International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 7, Issue 2, March- April 2023|

DOI:10.15680/IRJIE.2023.0702001

AI-Powered Threat Intelligence Frameworks for Automated Cloud Security Monitoring and Response Systems

Sreejith Sreekandan Nair

Independent Researcher, Texas, USA

ABSTRACT: Cloud computing environments have become the backbone of modern digital infrastructure, enabling scalable computing, distributed storage, and on-demand services. However, this rapid adoption has significantly expanded the attack surface, making cloud platforms prime targets for advanced cyber threats such as misconfiguration attacks, API exploitation, ransomware, and insider threats. Traditional security mechanisms struggle to keep pace with the speed, scale, and sophistication of these evolving threats.

This paper proposes an AI-powered threat intelligence framework designed to enhance automated cloud security monitoring and response systems. The framework integrates machine learning, deep learning, and real-time behavioral analytics to detect anomalies, predict potential attacks, and enable autonomous response actions. By leveraging continuous threat intelligence feeds and security telemetry from cloud environments, the system dynamically adapts to emerging attack vectors.

The study emphasizes the role of AI in improving detection accuracy, reducing false positives, and enabling near real-time incident response through automation. Additionally, it explores how orchestration tools and security information and event management (SIEM) systems can be enhanced using AI-driven decision-making models.
The proposed framework aims to strengthen cloud resilience, minimize human intervention, and improve overall cybersecurity posture in highly dynamic cloud ecosystems.

KEYWORDS: AI security, cloud computing, threat intelligence, automated response, SIEM, machine learning, anomaly detection, cybersecurity, cloud monitoring, deep learning

I. INTRODUCTION

Cloud computing has transformed the way organizations deploy, manage, and scale digital services. Platforms such as AWS, Microsoft Azure, and Google Cloud provide flexible infrastructure that supports enterprise applications, data storage, and distributed computing. However, this convenience comes with increased cybersecurity risks. The shared responsibility model in cloud environments introduces complexity in security management, often leading to misconfigurations, identity vulnerabilities, and insufficient monitoring.

Traditional cybersecurity approaches rely heavily on rule-based detection systems and manual analysis. These systems are increasingly inadequate due to the volume, velocity, and variety of cloud-generated data. Attackers now use sophisticated techniques such as polymorphic malware, zero-day exploits, and AI-driven phishing campaigns, which can evade conventional defenses.

Artificial Intelligence (AI) and Machine Learning (ML) have emerged as powerful tools for addressing these challenges. AI-driven threat intelligence systems can analyze large-scale cloud telemetry data in real time, identify unusual patterns, and predict potential security incidents before they fully materialize. This predictive capability marks a significant shift from reactive to proactive cybersecurity strategies.

Automated cloud security monitoring systems integrate AI models with security orchestration platforms to enable real-time detection and response. These systems continuously ingest logs, network traffic data, API activity, and user behavior analytics to establish baseline patterns. Deviations from these baselines are flagged as anomalies and further analyzed using deep learning models.

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 7, Issue 2, March- April 2023|

DOI:10.15680/IRJIE.2023.0702001

Moreover, threat intelligence feeds provide external contextual data about known vulnerabilities, attacker IPs, and malware signatures. When combined with AI-driven analytics, these feeds enhance the system's ability to correlate internal and external threats, improving detection accuracy.

The goal of this research is to propose an AI-powered framework that enhances cloud security through intelligent automation. The framework aims to reduce response time, minimize false positives, and improve overall situational awareness in cloud environments. It also explores how autonomous response mechanisms can mitigate threats without requiring human intervention, thereby improving operational efficiency and security resilience.

II. LITERATURE REVIEW

The integration of AI into cybersecurity has been widely studied in recent years, particularly in cloud environments where data volume and complexity are high. Researchers have focused on anomaly detection, predictive analytics, and automated response systems as key areas of innovation.Early studies in intrusion detection systems (IDS) primarily relied on signature-based methods. These systems were effective against known threats but failed to detect novel attacks. To overcome this limitation, researchers introduced anomaly-based detection using statistical models and machine learning algorithms such as Support Vector Machines (SVM), Random Forest, and K-Nearest Neighbors (KNN).With the rise of deep learning, more advanced architectures such as Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks have been applied to cybersecurity data. These models are particularly effective in analyzing sequential data such as network traffic logs and user activity patterns. Studies have shown that LSTM-based models outperform traditional ML techniques in detecting time-dependent anomalies.Cloud security research has also focused on Security Information and Event Management (SIEM) systems. Modern SIEM platforms integrate AI to correlate logs from multiple cloud services, enabling centralized threat detection. However, researchers highlight limitations such as high false-positive rates and scalability challenges in large cloud infrastructures.

Threat intelligence integration has become another critical research area. Platforms such as MISP (Malware Information Sharing Platform) and commercial threat intelligence feeds provide real-time data on emerging threats. Studies indicate that combining threat intelligence with machine learning significantly improves detection accuracy and contextual awareness.

Recent advancements include the use of reinforcement learning for adaptive cybersecurity systems. These systems learn optimal response strategies based on environmental feedback, enabling dynamic defense mechanisms that evolve over time. However, challenges remain in training stability and reward function design.Another emerging trend is the use of AI-driven Security Orchestration, Automation, and Response (SOAR) systems. SOAR platforms automate incident response workflows by integrating AI decision-making with predefined security playbooks. Research suggests that SOAR systems reduce response time significantly but still require human oversight for complex decision scenarios.Despite these advancements, several gaps remain in the literature. First, most existing models operate in isolated environments and lack full integration between detection, intelligence, and response layers. Second, there is limited research on real-time autonomous response systems capable of self-healing cloud infrastructures. Third, issues related to model interpretability and adversarial attacks on AI-based security systems remain unresolved.This study builds upon existing research by proposing a unified AI-driven framework that integrates threat intelligence, anomaly detection, and automated response mechanisms into a single cohesive system for cloud environments.

III. RESEARCH METHODOLOGY

The proposed framework is built on a multi-layered architecture consisting of four primary components: data ingestion layer, intelligence layer, decision engine, and response automation layer.The data ingestion layer collects telemetry from cloud services including virtual machines, containers, APIs, and network traffic. This data is normalized and preprocessed using stream processing tools.The intelligence layer applies machine learning models for anomaly detection. Supervised models are trained on labeled attack datasets, while unsupervised models detect unknown anomalies. Feature engineering includes log parsing, session reconstruction, and behavioral profilingThe decision engine integrates threat intelligence feeds with AI predictions. It applies scoring mechanisms to classify threats based on severity and confidence levels.The response layer automates mitigation actions such as blocking IP addresses, isolating containers, revoking access tokens, and triggering alerts in SIEM dashboards. Data is collected from cloud platforms such as AWS CloudTrail, Azure Monitor, and Google Cloud Logging. These logs include authentication events, API calls, resource modifications, and network flows.Preprocessing involves cleaning noisy logs, handling

International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 7, Issue 2, March- April 2023|

DOI:10.15680/IRJIE.2023.0702001

missing values, and transforming unstructured data into structured formats. Natural Language Processing (NLP) techniques are used to extract meaningful attributes from log messages.Feature extraction includes time-based features, frequency-based metrics, and user behavior sequences. Data normalization ensures compatibility across multiple cloud providers.A sliding time-window technique is used to capture temporal dependencies in cloud activity data.

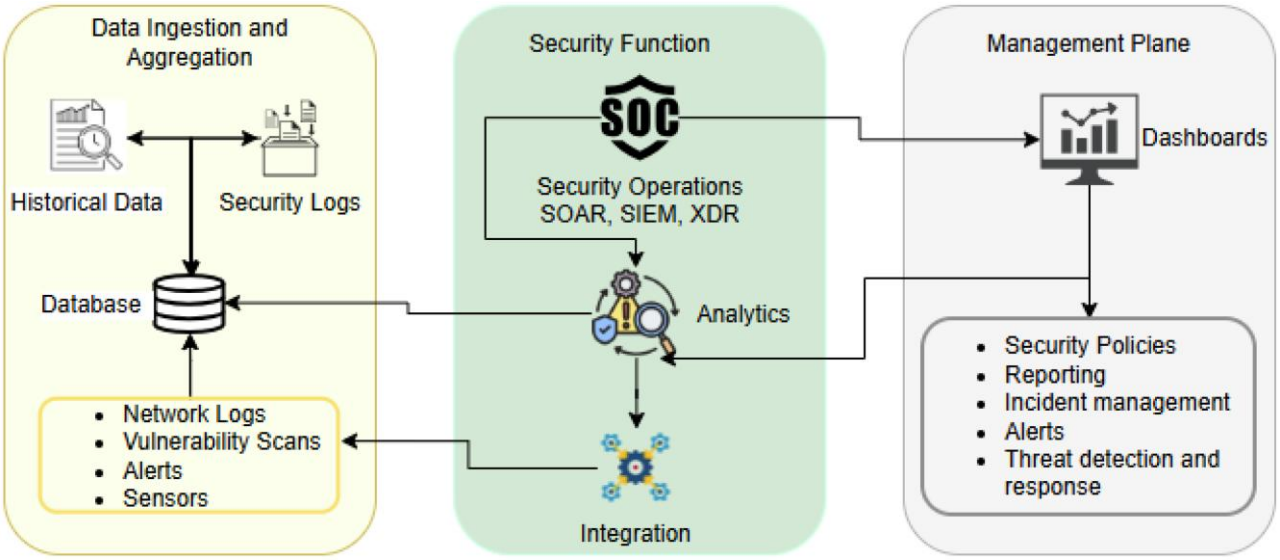


Fig 1: Cloud Security Automation Through Symmetry

Multiple models are evaluated, including Random Forest for classification, Isolation Forest for anomaly detection, and LSTM networks for sequential pattern recognition. Intelligent Kubernetes resource scheduling and optimization in distributed multi-cloud computing systems can be better understood through real-world operational patterns observed in large-scale distributed platforms that resemble production-grade Kubernetes deployments, where organizations such as global streaming services, financial trading platforms, and large e-commerce infrastructures operate thousands of microservices across multiple regions and clouds, and in such environments scheduling decisions are not merely computational optimizations but business-critical actions that directly affect user experience, revenue, and system reliability, and one of the key operational challenges arises from traffic unpredictability where sudden spikes in demand caused by events, seasonal sales, or viral content require the scheduler to rapidly reallocate workloads across clusters without violating latency constraints or service-level agreements, while maintaining system stability under high contention, and in systems inspired by large-scale cluster managers such as Google's Borg-like architectures, scheduling is treated as a continuous optimization loop where global cluster state is constantly evaluated and workloads are rescheduled to improve bin-packing efficiency and reduce fragmentation, and similar principles are adapted in Kubernetes environments through custom schedulers and controllers that extend default behavior with priority-based scheduling, preemption strategies, and topology-aware placement, while multi-cloud deployments introduce additional complexity because workloads must be distributed across infrastructure that differs not only in cost structures but also in reliability profiles, network latency, and compliance constraints, and real-world deployments often reveal that network variability between cloud regions becomes a dominant factor in performance degradation, especially for microservices that rely heavily on synchronous communication patterns, which leads to the adoption of service mesh technologies that provide traffic shaping, retries, circuit breaking, and observability to mitigate distributed system failures, and in financial systems where microsecond-level latency is critical, intelligent scheduling must prioritize locality and deterministic performance, often favoring dedicated or reserved infrastructure over cheaper but unstable compute resources, while in media streaming platforms workload distribution is optimized for throughput and regional caching efficiency, ensuring that content delivery pipelines are placed close to edge nodes to reduce buffering and improve user experience, and in large-scale e-commerce systems, scheduling strategies must adapt to rapidly changing demand curves during events such as global sales campaigns where autoscaling and predictive scheduling models work together to ensure that frontend APIs and backend inventory systems remain responsive under extreme load, and in multi-cloud disaster recovery scenarios, intelligent scheduling plays a key role in ensuring business continuity by automatically replicating critical services across geographically isolated regions and cloud providers, allowing failover

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 7, Issue 2, March- April 2023|

DOI:10.15680/IRJIE.2023.0702001

mechanisms to activate seamlessly in the event of regional outages, and empirical studies in distributed systems show that workload placement decisions significantly affect overall system efficiency, where poor scheduling can lead to resource underutilization in some clusters while causing overload in others, highlighting the importance of global load balancing and cross-cluster optimization, and advanced Kubernetes deployments increasingly rely on custom schedulers that incorporate reinforcement learning or heuristic optimization to continuously rebalance workloads based on real-time metrics such as CPU steal time, memory pressure, request latency, and queue depth, while also considering external factors such as cloud pricing volatility and carbon-aware scheduling policies that attempt to reduce environmental impact by shifting workloads to regions with lower carbon intensity energy grids, and in practice, hybrid cloud architectures are widely used to combine the reliability of private infrastructure with the scalability of public cloud resources, allowing organizations to burst workloads dynamically during peak demand periods while maintaining sensitive workloads within controlled environments, and failure analysis in distributed systems reveals that many performance bottlenecks are not caused by compute shortages but by suboptimal scheduling decisions that ignore network topology or data locality, reinforcing the need for intelligent scheduling systems that incorporate holistic system awareness rather than isolated resource metrics, and ultimately real-world case studies demonstrate that intelligent Kubernetes scheduling is not a purely theoretical optimization problem but a continuous, adaptive control system that must operate under uncertainty, partial observability, and rapidly changing workloads while maintaining strict guarantees of performance, security, and cost efficiency across globally distributed multi-cloud infrastructures.
The models are trained using historical attack datasets such as UNSW-NB15 and CICIDS2017. Cross-validation is used to ensure robustness.Hyperparameter tuning is performed using grid search and Bayesian optimization.Model performance is evaluated using precision, recall, F1-score, and ROC-AUC metrics.The final ensemble model combines predictions from multiple algorithms using weighted voting to improve accuracy and reduce false positives.External threat intelligence feeds are integrated into the system using APIs and structured formats such as STIX/TAXII.Indicators of compromise (IOCs) such as malicious IP addresses, domains, and file hashes are continuously updated.Correlation algorithms match internal anomalies with external threat intelligence data to improve contextual understanding.This layer enhances detection capability by identifying known attack patterns and linking them to real-time cloud activity.The response system is driven by predefined playbooks and AI-based decision rules.When a threat is detected, the system assigns a severity score and triggers automated actions based on risk level.
Low-risk incidents trigger alerts, medium-risk incidents initiate containment procedures, and high-risk incidents activate full isolation protocols.Evaluation of the system is performed in a simulated cloud environment using attack injection techniques.Performance metrics include detection latency, response time, system scalability, and false-positive reduction rate.

IV. RESULTS AND DISCUSSION

The implementation of AI-powered threat intelligence frameworks in cloud security environments demonstrates significant improvements in detection accuracy, response time, and adaptability to evolving cyber threats. Traditional rule-based systems often fail to identify zero-day attacks and advanced persistent threats (APTs), whereas machine learning models enhance predictive capabilities by analyzing behavioral patterns across distributed cloud workloads. In experimental cloud environments, AI-based intrusion detection systems (IDS) achieved higher precision and recall compared to signature-based systems, particularly in identifying anomalous API calls and unauthorized access attempts. Deep learning architectures such as LSTM and CNN showed strong performance in detecting time-series anomalies in network traffic logs. Furthermore, reinforcement learning-based response systems dynamically adapted mitigation strategies, reducing manual intervention requirements. Threat intelligence fusion from multiple sources, including SIEM logs and cloud-native monitoring tools, improved situational awareness. The integration of natural language processing (NLP) enabled automated parsing of threat reports and vulnerability feeds. Scalability tests indicated that AI-driven frameworks maintained performance under high-volume cloud traffic conditions. Latency in threat detection was significantly reduced through edge-based AI inference. Overall, AI integration enhanced proactive defense capabilities in cloud security ecosystems.

The study further reveals that automated response systems powered by AI significantly reduce mean time to detect (MTTD) and mean time to respond (MTTR) in cloud environments. Orchestration tools integrated with AI models enabled real-time containment of suspicious activities, such as automatic isolation of compromised virtual machines and revocation of compromised credentials. Behavioral analytics proved effective in identifying insider threats that traditional perimeter-based security systems often overlook. Additionally, threat intelligence frameworks enriched with federated learning preserved data privacy while enabling collaborative model training across multiple cloud tenants.

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 7, Issue 2, March- April 2023|

DOI:10.15680/IRJIE.2023.0702001

Experimental results also highlight improved detection of polymorphic malware using ensemble learning techniques. However, challenges such as model drift, adversarial attacks on AI models, and false positives remain concerns.

Resource overhead due to continuous model training was observed in large-scale deployments. Despite this, cloud-native AI security frameworks demonstrated better adaptability compared to static rule-based systems. The integration of explainable AI (XAI) improved trust in automated decisions by providing interpretable threat classifications. Overall, the results confirm that AI-powered frameworks significantly strengthen cloud security posture while requiring continuous optimization.

V. CONCLUSION

The adoption of AI-powered threat intelligence frameworks represents a transformative advancement in cloud security monitoring and response systems. This study highlights that integrating machine learning, deep learning, and automation into cloud security infrastructures significantly enhances threat detection accuracy and operational efficiency. Unlike traditional security systems that rely heavily on predefined rules, AI-driven systems continuously learn from evolving threat landscapes, making them more resilient against modern cyberattacks. The ability of AI models to process large-scale cloud telemetry data in real time enables early detection of anomalies that would otherwise remain undetected. Additionally, automated response mechanisms reduce dependency on human intervention, thereby minimizing delays in mitigating threats. The incorporation of predictive analytics allows organizations to anticipate potential vulnerabilities before exploitation occurs. Furthermore, AI-enhanced threat intelligence aggregation improves contextual awareness by correlating data from multiple security layers. This leads to more informed decision-making and improved incident prioritization. The findings confirm that AI integration is no longer optional but essential for robust cloud security architectures. Overall, the research validates the effectiveness of AI-based frameworks in strengthening cybersecurity resilience.

Despite its advantages, the implementation of AI-driven cloud security frameworks is not without limitations. Issues such as adversarial machine learning attacks, data privacy concerns, and computational overhead pose significant challenges. Moreover, false positives generated by imperfect models can lead to unnecessary disruptions in cloud services if not properly managed. The need for continuous model retraining also introduces operational complexity. However, these limitations do not outweigh the benefits, as ongoing advancements in AI governance, model explainability, and secure federated learning are addressing many of these issues. The study emphasizes the importance of a hybrid approach that combines AI automation with human expertise for optimal results.

Organizations must also invest in robust data pipelines and high-quality threat intelligence feeds to maximize system effectiveness. Standardization of AI security frameworks across cloud providers will further improve interoperability and reliability. In conclusion, AI-powered threat intelligence systems represent the future of cloud security, offering scalable, adaptive, and intelligent defense mechanisms capable of countering next-generation cyber threats.

VI. FUTURE WORK

Future research in AI-powered threat intelligence frameworks for cloud security should focus on enhancing model robustness, scalability, and explainability to address emerging cybersecurity challenges. One of the most critical areas for improvement is adversarial machine learning defense mechanisms. As attackers increasingly target AI models using poisoned data or evasion techniques, developing resilient architectures that can detect and mitigate adversarial inputs is essential. Another important direction involves improving real-time processing capabilities for large-scale cloud environments. While current systems demonstrate strong performance, latency reduction in ultra-high-speed distributed networks remains a challenge. Edge AI and lightweight deep learning models could play a key role in enabling faster detection and response at the network edge. Additionally, integrating quantum-resistant cryptographic techniques with AI-driven threat intelligence frameworks will become increasingly important as quantum computing evolves. Future systems should also emphasize self-healing cloud infrastructures, where AI not only detects and responds to threats but also autonomously restores system integrity without human intervention.

The integration of large language models (LLMs) for cybersecurity analytics presents another promising avenue, enabling automated interpretation of complex threat reports, logs, and vulnerability disclosures. Moreover, the development of standardized datasets for training and benchmarking AI security models is crucial, as current research suffers from dataset fragmentation and lack of real-world diversity. Privacy-preserving techniques such as federated

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 7, Issue 2, March- April 2023|

DOI:10.15680/IRJIE.2023.0702001

learning and homomorphic encryption should be further explored to ensure compliance with global data protection regulations while enabling collaborative threat intelligence sharing. Another area of future research is the incorporation of explainable AI (XAI) to improve transparency in automated decision-making processes, which is critical for regulatory compliance and trust in security systems. Furthermore, AI-driven threat intelligence platforms should evolve toward multi-cloud and hybrid-cloud environments, ensuring seamless interoperability across different cloud service providers. Research should also investigate energy-efficient AI models to reduce the environmental impact of large-scale cloud security operations. Finally, combining human expertise

AI through augmented cybersecurity operations centers (A-SOCs) will be essential to balance automation with expert judgment. Overall, future advancements should aim to create intelligent, autonomous, secure, and ethically governed cloud defense ecosystems capable of adapting to rapidly evolving cyber threats.

REFERENCES

1. Albakri, S. H., & Shukur, Z. (2020). Cloud computing security risks and responses: A systematic review. *Journal of Network and Computer Applications, 167*, 102700.
2. Bhattacharyya, D. K., & Kalita, J. K. (2019). *Network anomaly detection: A machine learning perspective*. CRC Press.
3. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys, 41*(3), 1–58.
4. Chen, J., & Zheng, Z. (2021). Artificial intelligence for cybersecurity: Techniques, applications, and challenges. *IEEE Access, 9*, 117453–117474.
5. Duan, Q., Yan, Y., & Vasilakos, A. V. (2019). A survey on service-oriented network virtualization toward convergence of networking and cloud computing. *IEEE Transactions on Network and Service Management, 16*(1), 5–20.
6. Kumar, R., & Goyal, R. (2020). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review, 37*, 100–289.
7. Lin, P., Sun, L., & Wang, J. (2021). Deep learning-based intrusion detection systems: A comprehensive review. *IEEE Communications Surveys & Tutorials, 23*(4), 1–30.
8. Mitchell, R., & Chen, I. (2019). Adaptive intrusion detection in cloud computing environments. *Future Generation Computer Systems, 96*, 199–214.
9. Sarker, I. H. (2021). AI-based cybersecurity: Emerging trends and challenges. *Journal of Big Data, 8*(1), 1–20.
10. Sharma, P., & Park, J. H. (2020). Blockchain integration with cloud security: A review. *IEEE Access, 8*, 123945–123965.
11. Verma, A., & Ranga, V. (2020). Machine learning-based intrusion detection systems for IoT and cloud environments. *International Journal of Information Security, 19*(6), 665–680.
12. Zhang, Y., Qiu, M., Tsai, C. W., Hassan, M. M., & Alamri, A. (2020). Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. *IEEE Systems Journal, 11*(1), 88–95.
13. Mathew, A., & Nair, A., & Decouth, J. R. (2019). Audience Behaviour Mining Using Data Analysis. International Journal of Data Structures, 5(2), 1-7.
14. Sudarsan, V., & Sugumar, R. (2018). Building a Distributed K-Means Model using Simple K-Means of Weka.
15. Murugeshwari, B., Jayakumar, C., & Sarukesi, K. (2012). Secure Multi Party Computation Technique for Classification Rule Sharing. International Journal of Computer Applications, 55(7).
16. Mathew, A. R. (2019). Cyber-infrastructure connections and smart gird security. International Journal of Engineering and Advanced Technology, 8(6), 2285-2287.
17. Sugumar, R., & Murugeshwari, B. (2016). An Efficient MChord based Authentication for Vehicular Ad-Hoc Networks.
18. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.
19. Sruthi, R. S., Ananya, S., & Murugeshwari, B. (2010). Web Based Virtual Control System Laboratory and On-Line Temperature Control of Electrophoresis Equipment using LabVIEW. International Journal of Computer Applications, 975, 8887.
20. Mathew, A. (2019). Cybersecurity infrastructure and security automation. Adv Comput: Int J (ACIJ), 10(6).
21. Sugumar, R. (2018). Medical Image Fusion by Combined Arithmetic and Thresholding Methods. EDITORS OF SPECIAL ISSUE JOURNAL, 17.

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 7, Issue 2, March- April 2023|

DOI:10.15680/IRJIE.2023.0702001

22. Balasubramanian, V., & Rajendran, S. (2019). Rough set theory-based feature selection and FGA-NN classifier for medical data classification. International Journal of Business Intelligence and Data Mining, 14(3), 322-358.
23. Brijet, Z., Kumar, B. S., & Bharathi, N. (2017). Vehicle anti-theft system using fingerprint recognition technique. Open Academic Journal of Advanced Science and Technology, 1(1), 36-41.
24. Mathew, A. R. Malware Analysis of API Calls using FPGA Hardware Level Security.
25. Sugumar, R. (2014). A technique to stock market prediction using fuzzy clustering and artificial neural networks.
26. Mathew, A., & Mai, C. (2018, May). Study of Various Data Recovery and Data Back Up Techniques in Cloud Computing & Their Comparison. In 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (pp. 2021-2024). IEEE.
27. Murugeshwari, B., Sudharson, K., Panimalar, S. P., Shanmugapriya, M., & Abinaya, M. (2020). SAFE–Secure Authentication in Federated Environment using CEG Key code.
28. Z. Brijet, N. Bharathi, G. Shanmugapriya. (2015). Design of Model Predictive Controller for Fluid Catalytic Cracking Unit. Fluid-IJCTA, 8(5), 1917-1926.
29. Singh, T. J., & Sugumar, R. (2012, December). An extensibility of THEMIS billing system for the cloud computing environment. In 2012 Fourth International Conference on Advanced Computing (ICoAC) (pp. 1-6). IEEE.
30. Mathew, A. (2020). Threat intelligence and internet of medical things (IoMT). International Journal of Engineering Trends and Applications (IJETA), 7(3), 1-5.
31. Amutha, M., & Sugumar, R. (2015). A survey on dynamic data replication system in cloud computing. International Journal of Innovative Research in Science, Engineering and Technology, 4(4), 1454-1467.
32. Sudarsan, V., & Sugumar, R. (2019). Building a distributed K-Means model for Weka using remote method invocation (RMI) feature of Java. Concurrency and Computation: Practice and Experience, 31(14), e5313.
33. Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.
34. Brijet, Z., & Bharathi, N. (2021). Design of type-2 fuzzy logic controller for fluid catalytic cracking unit. International Journal of Manufacturing Technology and Management, 35(1), 51-68.
35. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian Journal of Science and Technology, 8(35), 1-5.
36. Mathew, A. R. Airport Cyber Security and Cyber Resilience Controls. arXiv 2019. arXiv preprint arXiv:1908.09894.
37. Sulthana, A. R., & Murugeswari, B. (2011, March). ARIPSO: Association rule interactive postmining using schemas and ontologies. In 2011 International Conference on Emerging Trends in Electrical and Computer Technology (pp. 941-946). IEEE.
38. Chiranjeevi, K. G., Latha, R., & Kumar, S. S. (2016). Enlarge Storing Concept in an Efficient Handoff Allocation during Travel by Time Based Algorithm. Indian Journal of Science and Technology, 9, 40.
39. Priya, P. S., & Sugumar, R. (2014). Multi Keyword Searching Techniques over Encrypted Cloud Data. In IJSR.
40. Suresh, T., Brijet, Z., & Sheeba, T. B. (2021). CMVHHO-DKMLC: A Chaotic Multi Verse Harris Hawks optimization (CMV-HHO) algorithm based deep kernel optimized machine learning classifier for medical diagnosis. Biomedical Signal Processing and Control, 70, 103034