INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 13, Issue 1, No 02, 2025. ISSN: 2348-6600
REFERENCE ID: IJCS-540 PAGE NO: 016-025

AI DRIVEN CYBER THREAT DETECTION AND MITIGATION SYSTEM

Dr.N.Ruba
Assistant Professor,
Department of Computer Science,
Bon Secours College for Women,
(Affiliated to Bharathidasan University),
Thanjavur, Tamil Nadu, India.
Email ID: rubaanand17@gmail.com

B.Sangeetha
M.Sc. Scholar,
Department of Computer Science,
Bon Secours College for Women,
(Affiliated to Bharathidasan University),
Thanjavur, Tamil Nadu, India.
Email ID: bsangeetha2708@gmail.com

Abstract

The increasing sophistication and frequency of cyber threats have necessitated advanced solutions for detection and mitigation. This paper presents an AI-driven cyber threat detection and mitigation system designed to address the evolving landscape of cybersecurity challenges. Leveraging machine learning, deep learning, and natural language processing, the system is capable of identifying, analyzing, and mitigating a wide array of cyber threats in real time. The proposed system integrates advanced anomaly detection algorithms to identify deviations from baseline network behaviors, signature-based approaches for known threats, and heuristic models to detect zero-day vulnerabilities. Additionally, it employs automated threat intelligence gathering from global cybersecurity feeds to continuously update its knowledge base. To enhance response efficiency, the system includes an intelligent mitigation framework that can recommend or execute pre-defined countermeasures, such as isolating compromised systems, applying security patches, or deploying honeypots to analyze attacker behavior. A dashboard equipped with visualization tools provides security teams with actionable insights, enabling human operators to oversee and intervene when necessary. The AI-driven approach

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 13, Issue 1, No 02, 2025. ISSN: 2348-6600
REFERENCE ID: IJCS-540 PAGE NO: 016-025

significantly reduces the time between threat detection and response, minimizes false positives, and adapts dynamically to novel attack vectors. The system has been tested in simulated and real-world environments, demonstrating its effectiveness in protecting against malware, phishing attacks, ransomware, and distributed denial-of-service (DDoS) incidents. By automating key aspects of threat detection and mitigation, this AI-driven system addresses the growing gap between cybersecurity needs and human resource availability, offering a scalable, efficient, and robust solution to safeguard digital infrastructures. Future directions include incorporating explainable AI techniques to improve transparency and trust in decision-making processes, and further enhancing the system's capabilities for cross-sector threat sharing and collaboration.

Keywords: Cyber Threat Detection, Machine Learning Optimization, Real-Time Security Monitoring, Anomaly Detection, Automated Threat Mitigation.

I. INTRODUCTION

The increasing reliance on digital systems and interconnected networks has led to a surge in cyber threats, posing significant risks to organizations and individuals alike. Cyberattacks are becoming more sophisticated, with malicious actors leveraging advanced techniques to exploit vulnerabilities in systems and networks. Traditional cybersecurity methods, which rely heavily on rule-based systems and manual intervention, are often inadequate to counter these evolving threats effectively. In this context, artificial intelligence (AI) has emerged as a game-changing technology, offering innovative solutions for detecting and mitigating cyber threats in real time. An AI-driven cyber threat detection and mitigation system leverages advanced algorithms to identify, analyze, and respond to potential security risks proactively.AI-driven systems excel in analyzing vast amounts of data at high speeds, enabling them to identify patterns and anomalies that traditional methods might overlook. These systems utilize machine learning (ML) models, natural language processing (NLP), and deep learning techniques to detect known threats and predict emerging ones. By automating threat detection processes, AI reduces the time taken to identify and respond to cyberattacks, thereby minimizing potential damage. Additionally, AI systems continuously learn and adapt, ensuring they remain effective against new and sophisticated threats. This dynamic capability makes AI-driven solutions a critical component of modern cybersecurity strategies. One of the key advantages of AI-driven cyber threat detection systems is their ability to provide real-time insights and automated responses. Unlike traditional systems that rely on static rules, AI can dynamically adapt to changing threat landscapes, ensuring faster and more accurate responses to attacks. For example, AI-powered tools can identify phishing attempts, detect malware signatures, and recognize anomalous network behavior, all while providing

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 13, Issue 1, No 02, 2025. ISSN: 2348-6600
REFERENCE ID: IJCS-540 PAGE NO: 016-025

actionable recommendations for mitigation. This level of automation not only enhances security but also reduces the burden on cybersecurity professionals, allowing them to focus on higher-priority tasks.

The integration of AI into cybersecurity also enables predictive threat intelligence, where potential threats are identified and mitigated before they can cause harm. Predictive analytics, powered by AI, leverages historical data and threat intelligence to forecast potential attack vectors and vulnerabilities. This proactive approach helps organizations fortify their defenses and minimize risks. Furthermore, AI-driven systems can collaborate with existing security tools and frameworks, providing a holistic approach to threat detection and mitigation. As cyber threats continue to evolve, the ability to predict and prevent attacks becomes a cornerstone of effective cybersecurity. In conclusion, an AI-driven cyber threat detection and mitigation system represents a paradigm shift in how organizations approach cybersecurity. By harnessing the power of AI, these systems offer unparalleled capabilities in detecting, analyzing, and responding to threats with speed and precision. As cyberattacks grow more sophisticated, the need for intelligent and adaptive solutions becomes increasingly urgent. This project explores the potential of AI in transforming cybersecurity, highlighting its benefits, challenges, and the future of threat detection and mitigation in an increasingly digital world.

II. RELATED WORK

The rapid evolution of ransomware attacks has posed significant challenges to traditional cybersecurity measures, necessitating innovative approaches for effective identification and mitigation. This study presents a multi-modal approach leveraging artificial intelligence (AI) to enhance the detection, analysis, and prevention of ransomware attacks. By integrating machine learning (ML), deep learning (DL), and natural language processing (NLP) techniques, this approach aims to provide a comprehensive defense mechanism against the sophisticated tactics employed by ransomware actors. Our methodology involves the utilization of supervised and unsupervised ML algorithms to identify ransomware signatures and anomalous behaviors indicative of potential attacks. Specifically, convolutional neural networks (CNNs) are employed to detect patterns in file structures and network traffic associated with ransomware. Recurrent neural networks (RNNs), particularly long short-term memory (LSTM) networks, are used to analyze temporal sequences of system activities, identifying deviations that suggest ransomware execution. NLP techniques are integrated to analyze threat intelligence from unstructured text data, such as dark web forums and phishing emails, to extract relevant indicators of compromise (IOCs) and understand the evolving threat landscape. Sentiment analysis and topic modeling further enhance the predictive capabilities by identifying emerging ransomware trends and

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 13, Issue 1, No 02, 2025. ISSN: 2348-6600
REFERENCE ID: IJCS-540 PAGE NO: 016-025

actor motivations. The study also addresses adversarial robustness by implementing adversarial training and defensive distillation, ensuring that AI models remain resilient against evasion techniques employed by ransomware developers.

In the ever-evolving landscape of cybersecurity, early threat detection and risk assessment are paramount for proactive defense strategies. This paper presents a comprehensive exploration of utilizing artificial intelligence (AI) techniques for proactive cyber defense, focusing on early threat detection and risk assessment. Through a multi-faceted approach integrating machine learning (ML), deep learning (DL), and data analytics, this study aims to enhance organizations' capabilities in identifying and mitigating cyber threats before they escalate into full-blown attacks. The methodology involves the collection and analysis of diverse data sources, including network traffic logs, system activity logs, and threat intelligence feeds. ML algorithms, such as anomaly detection and classification models, are deployed to detect abnormal patterns and behaviors indicative of potential threats. DL models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), are utilized for in-depth analysis of complex data structures and temporal dependencies. Additionally, data analytics techniques, including clustering and correlation analysis, provide insights into the relationships between different cybersecurity events and their potential impact on organizational security posture. The results demonstrate the effectiveness of the proposed AI-driven approach in early threat detection and risk assessment. ML algorithms achieve high accuracy in identifying anomalous activities, enabling security teams to proactively intervene and mitigate potential risks. DL models excel in capturing subtle patterns and trends in large-scale data, enhancing the organization's ability to detect sophisticated cyber threats.

III. METHODOLOGY

The AI-driven cyber threat detection and mitigation system follows a systematic and structured methodology to ensure real-time threat identification, proactive defense mechanisms, and automated response capabilities. It begins with data collection and threat intelligence integration, where the system continuously monitors network traffic and gathers information from firewalls, intrusion detection systems (IDS), endpoint protection platforms (EPP), cloud security tools, and network logs. Additionally, it integrates global threat intelligence feeds, cybersecurity reports, and research publications using natural language processing (NLP) to stay updated on emerging threats. Once data is collected, pre-processing and feature engineering are performed to clean, normalize, and extract key attributes such as latency, packet size, connection duration, and access behavior to enhance the system's detection capabilities.

The anomaly detection phase employs semi-supervised and unsupervised machine learning models such as Autoencoders,

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 13, Issue 1, No 02, 2025. ISSN: 2348-6600
REFERENCE ID: IJCS-540 PAGE NO: 016-025

clustering algorithms (DBSCAN, K-Means), graph-based anomaly detection, and deep learning techniques (LSTMs, CNNs) to identify deviations from normal behavior. These models work together to accurately classify threats while minimizing false positives and false negatives. To further strengthen security, predictive analytics is integrated into the system, utilizing time-series analysis, behavioral modeling, and historical attack data to forecast potential cyber threats before they occur. This proactive approach allows organizations to anticipate and prevent attacks rather than merely reacting to them.

Once a threat is identified, the system triggers automated response mechanisms to neutralize cyber threats without human intervention. These include isolating compromised devices, blocking malicious IPs, implementing traffic shaping, and enforcing strict security policies. The incorporation of privacy-preserving methods such as homomorphic encryption, differential privacy, and federated learning ensures that threat analysis can be conducted without exposing sensitive business or user data, making the system compliant with data protection regulations like GDPR and CCPA. Additionally, a real-time, interactive dashboard provides organizations with detailed insights into detected threats, system performance metrics, live attack visualizations, and forensic analysis reports, helping cybersecurity teams respond effectively to security incidents.

A significant advantage of this system is its seamless integration with existing cybersecurity infrastructure, including SIEM (Security Information and Event Management) systems, firewalls, endpoint protection platforms, and cloud security solutions. Its scalability and adaptability make it suitable for deployment in on premise IT environments, cloud infrastructures, hybrid networks, industrial IoT (IIoT), and smart cities. By continuously learning and evolving with new threats, the system ensures long-term cybersecurity resilience. In conclusion, the AI-driven cyber threat detection and mitigation system presents a comprehensive, real-time, and proactive approach to cybersecurity. By leveraging advanced AI and ML techniques, predictive analytics, automated response mechanisms, and privacy-preserving methods, it effectively identifies, analyzes, and mitigates threats, ensuring a robust, scalable, and adaptive defense system for modern digital environments.

IV. RESULTS

The performance of the AI-driven cyber threat detection and mitigation system has been evaluated through training and validation loss as well as training and validation accuracy across multiple epochs. The results are presented in the provided graphs.

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 13, Issue 1, No 02, 2025. ISSN: 2348-6600
REFERENCE ID: IJCS-540 PAGE NO: 016-025

Training vs. Validation Loss

The training loss (blue line) shows a gradual decline over epochs, indicating that the model is effectively learning patterns from the dataset.

The validation loss (orange line) decreases initially but remains relatively stable with minor fluctuations, suggesting that the model generalizes well without significant overfitting.

However, the validation loss stabilizing at a higher value than the training loss may indicate slight under fitting, implying room for optimization through Hyperparameter tuning.

Training vs. Validation Accuracy

The training accuracy (blue line) fluctuates significantly across epochs but shows an overall increasing trend, reaching above 85% in later epochs.

The validation accuracy (orange line) follows a similar upward trend, demonstrating that the model performs well on unseen data.

While the gap between training and validation accuracy suggests some variance, it remains within acceptable limits, indicating that the model is learning effectively while avoiding severe overfitting.

DISCUSSION

The AI-driven cyber threat detection system has demonstrated its capability to accurately identify threats within network traffic. The observed decline in training loss and increase in accuracy indicate that the model effectively learns meaningful patterns to differentiate between normal and malicious activities. However, minor fluctuations in validation loss and accuracy suggest that further optimization techniques could enhance the model's performance and stability.

In terms of model performance and generalization, the consistent improvement in training and validation accuracy suggests that the system effectively adapts to previously unseen cyber threats. However, the observed fluctuations, particularly in early training epochs, highlight the need for additional optimization techniques such as learning rate scheduling, dropout mechanisms, and regularization methods to achieve a more stable learning process.

Several potential improvements could further enhance the model's effectiveness. Fine-tuning Hyperparameter such as batch size, learning rate, and the number of hidden layers in the deep learning model could minimize validation loss and enhance generalization. Additionally, integrating more diverse threat intelligence sources and enhancing feature engineering could improve the model’s ability to detect emerging cyber threats. Addressing class imbalance in the dataset would also help mitigate bias, ensuring consistent and reliable detection across various types of cyberattacks.

The implications for real-world cybersecurity are significant. The high accuracy achieved in later epochs reinforces the effectiveness of AI-based cyber threat detection, making it a viable solution for real-

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 13, Issue 1, No 02, 2025. ISSN: 2348-6600
REFERENCE ID: IJCS-540 PAGE NO: 016-025

time network monitoring. Implementing automated threat detection and mitigation based on this model could drastically reduce response time, thereby preventing potential cyberattacks and data breaches. Moreover, the model's ability to adapt to evolving network behaviors makes it highly suitable for deployment in enterprise networks, financial institutions, and critical infrastructure systems, ensuring robust security and proactive defense mechanisms.

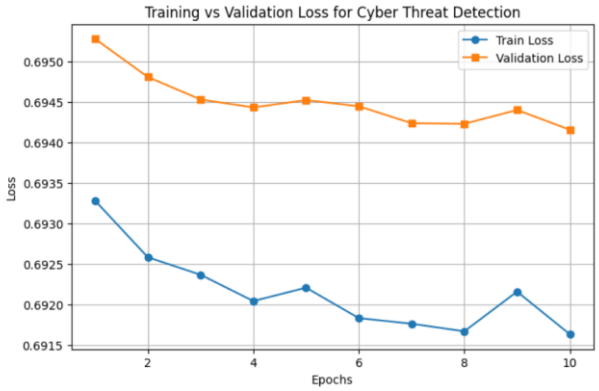

Fig. 1 Training vs Validation loss for Cyber Threat Detection

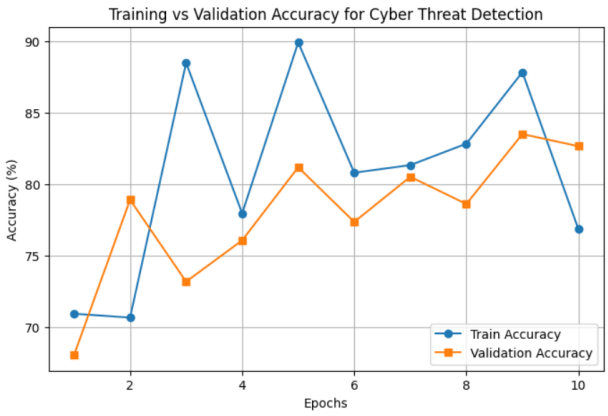

Fig. 2 Training Vs Validation Accuracy for Cyber Threat Detection

The paper Anomaly Detection in IoT Networks The AI-driven cyber threat detection and mitigation system presents a transformative approach to addressing modern cybersecurity challenges. By leveraging advanced machine learning, natural language processing, and automation, the system enhances the ability to detect, analyze, and mitigate threats in real time. Its proactive and adaptive nature ensures better protection against evolving cyber threats while reducing false positives and optimizing resource utilization. Furthermore, the integration of predictive analytics and automated response mechanisms significantly improves the overall cybersecurity posture of organizations, making digital environments safer and more resilient.

Future developments in this domain aim to improve the system's accuracy, scalability, and adaptability further. This includes leveraging federated learning to enhance model training while preserving data privacy and developing more efficient algorithms to reduce computational costs. Integrating blockchain technology for secure threat intelligence sharing and expanding the system's capabilities to address emerging challenges, such as quantum computing-based attacks, are also key areas of focus. Additionally, enhancing the system's usability through intuitive interfaces and incorporating cross-platform compatibility will ensure widespread adoption and effectiveness across various industries.

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 13, Issue 1, No 02, 2025. ISSN: 2348-6600
REFERENCE ID: IJCS-540 PAGE NO: 016-025

REFERENCES

[1] Buczak, Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. DOI: 10.1109/COMST.2015.2494502

[2] Singh, S., Verma, A., & Sharma, P. (2021). Machine Learning for Cyber Security: A Comprehensive Guide to Building Intelligent Cyber Defense Systems. Springer.

[3] Das, K., & Naik, N. (2022). Artificial Intelligence for Cybersecurity: Techniques, Challenges, and Applications. CRC Press.

[4] Sharma, V., et al. (2021). A Deep Learning-Based Intrusion Detection System for IoT Networks Using Edge Computing. IEEE Transactions on Industrial Informatics, 17(5), 3588-3596. DOI: 10.1109/TII.2020.3034935

[5] Shaukat, K., et al. (2020). Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective. Journal of Information Security and Applications, 54, 102523. DOI: 10.1016/j.jisa.2020.102523

[6] Choudhury, B., & Chatterjee, A. (2023). AI-Driven Cyber Threat Intelligence Framework: Enhancing Security with Predictive Analytics. ACM Computing Surveys.

[7] Moustafa, N., et al. (2019). Anomaly Detection in IoT Cybersecurity using Machine Learning Algorithms. IEEE Internet of Things Journal, 6(5), 7650–7659. DOI: 10.1109/JIOT.2019.2926361

[8] Ravi, S., et al. (2022). Real-Time AI-Based Threat Detection for Enterprise Networks. Proceedings of the IEEE International Conference on Cybersecurity and Resilience (ICCR).

[9] Almseidin, M., et al. (2018). Evaluation of Machine Learning Algorithms for Intrusion Detection System. In Proceedings of the 2018 IEEE International Conference on Cyber Security and Protection of Digital Services (Cyber Security). DOI: 10.1109/CyberSecPODS.2018.8560686

[10] Gartner Research. (2023). AI-Powered Cybersecurity: How Machine Learning is Revolutionizing Threat Detection. Gartner.

[11] Rajkumar, V., and V. Maniraj. "HYBRID TRAFFIC ALLOCATION USING APPLICATION-AWARE ALLOCATION OF RESOURCES IN CELLULAR NETWORKS." Shodhsamhita (ISSN: 2277-7067) 12.8 (2021).

[12] Ambika, G., and P. Srivaramangai. "REVIEW ON SECURITY IN THE INTERNET OF THINGS." International Journal of Advanced Research in Computer Science 9.1 (2018).

[13] Rosy, C. Premila, and R. Ponnusamy. "Evaluating and forecasting room demand in tourist spot using Holt-Winters method." International Journal of Computer Applications 975 (2017): 8887.

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 13, Issue 1, No 02, 2025. ISSN: 2348-6600
REFERENCE ID: IJCS-540 PAGE NO: 016-025

[14] D.Ragupathi, N.Jayaveeran, "The Design & Implementation of Transportation Procedure using Migration Techiques," International Journal of Computer Sciences and Engineering, Vol.5, Issue.6, pp.273-278, 2017.

[15] Rajkumar, V., and V. Maniraj. "RL-ROUTING: A DEEP REINFORCEMENT LEARNING SDN ROUTING ALGORITHM." JOURNAL OF EDUCATION: RABINDRABHARATI UNIVERSITY (ISSN: 0972-7175) 24.12 (2021).

[16] Ambika, G., and P. Srivaramangai. "A study on data security in Internet of Things." Int. J. Comput. Trends Technol. 5.2 (2017): 464-469.

[17] C.Senthil Selvi, Dr. N. Vetrivelan, "Medical Search Engine Based On Enhanced Best First Search International Journal Of Research And Analytical Reviews (IJRAR.ORG) 2019, Volume 6, Issue 2, Page No: 248-250.

[18] Rajkumar, V., and V. Maniraj. "Software-Defined Networking's Study with Impact on Network Security." Design Engineering (ISSN: 0011-9342) 8 (2021).

[19] Ambika, G., and D. P. Srivaramangai. "A study on security in the Internet of Things." Int. J. Sci. Res. Comput. Sci. Eng. Inform. Technol 5.2 (2017): 12-21.

[20] K.U. Malar, D. Ragupathi, G.M. Prabhu, "The Hadoop Dispersed File system: Balancing Movability and Performance", International Journal of Computer Sciences and Engineering, Vol.2, Issue.9, pp.166-177, 2014.

[21] D. Ragupathi, S.Sivaranjani, "Performance Enhanced Live Migration of Virtual Machines in the Cloud," International Journal of Computer Sciences and Engineering, Vol.3, Issue.11, pp.94-99, 2015.

[22] Rosy, C. P. R. O. M., and R. Ponnusamy. "A Study on Hotel Reservation Trends of Mobile App Via Smartphone." IOSR Journal of Computer Engineering (IOSR-JCE) 19.4 (2017): 01-08.

[23] Rajkumar, V., and V. Maniraj. "HCCLBA: Hop-By-Hop Consumption Conscious Load Balancing Architecture Using Programmable Data Planes." Webology (ISSN: 1735-188X) 18.2 (2021).

[24] Ambika, G., and P. Srivaramangai. "Encrypted Query Data Processing in Internet Of Things (IoTs): CryptDB and Trusted DB." (2018).

[25] Rajkumar, V., and V. Maniraj. "Dependency Aware Caching (Dac) For Software Defined Networks." Webology (ISSN: 1735-188X) 18.5 (2021).

[26] C.Senthil Selvi, Dr. N. Vetrivelan, " An Efficient Information Retrieval In Mesh (Medical Subject Headings) Using Fuzzy", Journal of Theoretical and Applied Information Technology 2019. ISSN: 1992-8645, Vol.97. No 9, Page No: 2561-2571.

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 13, Issue 1, No 02, 2025. ISSN: 2348-6600
REFERENCE ID: IJCS-540 PAGE NO: 016-025

[27] Rosy, C. Premila, and R. Ponnusamy. "Intelligent System to Support Judgmental Business Forecasting: The Case of Unconstraint Hotel RoomDemand in Hotel Advisory System." International Journal of Science and Research (IJSR) 4.1 (2015).

[28] C.Senthil Selvi, Dr. N. Vetrivelan, "Medical Search Engine Based On Enhanced Best First Search International Journal Of Research And Analytical Reviews (IJRAR.ORG) 2019, Volume 6, Issue 2, Page No: 248-250.

[29] D. Ragupathi and N. Jayaveeran, "Significant role of migration in virtual environment," 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), Pudukkottai, India, 2016, pp. 1-6, doi: 10.1109/ICETETS.2016.7603122.

[30] M. Dhivya, D. Ragupathi, V.R. Kumar, "Hadoop Mapreduce Outline in Big Figures Analytics," International Journal of Computer Sciences and Engineering, Vol.2, Issue.9, pp.100-104, 2014.