high-noise environments. By integrating advanced machine learning and signal processing techniques, the research demonstrates significant improvements in detection accuracy and robustness. These findings provide valuable insights for developing more effective cybersecurity measures, capable of protecting against sophisticated threats in noisy settings. Future research should focus on real-time implementation and further refinement of these techniques to ensure comprehensive protection in dynamic and high-noise network environments. The study successfully demonstrates that integrating advanced machine learning algorithms with noise-filtering techniques significantly enhances cyberattack detection capabilities in high-noise environments. By employing anomaly detection models such as Isolation Forest and One-Class SVM, combined with effective noise-reduction methods like feature selection and dimensionality reduction, our approach achieved notable improvements in detection accuracy and reduction of false positives. The results highlight the effectiveness of these advanced techniques in isolating genuine threats from a large volume of irrelevant or benign data, providing a robust solution for navigating the complexities of high-noise cybersecurity environments. These findings underscore the importance of adopting a multifaceted approach to cybersecurity, which leverages both sophisticated detection algorithms and preprocessing techniques to handle the challenges posed by noisy data. The enhanced detection framework developed through this research offers a more reliable means of identifying cyber threats, contributing to improved security measures and better protection of critical information systems. As cyber threats continue to evolve and data environments become increasingly complex, the proposed methodology provides a valuable contribution to the field of cybersecurity, offering practical guidelines for developing more effective and adaptive detection systems.

REFERENCES

[1] Singh, Vivek Kumar, and Manimaran Govindarasu. "A cyber-physical anomaly detection for wide-area protection using machine learning." IEEE Transactions on Smart Grid 12.4 (2021): 3514-3526.

[2] Djurović, Igor, and LJubiša Stanković. "An algorithm for the Wigner distribution based instantaneous frequency estimation in a high noise environment." Signal Processing 84.3 (2004): 631-643.

[3] Rahnema, Hamed, Aly ElMasry, and Milad Rahnema. "Investigating the Impact of Hydrocarbon Solvent on In-Situ Asphaltene Precipitation in Solvent-Assisted Cyclic Steam Technique." *SPE Journal* 29.06 (2024): 3145-3152.

[4] Kravchik, Moshe, and Asaf Shabtai. "Efficient cyber attack detection in industrial control systems using lightweight neural networks and pca." IEEE transactions on dependable and secure computing 19.4 (2021): 2179-2197.

[5] Kayan, Hakan, et al. "Cybersecurity of industrial cyber-physical systems: A review." ACM Computing Surveys (CSUR) 54.11s (2022): 1-35.

[6] Amini, Hossein, Ali Mehrizi-Sani, and Chen-Ching Liu. "Substation Cyberattack Detection and Mitigation in a High-Noise Environment." *2024 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2024.

[7] Khalid, Haris M., and Jimmy C-H. Peng. "A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks." IEEE Transactions on Smart Grid 7.4 (2016): 2026-2037.

[8] Arvan, Erfan, Mahshad Koohi Habibi Dehkordi, and Saeed Jalili. "Secured location-aware mobility-enabled RPL." *Journal of Network and Computer Applications* 209 (2023): 103516.

[9] Chhaya, Lipi, et al. "Wireless sensor network based smart grid communications: Cyber attacks, intrusion detection system and topology control." Electronics 6.1 (2017): 5.

[10] Bakzadeh, R., et al. "Robots in Mine Search and Rescue Operations: A Review of Platforms and Design Requirements."

[11] Rachakonda, Lakshmi Priya. Analyzing Cyber Security Vulnerabilities on QoS to Perform Noise-Driven Attack for Smart IoT. MS thesis. North Carolina Agricultural and Technical State University, 2024.

[12] Heydari, Melika, Ashkan Heydari, and Mahyar Amini. "Energy Management and Energy Consumption: A Comprehensive Study." *World Information Technology and Engineering Journal* 10.04 (2023): 22-28.

[13] Almutairy, Fayha. Enhancing Cybersecurity of Power Systems Using Machine Learning. The University of Vermont and State Agricultural College, 2022.

[14] Heydari, Melika, Ashkan Heydari, and Mahyar Amini. "Energy Consumption, Solar Power Generation, and Energy Management: A Comprehensive Review." *World Engineering and Applied Sciences Journal* 11.02 (2023): 196-202.

[15] Pigola, Angélica, et al. "Enhancing cybersecurity capability investments: Evidence from an experiment." Technology in Society 76 (2024): 102449.

[16] Heydari, Melika, Ashkan Heydari, and Mahyar Amini. "Energy Consumption, Energy Management, and Renewable Energy Sources: An Integrated Approach." *International Journal of Engineering and Applied Sciences* 9.07 (2023): 167-173.

[17] Meraneh, Awaleh Houssein. Enhancing the security of industrial cyber-physical systems trough side-channel leakage. Diss. Ecole nationale supérieure Mines-Télécom Atlantique, 2024.

[18] Heydari, Melika, Ashkan Heydari, and Mahyar Amini. "Solar Power Generation and Sustainable Energy: A Review." *International Journal of Technology and Scientific Research* 12.03 (2023): 342-349.

[19] Sharifani, Koosha and Mahyar Amini. "Machine Learning and Deep Learning: A Review of Methods and Applications." World Information Technology and Engineering Journal 10.07 (2023): 3897-3904.

[20] Amini, Mahyar and Ali Rahmani. "How Strategic Agility Affects the Competitive Capabilities of Private Banks." *International Journal of Basic and Applied Sciences* 10.01 (2023): 8397-8406.

[21] Amini, Mahyar and Ali Rahmani. "Achieving Financial Success by Pursuing Environmental and Social Goals: A Comprehensive Literature Review and Research Agenda for Sustainable Investment." *World Information Technology and Engineering Journal* 10.04 (2023): 1286-1293.

[22] Jahanbakhsh Javid, Negar, and Mahyar Amini. "Evaluating the effect of supply chain management practice on implementation of halal agroindustry and competitive advantage for small and medium enterprises ." International Journal of Computer Science and Information Technology 15.6 (2023): 8997-9008

[23] Amini, Mahyar, and Negar Jahanbakhsh Javid. "A Multi-Perspective Framework Established on Diffusion of Innovation (DOI) Theory and Technology, Organization and Environment (TOE) Framework Toward Supply Chain Management System Based on Cloud Computing Technology for Small and Medium Enterprises ." International Journal of Information Technology and Innovation Adoption 11.8 (2023): 1217-1234

[24] Amini, Mahyar and Ali Rahmani. "Agricultural databases evaluation with machine learning procedure." Australian Journal of Engineering and Applied Science 8.6 (2023): 39-50

[25] Amini, Mahyar, and Ali Rahmani. "Machine learning process evaluating damage classification of composites." International Journal of Science and Advanced Technology 9.12 (2023): 240-250

[26] Amini, Mahyar, Koosha Sharifani, and Ali Rahmani. "Machine Learning Model Towards Evaluating Data gathering methods in Manufacturing and Mechanical Engineering." International Journal of Applied Science and Engineering Research 15.4 (2023): 349-362.

[27] Sharifani, Koosha and Amini, Mahyar and Akbari, Yaser and Aghajanzadeh Godarzi, Javad. "Operating Machine Learning across Natural Language Processing Techniques for Improvement of Fabricated News Model." International Journal of Science and Information System Research 12.9 (2022): 20-44.

[28] Amini, Mahyar, et al. "MAHAMGOSTAR.COM AS A CASE STUDY FOR ADOPTION OF LARAVEL FRAMEWORK AS THE BEST PROGRAMMING TOOLS FOR PHP BASED WEB DEVELOPMENT FOR SMALL AND MEDIUM ENTERPRISES." Journal of Innovation & Knowledge, ISSN (2021): 100-110.

[29] Amini, Mahyar, and Aryati Bakri. "Cloud computing adoption by SMEs in the Malaysia: A multi-perspective framework based on DOI theory and TOE framework." Journal of Information Technology & Information Systems Research (JITISR) 9.2 (2015): 121-135.

[30] Amini, Mahyar, and Nazli Sadat Safavi. "A Dynamic SLA Aware Heuristic Solution For IaaS Cloud Placement Problem Without Migration." International Journal of Computer Science and Information Technologies 6.11 (2014): 25-30.

[31] Amini, Mahyar. "The factors that influence on adoption of cloud computing for small and medium enterprises." (2014).

[32] Amini, Mahyar, et al. "Development of an instrument for assessing the impact of environmental context on adoption of cloud computing for small and medium enterprises." Australian Journal of Basic and Applied Sciences (AJBAS) 8.10 (2014): 129-135.

[33] Amini, Mahyar, et al. "The role of top manager behaviours on adoption of cloud computing for small and medium enterprises." Australian Journal of Basic and Applied Sciences (AJBAS) 8.1 (2014): 490-498.

[34] Amini, Mahyar, and Nazli Sadat Safavi. "A Dynamic SLA Aware Solution For IaaS Cloud Placement Problem Using Simulated Annealing." International Journal of Computer Science and Information Technologies 6.11 (2014): 52-57.

[35] Sadat Safavi, Nazli, Nor Hidayati Zakaria, and Mahyar Amini. "The risk analysis of system selection and business process re-engineering towards the success of enterprise resource planning project for small and medium enterprise." World Applied Sciences Journal (WASJ) 31.9 (2014): 1669-1676.

[36] Sadat Safavi, Nazli, Mahyar Amini, and Seyyed AmirAli Javadinia. "The determinant of adoption of enterprise resource planning for small and medium enterprises in Iran." International Journal of Advanced Research in IT and Engineering (IJARIE) 3.1 (2014): 1-8.

[37] Sadat Safavi, Nazli, et al. "An effective model for evaluating organizational risk and cost in ERP implementation by SME." IOSR Journal of Business and Management (IOSR-JBM) 10.6 (2013): 70-75.

[38] Safavi, Nazli Sadat, et al. "An effective model for evaluating organizational risk and cost in ERP implementation by SME." IOSR Journal of Business and Management (IOSR-JBM) 10.6 (2013): 61-66.

[39] Amini, Mahyar, and Nazli Sadat Safavi. "Critical success factors for ERP implementation." International Journal of Information Technology & Information Systems 5.15 (2013): 1-23.

[40] Amini, Mahyar, et al. "Agricultural development in IRAN base on cloud computing theory." International Journal of Engineering Research & Technology (IJERT) 2.6 (2013): 796-801.

[41] Amini, Mahyar, et al. "Types of cloud computing (public and private) that transform the organization more effectively." International Journal of Engineering Research & Technology (IJERT) 2.5 (2013): 1263-1269.

[42] Amini, Mahyar, and Nazli Sadat Safavi. "Cloud Computing Transform the Way of IT Delivers Services to the Organizations." International Journal of Innovation & Management Science Research 1.61 (2013): 1-5.

[43] Abdollahzadegan, A., Che Hussin, A. R., Moshfegh Gohary, M., & Amini, M. (2013). The organizational critical success factors for adopting cloud computing in SMEs. Journal of Information Systems Research and Innovation (JISRI), 4(1), 67-74.

[44] Khoshraftar, Alireza, et al. "Improving The CRM System In Healthcare Organization." International Journal of Computer Engineering & Sciences (IJCES) 1.2 (2011): 28-35.