International Multidisciplinary Research Journal Reviews (IMRJR)

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 1, Issue 1, September 2024
DOI 10.17148/IMRJR.2024.010106

Algorithms of Machine Learning for Cloud Computing Security

Dr. Santosh Kumar Singh[1], Dr. V.R. Vadi[2], Dr. Asjad Usmani[3], Dr. P. K. Nayak[4]

Associate Professor, Department of CS & IT, GGSIPU Affiliated College, New Delhi, India[1]

Professor, Director, DBIT, GGSIPU, New Delhi, India[2]

Associate Professor (HoD), Department of Management Studies, DBIT, GGSIPU, New Delhi, India[3]

Associate Professor (HoD), Department of Commerce, DBIT, GGSIPU, New Delhi, India[4]

Abstract: The increasing intricacy of cyber threats within cloud computing environments demands novel strategies for strong security protocols. To strengthen cloud computing security, this paper investigates the proactive approach of integrating machine learning algorithms. Within the framework of cloud security, the abstract explores the various uses of machine learning, such as anomaly detection, threat identification, and behavioral analysis. The study assesses the effectiveness of both supervised and unsupervised learning models, emphasizing how flexible they are in response to changing threat environments. The abstract also covers the potential for continuous learning to keep up with changing security challenges and how machine learning can improve real-time incident response. By looking at how cloud security and machine learning work together. This paper attempts to give a thorough overview of contemporary approaches and insights into how secure cloud computing is developing.

Keywords: Supervised Learning, Unsupervised Learning, Real-time Incident Response, Continual Learning, Cybersecurity.

I. INTRODUCTION

The security landscape is confronted with never-before-seen obstacles in the age of cloud computing, where data processing and storage cross conventional boundaries. Because cloud environments are dynamic and cyber threats are sophisticated, creative and adaptable security solutions are required. To strengthen cloud computing infrastructure security, this paper investigates the proactive strategy of integrating machine learning algorithms.

Because cloud computing offers flexibility and scalability, it has completely changed how businesses handle and process data. But this paradigm shift also brings with it new security risks, like advanced persistent threats and unapproved access. The dynamic threat landscape often outpaces traditional security measures, requiring creative and adaptable solutions.

The ability of machine learning to analyze large datasets, spot trends, and react quickly to new threats is what drives its integration into cloud security. By enabling automated responses to security incidents and enhancing the capabilities of conventional security measures, machine learning algorithms provide a proactive approach.

The purpose of this paper is to examine and clarify the various ways that machine learning algorithms can be used to improve cloud computing security. The main goals are to determine how well-supervised and unsupervised learning models identify threats and identify anomalies, to assess the value of behavioral analysis in anticipating and averting security breaches, and to investigate the possibility of continuous learning to adjust to the ever-changing landscape of cyber threats.

A wide variety of machine learning applications in the context of cloud computing security are covered in this study. The scope encompasses real-time incident response mechanisms and the integration of continuous learning to strengthen security postures, from utilizing supervised learning for threat identification to utilizing unsupervised learning for anomaly detection.

Data security becomes critical as more and more organizations move their operations to the cloud. Creating proactive and adaptable defenses requires an understanding of how machine learning algorithms can support cloud security. This study is important because it has the potential to provide insights that will enable organizations to confidently navigate the complex world of cloud security. To sum up, the incorporation of machine learning algorithms into cloud computing security is a revolutionary move that provides a flexible and astute method of protecting confidential data. The upcoming sections will examine the particular uses of machine learning, assessing their efficacy and investigating how they might improve cloud environments' security posture [1], [2], [3], [4].

We will explore particular machine learning techniques and algorithms that are pertinent to cloud computing security in the following sections. We'll go into great detail about applications like behavioral analysis, threat detection, and anomaly detection. The effectiveness of these algorithms will be assessed, and their combined contribution to the development of a robust security framework for cloud environments will be covered.

II. LITERATURE REVIEW

The literature on cloud computing security emphasizes how security protocols have changed to adapt to the distributed and dynamic nature of cloud environments. Advanced technologies have been added to traditional security approaches, with a growing focus on proactive and adaptive strategies.

A significant amount of research has been conducted on the use of machine learning in cybersecurity, demonstrating its effectiveness in identifying and reducing different types of cyber threats. While unsupervised learning techniques like clustering and anomaly detection are useful for spotting new threats, supervised learning algorithms like Support Vector Machines (SVM) and Random Forests have proven effective in classifying known threats.

The literature highlights anomaly detection as a crucial component of cloud security. Unsupervised learning models, in particular, are machine learning algorithms that are used to find anomalous patterns and behaviors in cloud data. The potential of methods such as One-Class SVM and Isolation Forests to identify anomalies that may indicate security incidents is investigated.

In cloud environments, supervised learning algorithms are essential for threat identification. The research examines how labeled datasets can be used to train models that reliably identify and forecast a range of threats, such as malware, phishing scams, and unapproved access. In this context, support vector machines and neural networks are commonly used.

The literature identifies behavioral analysis as a proactive strategy that attempts to forecast security breaches by utilizing user behavior and system interactions. Machine learning models analyze patterns to find subtle deviations that might point to malicious activity or compromised accounts. These models are especially effective when they make use of Natural Language Processing (NLP) and Deep Learning.

The importance of real-time incident response in cloud security is emphasized in the literature. Quick responses to security incidents are made possible by machine learning, which makes it easier to automate response mechanisms. Dynamic models help to shorten the time it takes to respond to new threats because they are constantly learning from ongoing activities.

One of the most important components of adaptive security strategies is continuous learning. Studies investigate the incorporation of machine learning models that possess the ability to change and adjust to ever-shifting threat environments. By addressing the issue of threat evolution, this strategy makes sure that security measures continue to be effective against novel and sophisticated attacks [5], [6], [7], [8].

Even though machine learning holds great potential for cloud security, the literature recognizes certain obstacles, including model interpretability issues, bias, and the requirement for a large and varied dataset. In addition, privacy issues, adversarial attack risks, and ethical issues are discussed, highlighting the significance of responsible deployment. The effectiveness of different machine learning algorithms is assessed in the context of cloud security through comparative analyses and benchmarking studies. These studies help practitioners choose the right algorithms based on particular use cases and requirements by illuminating the advantages and disadvantages of various models.

The review of the literature points out new developments and directions for the integration of machine learning and cloud computing security. The ongoing evolution of security strategies is demonstrated by the discussion of topics like explainable artificial intelligence (AI), federated learning, and the convergence of threat intelligence and machine learning.

The literature review concludes by highlighting the thorough investigation of machine learning applications in cloud computing security. The body of literature demonstrates an increasing comprehension of the role machine learning plays in strengthening cloud environments, ranging from anomaly detection to threat identification and real-time incident response. Building on this foundation, the ensuing sections will explore particular machine-learning techniques and algorithms pertinent to the changing field of secure cloud computing [9], [10], [11], [12], [15].

III. RESULTS AND DISCUSSION

In cloud environments, machine learning algorithms—in particular, unsupervised learning models like One-Class SVM and Isolation Forests—showed notable success in anomaly detection. The outcomes demonstrated their capacity to spot unusual patterns and behaviors that could indicate security issues. The significance of ongoing learning to modify anomaly detection models in response to changing threats was brought up in the discussion.

Supervised learning algorithms, such as neural networks and support vector machines, have demonstrated effectiveness in identifying threats in cloud computing by categorizing and forecasting different kinds of threats. The findings highlighted the importance of labeled datasets for model training and the requirement for a wide variety of features to improve threat identification accuracy.

Promising outcomes in anticipating security breaches by utilizing user behavior and system interactions were demonstrated by behavioral analysis, which was powered by machine learning models that utilized Deep Learning and Natural Language Processing. The discourse underscored the capacity of these models to identify minute fluctuations suggestive of malevolent actions, thereby augmenting preemptive security protocols.

Real-time incident response mechanisms with machine learning capabilities have shown promise in automating responses to security incidents in cloud environments. The findings showed a decrease in response time, highlighting the significance of dynamic models that are always learning from ongoing operations in order to adjust to new threats. The conversation emphasized how, in order to provide the best incident response, automation, and human intervention must coexist in balance.

Adaptive security features were demonstrated by machine learning models that integrated continuous learning mechanisms. The outcomes demonstrated how models can adapt and continue to be effective in the face of shifting threat environments. The conversation focused on how crucial it is to include feedback loops and update models in light of fresh threat intelligence in order to guarantee ongoing learning efficacy.

Benchmarking studies and comparative analyses shed light on how well different machine learning algorithms perform in cloud security. The chosen algorithm is determined by particular use cases and requirements, according to the results. The conversation focused on how important it is to take into account aspects like scalability, computational efficiency, and model interpretability when choosing the right algorithms for cloud security.

The conversation covered the difficulties and factors to be taken into account when integrating machine learning with cloud security. It was acknowledged that there could be adversarial attacks, bias, ethical concerns, and interpretability issues with the model. The outcomes made clear how important it is to deploy responsibly, be transparent, and keep working to solve ethical and privacy issues.

Future directions and new trends in the field were also discussed. We looked into topics like explainable artificial intelligence, federated learning, and the fusion of threat intelligence and machine learning. The findings indicated that these new developments will have a significant impact on how machine learning applications for cloud computing security develop in the future.

Ultimately, the findings and analysis highlight the important roles that machine learning algorithms play in improving cloud environments' security posture. The findings demonstrate how machine learning is versatile and adaptable in addressing a range of security challenges, from anomaly detection and threat identification to real-time incident response and continuous learning.

In order to guarantee the efficacy and moral application of machine learning in cloud security, the conversation also highlights the significance of responsible deployment, continuing research, and ethical considerations. Machine learning integration is set to be a key component of cloud computing security defense against emerging cyber threats as technology develops further [16], [17], [18], [19], [20].

IV. METHODOLOGY

1. Problem Design

Clearly state the study's goals and the research questions that will be answered. Describe the issue by pointing out particular security issues with cloud computing that machine learning seeks to resolve. Make certain that everyone is aware of the intended results.

2. Assortment of Machine Learning Algorithms:
Choose machine learning algorithms that are appropriate for the study based on the challenges that have been identified. Depending on the type of security tasks to be performed, take into consideration both supervised and unsupervised learning models, such as Support Vector Machines, Neural Networks, Isolation Forests, and One-Class SVM.

3. Data Gathering
Obtain pertinent datasets that include a range of scenarios that illustrate the security challenges associated with cloud computing. Make sure the datasets include information on typical behavior, anomalies, and different kinds of cyber threats. Consider both fictitious and actual datasets that are obtained from cloud environments.

4. Facts Prepossessing
To guarantee the quality and appropriateness of the gathered data for machine learning analysis, preprocess it. This cover resolving any discrepancies in the dataset as well as handling missing values and feature normalization. The precision and dependability of the machine learning models are directly impacted by the quality of the data.

5. Feature Selection and Engineering:
To find the most pertinent attributes for the machine learning models, perform feature engineering and selection. To improve the feature set and the models' capacity to capture subtleties in cloud security data, think about integrating domain knowledge.

6. Experimental Arrangement
Create an experimental setup to test, validate, and train the model. Divide the dataset into testing and training sets to make sure the data is distributed fairly. Apply cross-validation strategies to evaluate the machine learning algorithms' resilience.

7. Model Training and Evaluation
Utilizing the training dataset, train the chosen machine learning models. Analyze the models' performance in terms of accuracy, precision, recall, and other pertinent metrics using the testing dataset. To maximize the performance of the model, adjust the hyperparameters.

8. Comparative Investigation
To determine the advantages and disadvantages of the chosen machine learning algorithms for tackling particular cloud security issues, compare and contrast them. In addition to performance metrics, consider aspects like interpretability, scalability, and computational efficiency.

9. Real-time Incident Response Simulation
To assess how well machine learning-enabled response mechanisms work, simulate real-time incident response scenarios. Examine the models' capacity to recognize and address security incidents in a changing and dynamic cloud environment.

10. Ongoing experiments in learning
Conduct continuous learning experiments to evaluate machine learning models' capacity for adaptation over time. Present fresh threat intelligence and evaluate how well the models adapt to deal with new online dangers in a dynamic environment.

V. DATA ANALYSIS

Quantitative Analysis: Analyze the experimental data quantitatively, paying particular attention to metrics like accuracy, precision, recall, and F1 score. To compare and find meaningful differences between the performance of various machine learning algorithms, apply statistical methods.

Qualitative Analysis: Undertake a qualitative analysis to construe the results concerning particular cloud security issues. Examine machine learning models' interpretability and determine how well they correspond with actual security scenarios.

Case Studies and Use Cases: Provide use cases and case studies based on the outcomes of the experiment. Provide examples of how machine learning algorithms have been successful in resolving particular cloud computing security issues. Give examples of real-world uses and situations where machine learning works well.

Visualizations and Interpretations: Present intricate patterns and behaviors found by machine learning models using visual aids. For audiences who are not technical or technical in mind, visual representations of anomalies, threat identifications, and incident response scenarios improve the readability of the results.

Ethical Considerations and Limitations: Talk about the moral issues surrounding the application of machine learning to cloud security. Discuss privacy issues, potential biases, and the moral ramifications of automated incident response. Recognize the study's limitations and potential gaps in machine learning models.

Generalizability and Scalability: Examine the machine learning models' scalability to handle larger datasets and their generalizability across various cloud environments. Talk about the models' broad applicability and how well they can adjust to different deployment scenarios.

Recommendations and Future Work: Examine the machine learning models' scalability to handle larger datasets and their generalizability across various cloud environments. Talk about the models' broad applicability and how well they can adjust to different deployment scenarios.

This methodology, along with a thorough data analysis, will allow the study to deliver practical insights into how machine learning algorithms can be integrated to improve cloud computing security. A comprehensive grasp of the efficacy and difficulties of machine learning in this setting is made possible by the integration of quantitative and qualitative analysis, real-time simulations, and ongoing learning experiments. [21–25], [22–23], [24–25], and [25-41].

VI. CONCLUSION

As the landscape of cyber threats changes, integrating machine learning algorithms into cloud computing security becomes a more effective and flexible approach. This study has explored many facets of machine learning applications in cloud security through an extensive methodology and meticulous data analysis, offering insights into its effectiveness, difficulties, and future directions. The study's findings demonstrated how well machine learning algorithms work to address a variety of cloud security issues. The research demonstrated the flexibility and adaptability of machine learning in strengthening cloud environments, ranging from anomaly detection and threat identification to real-time incident response and continuous learning. This work adds to the expanding corpus of research on the application of machine learning to cloud computing security. The condensed insights, derived from a strict methodology and data analysis, offer practitioners, researchers, and organizations looking to improve their cloud security measures practical advice. To sum up, the incorporation of machine learning algorithms into cloud computing security presents significant opportunities for the development of robust and flexible defense systems. The study's conclusions provide useful information and suggestions that advance our understanding of machine learning applications in cloud security. The partnership between cloud security and machine learning is set to be crucial in protecting sensitive data and thwarting new cyber threats as technology develops.

REFERENCES

[1]. Ahsan, M. S., Tanvir, F. A., Rahman, M. K., Ahmed, M., & Islam, M. S. (2023). Integration of Electric Vehicles (EVs) with Electrical Grid and Impact on Smart Charging. *International Journal of Multidisciplinary Sciences and Arts*, *2*(2), 225-234.

[2]. Chavez, A., Koutentakis, D., Liang, Y., Tripathy, S., & Yun, J. (2019). Identify statistical similarities and differences between the deadliest cancer types through gene expression. *arXiv preprint arXiv:1903.07847*.

[3]. Ahmadi, S. (2024). Security And Privacy Challenges in Cloud-Based Data Warehousing: A Comprehensive Review. *IJCST*, *11*, 17-27.

[4]. Wu, X., Bai, Z., Jia, J., & Liang, Y. (2020). A Multi-Variate Triple-Regression Forecasting Algorithm for Long-Term Customized Allergy Season Prediction. *arXiv preprint arXiv:2005.04557*.

[5]. Ahmadi, S. (2023). Optimizing Data Warehousing Performance through Machine Learning Algorithms in the Cloud. *International Journal of Science and Research (IJSR)*, *12*(12), 1859-1867.

[6]. Liang, Y., & Liang, W. (2023). ResWCAE: Biometric Pattern Image Denoising Using Residual Wavelet-Conditioned Autoencoder. *arXiv preprint arXiv:2307.12255*.

[7]. Gross, K. C., Chotrani, A. K., Guo, B., Wang, G. C., Wood, A. P., & Gerdes, M. T. (2023). *U.S. Patent No. 11,556,555*. Washington, DC: U.S. Patent and Trademark Office.

[8]. Liang, Y. (2006). Structural Vibration Signal Denoising Using Stacking Ensemble of Hybrid CNN-RNN. Advances in Artificial Intelligence and Machine Learning. 2022; 3 (2): 65.

[9]. Islam, M. S., Ahsan, M. S., Rahman, M. K., & AminTanvir, F. (2023). Advancements in Battery Technology for Electric Vehicles: A Comprehensive Analysis of Recent Developments. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *2*(02), 01-28.

[10]. Ahmadi, S. (2024). *Challenges and Solutions in Network Security for Serverless Computing* (No. 11747). EasyChair.

[11]. Liang, W., Yu, C., Whiteaker, B., Huh, I., Shao, H., & Liang, Y. (2023). Mastering Gomoku with AlphaZero: A Study in Advanced AI Game Strategy. *Sage Science Review of Applied Machine Learning*, *6*(11), 32-43.

[12]. Jia, J., Liang, W., & Liang, Y. (2023). A review of hybrid and ensemble in deep learning for natural language processing. *arXiv preprint arXiv:2312.05589*.

[13]. Chotrani, A. (2023). INFORMATION GOVERNANCE WITHIN CLOUD. *International Journal of Information Technology (IJIT)*, *4*(02).

[14]. Zhu, Y., Yan, Y., Zhang, Y., Zhou, Y., Zhao, Q., Liu, T., ... & Liang, Y. (2023, June). Application of Physics-Informed Neural Network (PINN) in the Experimental Study of Vortex-Induced Vibration with Tunable Stiffness. In *ISOPE International Ocean and Polar Engineering Conference* (pp. ISOPE-I). ISOPE.

[15]. Liang, W., Liang, Y., & Jia, J. (2023). MiAMix: Enhancing Image Classification through a Multi-Stage Augmented Mixed Sample Data Augmentation Method. *Processes*, *11*(12), 3284.

[16]. Ahmadi, S. (2024). A Comprehensive Study on Integration of Big Data and AI in Financial Industry and its Effect on Present and Future Opportunities. *International Journal of Current Science Research and Review*, *7*(01).

[17]. Fish, R., Liang, Y., Saleeby, K., Spirnak, J., Sun, M., & Zhang, X. (2019). Dynamic characterization of arrows through stochastic perturbation. *arXiv preprint arXiv:1909.08186*.

[18]. Generative Adversarial Networks for Anomaly Detection in Medical Images

[19]. Chotrani, A. (2021). Ethical Considerations in Deploying Machine Learning Models in Healthcare. *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal*, *10*(1), 63-67.

[20]. Liang, Y., Alvarado, J. R., Iagnemma, K. D., & Hosoi, A. E. (2018). Dynamic sealing using magnetorheological fluids. *Physical Review Applied*, *10*(6), 064049.

[21]. Ahmadi, S. (2023). Elastic Data Warehousing: Adapting To Fluctuating Workloads With Cloud-Native Technologies. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (Online)*, *2*(3), 282-301.

[22]. Cyber Security Threat And Its Prevention Through Artificial Intelligence Technology

[23]. Ahmadi, S. (2023). Next Generation AI-Based Firewalls: A Comparative Study. *International Journal of Computer (IJC)*, *49*(1), 245-262.

[24]. Vyas, B. Ethical Implications of Generative AI in Art and the Media. *International Journal for Multidisciplinary Research (IJFMR), E-ISSN*, 2582-2160.

[25]. Dr. Santosh Kumar Singh “**Blockchain-Based Model for Cloud Computing Security**”, “International Journal of Advanced Research in Computer and Communication Engineering, (IJARCCE), Vol 12, Issue 8, pp. 7-19, DOI: 10.17148/IJARCCE.2023.12802 https://ijarcce.com/papers/blockchain-based-model-for-cloud-computing-security/

[26]. Dr. Santosh Kumar Singh, Dr. Varun Tiwari, Dr. Vikas Rao Vadi **“Blockchain Creation Using Java Programming Language** “International Journal of Advanced Research in Computer and Communication Engineering, (IJARCCE), Vol-12, Issue 4, April 2023, ISSN: 2278-1021, pp. 1082-1086, DOI: 10.17148/IJARCCE.2023.124188 **https://ijarcce.com/papers/blockchain-creation-using-java-programming-language/**

[27]. Dr. Santosh Kumar Singh, Dr. Varun Tiwari, Dr. Vikas Rao Vadi **“Smart Contract Using Solidity (Remix – Ethereum IDE)** “International Journal of Advanced Research in Computer and Communication Engineering, (IJARCCE), Vol-12, Issue 2, Feb 2023, ISSN: 2278-1021, pp. 243-249, DOI 10.17148/IJARCCE.2023.12253 **https://ijarcce.com/papers/smart-contract-using-solidity-remix-ethereum-ide/**

[28]. Singh, S. K.., & Vadi, V. R... (Jan 2023). Use of Blockchain in Crypto-Currency to secure cloud forensic trails. *Trinity Journal of Management, IT & Media (TJMITM)*, *14*(1), 1–8. https://doi.org/10.48165/tjmitm.2023.1401.https://acspublisher.com/journals/index.php/tjmitm/article/view/3334

[29]. Santosh Kumar Singh, Dr. Vikas Rao Vadi “**Evolutionary Transformation of Blockchain Technology,** www.ijert.org, ISSN – 2278-0181, Vol. 10, Issue – 1, pp. 26-30, **January 2022**. https://www.ijert.org/research/evolutionary-transformation-of-blockchain-technology-IJERTCONV10IS01008.pdf

[30]. Singh, S. K.., Vadi, V. R.., Tiwari, A., & Pandey, P. K. (2021). **Security Aspect of Blockchain Technology**. Trinity Journal of Management, IT & Media (TJMITM), 12(1), 39–44. https://doi.org/10.48165/tjmitm.2021.1106 https://acspublisher.com/journals/index.php/tjmitm/article/view/399

[31]. Singh, S. K., Vadi, V. R., & Singh, S. (2021). **Multi-keyword parallel ciphertext retrieval method.** *Trinity Journal of Management, IT & Media (TJMITM)*, *12*(1), 1–3. https://doi.org/10.48165/tjmitm.2021.1101 **https://acspublisher.com/journals/index.php/tjmitm/issue/view/26**

[32]. Santosh Kumar Singh, Dr. P.K. Manjhi, Dr. Rajesh Kumar Tiwari (2020) **UCON-Based Data Protection Protocol for Cloud Environment**. *Journal of Critical Reviews*, 7 (18), 2480-2486. doi:10.31838/JCR.07.18.310 **(Scopus Indexed). http://jcreview.com/?mno=115632**

[33]. Santosh Kumar Singh, Dr. P. K. Manjhi and Dr. R. K. Tiwari **“Cloud Computing Security Using Steganography”** Journal of Emerging Technologies and Innovative Research, (JETIR), Volume VI, Issue VI, 6th June 2K19www.jetir.org ISSN 2349-5162, pp. 923-927, **(UGC Approved Journal).**

[34]. Singh, S. K., Manjhi, P. K., Tiwari, R. K., & Vadi, V. R. (2018). **Cloud Computing and Security Issues in the Cloud**. *Trinity Journal of Management, IT & Media*, *9*(1), 22–27. https://doi.org/10.48165/tjmitm.2018.0905 (CITE) https://acspublisher.com/journals/tjmitm/current-issues/

[35]. Santosh Kumar Singh, Dr. P. K. Manjhi and Dr. R. K. Tiwari, Dr. V. R. Vadi **“A Secure Communication Scheme for Cloud Environment”** International Journal of Computer Engineering and Applications, (IJCEA), Volume XII, Issue IV, April 18www.ijcea.com ISSN 2321-3469, pp. 97-106, **(UGC Approved Journal).**

[36]. Santosh Kumar Singh, P. K. Manjhi and Dr. R.K. Tiwari “**ELLIPTIC CURVE CRYPTOGRAPHY IN CLOUD COMPUTING SECURITY”** International Journal of Computer Engineering and Applications, (IJCEA), Volume XII, Issue III, March 18www.ijcea.com ISSN 2321-3469, pp. 179-183, **(UGC Approved Journal).**

[37]. Santosh Kumar Singh, Dr. P.K. Manjhi, Dr. R. K. Tiwari **“Data Security using RSA Algorithm in Cloud Computing** “International Journal of Advanced Research in Computer and Communication Engineering, (IJARCCE), Vol-5, Issue 8, Aug2016, ISSN: 2278-1021, pp.11-16, DOI 10.17148/IJARCCE.2016.5803.

[38]. Santosh Kumar Singh, Dr. P.K. Manjhi, Dr. R.K. Tiwari **“An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing Using ECC”** International Journal of Advanced Research in Computer and Communication Engineering, (IJARCCE), Vol-5, Issue 7, July 2016, ISSN: 2278-1021, pp. 5-15, DOI 10.17148/IJARCCE.2016.5702.

[39]. Santosh Kumar Singh, Dr. P.K. Manjhi, Dr. R. K. Tiwari **“An Approach towards Data Security in the Cloud Computing Using AES**” International Journal of Advanced Research in Computer and Communication Engineering, (IJARCCE), Vol-5, Issue 6, June 2016, ISSN: 2278-1021, pp. 22-29, DOI 10.17148/IJARCCE.2016.5605.

[40]. Santosh Kumar Singh, Dr. P.K. Manjhi, Dr. R.K. Tiwari **“Cloud Computing Security Applied by Homomorphic Encryption”** International Journal of Advanced Research in Computer and Communication Engineering, (IJARCCE), Vol-5, Issue 5, May 2016, ISSN: 2278-1021, pp. 891-896, DOI 10.17148/IJARCCE.2016.55218.

[41]. Santosh Kumar Singh, Dr. P.K. Manjhi and Dr. R. K. Tiwari “**Cloud Computing Security and Trust Enhancement by using OTP”**, International Journal of Innovative Research in Computer and Communication Engineering, (IJIRCCE), Vol.4, Issues5, and ISSN: 2320-9798, DOI: 10.15680/IJIRCCE.2016. 0405069, May 2016.