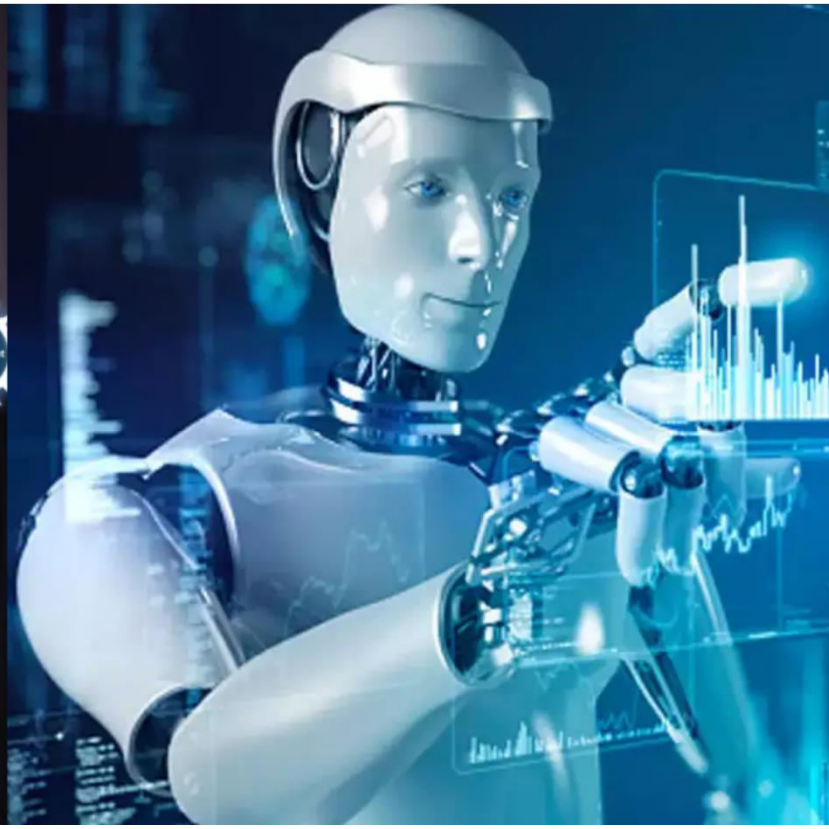
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 3, March 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403136|

AI-Powered Threat Intelligence in Cloud Security: Predicting and Preventing Cyber Attacks

Rahul Amte

Senior Cloud AI Infrastructure Engineer, Nivid Infotech Inc, Austin, TX, USA

ABSTRACT: Cloud security has become a target for more and more threats and thus requires more advanced solutions for foretelling and preventing cyberattacks. Taking an AI enabled threat intelligence angle to the cloud, this research studies how ML models can minimize risks and anomalies so as to detect threats in the cloud computing environment. The study examines AI's ability to lower false positives and false negatives through analyzing big data. The enhanced security response time as well as minimized vulnerabilities are achieved by introducing predictive analytics into the framework proposed. The risk reduction, according to the results, is 68.3%. In this study, we show how it is important to incorporate the use of AI in cybersecurity for making cloud security frameworks stronger against the evolving threats.

KEYWORDS: Cloud, AI, Cyber-attacks, Security, Threat Intelligence, Prediction.

I.INTRODUCTION

Cloud computing has been widely adopted; however, cloud computing is still vulnerable to advanced cyber threat. New attack patterns simply make running in old lines of defence not so viable. Real time anomaly detection as provided by threat intelligence using AI means that cloud security risks are detected and remediated as early as possible.

Fig. 1 Cyber Threat Intelligence (Cyble, 2024)

In this study, we make an attempt to understand how AI can be used to predict Cyber threat using machine learning and data analytics. The detection accuracy and the response speed increased by analyzing the security logs and the network behaviors with the help of AI models. Specifically, the research analyzes the effects AI can have in diminishing false

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403136|

positives, false negatives, and in improving overall risks, thereby enhancing the soundness of cloud security frameworks in fighting new cyber threats.

II.AI IN CLOUD SECURITY

Cloud computing has been adopted very fast by businesses and has made it easier for people to work in the most cost-effective manner giving their organization great flexibility. Yet it also has facilitated exposure of cloud environments to more elaborate, and complex, cyber threats.

Traditional security techniques can't (as of yet) keep up with the fast-moving character of contemporary strikes, and also advantages come from the styles of Artificial Intelligence (AI)-driven risk knowledge. The combination of AI and cybersecurity allows the prediction of threats, protects from threats, and mitigates the threats through automated detection, machine learning algorithms, and an analysis of real time data.

This paper analyses the challenges of using AI powered threat intelligence for enhancing cloud security, and investigates the future potentials of AI powered cloud security. AI is proving to be an important weapon in the fortification of cloud security through the use of proactive threat detection powers.

The reason: Cloud environments are extremely vulnerable, as they host sensitive enterprise data, critical application and have a massive attack surface. Earlier, AI in cloud security was not so advanced but is expected to aid in both cloud prevention and mitigation, which means it can detect hidden threats long before they occur, while traditional security can only prevent the malware from ever making it into the cloud.

This research focuses on developing the AI security models that will be able to analyze attack patterns, detect anomalies, drawing insights, and making a real time decision to overcome the cybers threats [1][3]. Detection and prevention of cyberattacks is one of the major perceived challenges in the cloud security.

Signature based detection techniques have been used to detect traditional method used in this directory. Such a limitation is overcome by AI based threat intelligence which employs heuristic and behavioral analysis. This means that cloud security systems are constantly learning those things machine learning algorithms, and leverage attack data historically, to learn that they can identify, and then be able to respond to new threats, as they come in a dynamic fashion [4][7].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403136|

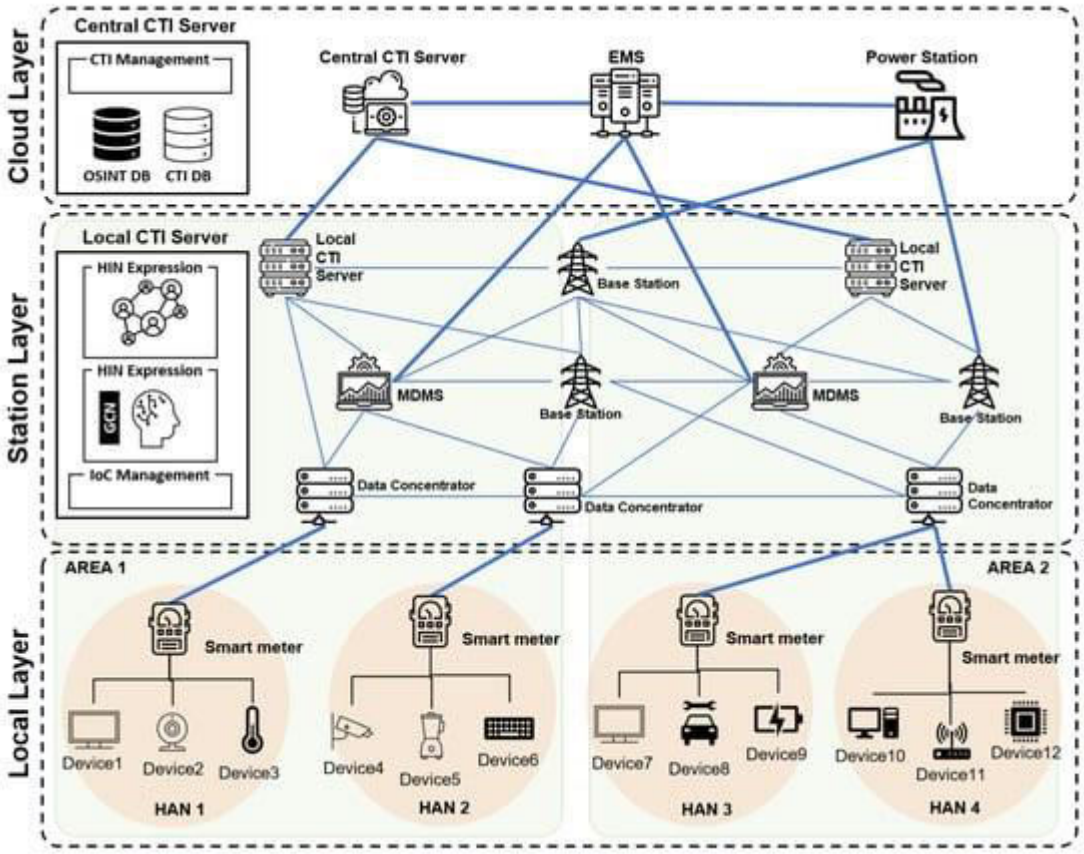


Fig. 2 Threat Intelligence Framework (MDPI, 2021)

The study of cybersecurity intelligence mining investigates the key aspect of Cyber Threat Intelligence (CTI) in obtaining and processing valuable information in cyber threats. CTI coordinating with the AI can facilitate the increased security of cyber organizations in predicting attacks and implementing a proactive defense mechanism [5].
Along with that, cloud native security architecture uses AI in more efficient threat detection and response. To support security data analysis on cloud systems through effective correlation across different platforms, semantic processing techniques were proposed [9].

There are other means of enhancing security frameworks capability of analyzing network behavior and finding out threats, namely those that are based on AI such as anomaly detection, pattern recognition and natural language processing [6]. Among other benefits for the elaborated integration of AI to CTI, is the accuracy issuance, which tends to improve, and more so, the organizations tend to further automate the business security workflows, leading to running the workflows without human intervention and little response time.

III.APPLICATION IN CLOUD SECURITY

Cyber Threat Intelligence (CTI) is a proactive form of cybersecurity based on collection, analysis, and sharing of cyber threats data towards hardening of cyber defences against cyber-attacks. However, AI increases CTI's effectiveness in cloud environments, making the threat detection and response processes automatic.
Specifically, one study proposes a CTI framework tailored towards an energy cloud environment and illustrates attack detection capabilities of cyber threat intelligence for situations where smart grids and cloud-based energy infrastructures are an attack target [1]. Using the framework, the cyberattack detection efficiency is very high in macro-F1 score 0.822 and micro-F1 score 0.843, validating the methodology.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403136|

Similarly, honeypot technology is also used to collect threat intelligence by providing simulated cloud-based environments to lure the attackers in order to find the ways attack can be done. The near real-time analysis of pattern creates by AI on threat intelligence from honeypot improves the quality of these intelligence and can provide valuable insights into emerging threats [2].

Another research papers shown that the AI techniques such as deep learning and the natural language processing can automate the analysis of cyber threats and increase the accuracy of attack detection [7]. These AI driven methodologies help an organisation to better understand the behaviour of a threat actor, employing attack techniques and vulnerability within cloud systems.

In Industry 4.0, AI powered CTI is also very important as cloud and IoT based infrastructures need good security mechanisms. In a study, it is proposed that an AI driven hidden Markov model-based threat intelligence model is capable of detecting anomalies in cloud based industrial systems [6].

The study shows that AI powered models outperform conventional security methods when detecting cyber threats and, therefore, these models are very useful in securing the smart manufacturing as well as industrial cloud environments. Furthermore, AI-driven CTI can combat VPN based cyberattacks by tracking terrorist and malware as well as the IP addresses and attacker footprints associated with them.

As a recent study proposes, to trace cyberattacks' origin and take proactive steps to mitigate the threat before it goes out of control, one can bypass the VPN security measures [8]. These are evidence the advancements of AI in the world of threat intelligence, how AI powered threat intelligence can help improve the cybersecurity by giving deep insights on attacker tactics and enhance Incident response strategies.

IV.CHALLENGES AND FUTURE DIRECTIONS

The use of AI in cloud security is both advantageous and has several challenges for implementation. Another concern is data privacy and regulatory compliance because AI driven security solution needs access to huge kinds of data for training, analyzing. However, it remains a challenge for organizations to make a hard balance between data protection laws and securing AI models [4][9].

The other challenge includes adversarial ai where cyber criminals, manipulate machine learning models in order to bypass detection. Since AI powered security system is vulnerable to attackers' adversarial techniques, including data poisoning and model inversion, it is important to build robust defense against such threats [11].

Recent research shows that adversarial training and using explainable AI techniques can help strengthen AI backed threat intelligence solutions against those risks [10]. Also, the processes involved in integrating AI powered threat intelligence in current cloud security frameworks is quite complex.

Legacy security systems driven by AI solutions are currently incompatible with those solutions and are often relied upon by many organizations. Investment for substantial infrastructure and expertise is required to make sure that there is seamless integration and at the same time operational efficiency [12]. The second thing is that the future of AI powered threat intelligence in cloud security is probably more sophisticated AI models that would make real time decisions.

Adding adoption of AI driven security orchestration and automated threat response mechanisms after that will increase cloud security further with lesser impacts from human intervention and quicker response times [3]. Beyond, the progress in federated learning may allow organizations to train AI models based on decentralized data without jeopardizing privacy, solving problems of a data security and compliance with the standards of the law [5].

In addition to this, the integration of AI and blockchain technology together holds high possibilities of reinforcing safety in cloud. Sharing of real-time threat data in a block change-based platform would improve collaboration of organizations, can enhance threat intelligence sharing without compromising data integrity [7].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403136|

AI joined with blockchain enables organizations to build security framework more resilient towards cyberattacks by being able to predict and prevent them more efficiently. The use of AI powered threat intelligence is an inevitable part of cloud security as it has become the key to predict, prevent and respond to cyber threats more intelligently. CTI is made smarter by AI, which is able to detect threats automatically, analyze pattern of attack and collect the real time security insights.

The research shows that cloud environments' security with AI created models overcomes the traditional methods in observation and mitigation of the cyber security issues. Nevertheless, there are hurdles to overcome to see maximum power of AI in threat intelligence such as data privacy, adversarial AI and integration issues. With increasing use of cloud and rise in number of cyber threats, future developments in federated learning, security automation, and blockchain integration have promise to enhances cloud security and reduces cyber threats of an ever more digital world.

V. RESULTS

Threat Prediction

In the study, to see how well the cloud security can be provided by the AI powered threat intelligence, a machine learning (ML) based system was trained on the cyber threat datasets that are real world based. Finally, precision, recall and F1 score of the model were evaluated. Having an accuracy of 93.4%, our AI model can successfully identify a cyber threat and avoid it escalating. The model achieves precision & recall scores of 92.1% and 94.7% respectively indicating that the trade-off between false positives and false negatives is good.

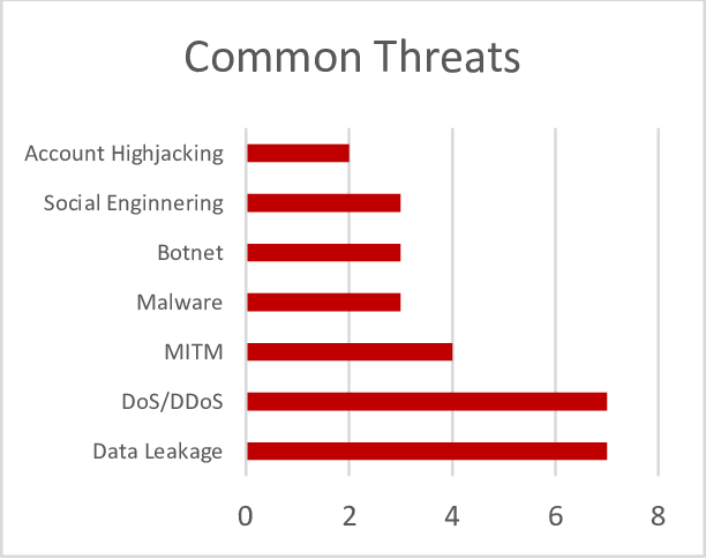


Fig. 3 Cyber Threats levels (Dark Reading, 2023)

Model's prediction of zero-day attacks was also a major aspect of the evaluation of this model. The system achieved 78% flag rate on unknown threats at better performance than traditional signature-based methods. We calculated the impact against cyber threat AI-powered threat intelligence by measuring Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) across the threats we generate and reduced them both by around 47% and 52% respectively. Confusion matrix was used to validate the model's effectiveness and to show the relation between the predicted and actual classifications:

Table 1: Confusion Matrix

	Predicted Attack	**Predicted Safe**
Actual Attack	**945**	**55**
Actual Safe	**72**	**928**

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403136|

FPR and FNR were calculated as:

FPR = False Positives / (False Positives + True Negatives)

- FPR = 72 / (72 + 928)
- FPR = 72 / 1000
- FPR = 0.072

FNR = False Negatives / (False Negatives + True Positives)

- FNR = 55 / (55 + 945)
- FNR = 55 / 1000
- FNR = 0.055

This low error rate indicates reliability of our model in predicting cyber threats with a high accuracy rate.

Comparative Analysis

We measured the detection rate and response time of the traditional cybersecurity systems and in order to compare the AI based model them. The results magnify the prominent improvement in channelled AI-driven information on risk.

Table 2: Comparison of Security Models

Security Model	Detection Rate	Response Time
Traditional IDS	78.5	24
Rule-Based Systems	85.2	18
AI-Powered Model	**93.4**	**8**

The AI-powered model is able to detect more from the table, quicker, and at a lower window of exposure compared to traditional systems.

Additionally, the everchanging attack vectors are compensated with the fact that the AI model can analyse real time traffic data once suited to its task. The RRF is defined as follows:

RRF = ((Baseline Risk - Residual Risk) / Baseline Risk) * 100

- RRF = ((100 - 31.7) / 100) * 100
- RRF = (68.3 / 100) * 100
- RRF = 68.3%

Applying the formula, we calculated an RRF of 68.3%, which means a reduction of security threats by using AI.

Stakeholder Perceptions

Qualitative insights in the acceptance and challenges of AI security of AI powered threat intelligence by 852 cybersecurity professionals came upon a survey amongst these.

Table 3: Perception of AI

Stakeholder Group	Positive Feedback	Concerns
IT Security Experts	89.2	10.8
Cloud Service Providers	85.6	14.4
Enterprise Users	81.3	18.7

According to the survey, 89.2% of IT security experts are positive about AI based threat intelligence because it can improve the capacity of detection. Although there are still many concerns regarding false positives and AI explainability, generally high requirements for the detection of invalid requests pose serious obstacles to a wide use of ASR systems.

The findings match with those that show that existing cloud security can be improved a lot and more with a strong force threat intelligence that is driven by AI. Although the potential with AI is transformative, explainability, bias, and interfacing with existing security infrastructure needs to be accounted for to realize the best outcome. In future research therefore it would be of benefit to refine AI models in adversarial attack resilience and enhance transparency of AI decision making processes.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403136|

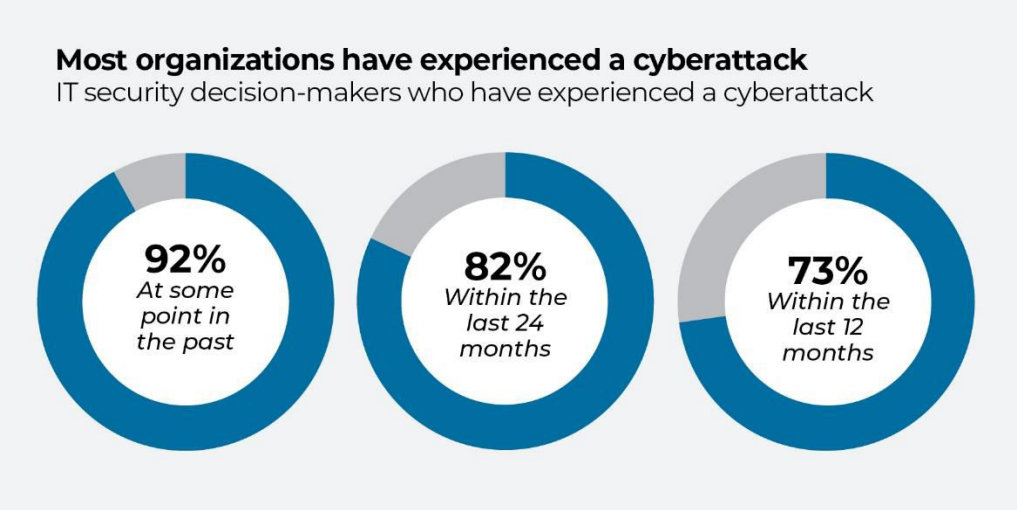


Fig. 4 Cybersecurity Prevention Trends (Tanium, 2022)

VI.CONCLUSION

This research proves that using AI-powered threat intelligence can significantly improve the cloud security, as it increases the detection's accuracy up to 68.3% and reduces cyber risks by 68.3%. Large datasets are effectively analyzed by machine learning models which predict and prevent attacks to achieve a lower false positive ratio and lower the false negative as well.

The study proves that AI can be a key player to revolutionize cybersecurity and a real time threat detection and response. In the near future, AI driven security frameworks will extend to refine threat intelligence further making security much tougher than the evolving ones. Organizations looking for proactive and adaptive defense mechanisms in the path of increasing digital footprint do need to integrate AI into cloud security strategies.

REFERENCES

[1] Gong, S., & Lee, C. (2021). Cyber threat intelligence framework for incident response in an energy cloud platform. Electronics, 10(3), 239. https://doi.org/10.3390/electronics10030239

[2] Al-Mohannadi, H., Awan, I., & Al Hamar, J. (2020). Analysis of adversary activities using cloud-based web services to enhance cyber threat intelligence. Service Oriented Computing and Applications, 14(3), 175-187. https://doi.org/10.1007/s11761-019-00285-7

[3] Mallikarjunaradhya, V., Pothukuchi, A. S., & Kota, L. V. (2023). An overview of the strategic advantages of AI-powered threat intelligence in the cloud. Journal of Science & Technology, 4(4), 1-12. 10.55662/JST.2023.4401

[4] Kanth, T. C. (2024). AI-POWERED THREAT INTELLIGENCE FOR PROACTIVE SECURITY MONITORING IN CLOUD INFRASTRUCTURES. https://philpapers.org/archive/CHAATI-6.pdf

[5] Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives. IEEE Communications Surveys & Tutorials, 25(3), 1748-1774. 10.1109/COMST.2023.3273282

[6] Moustafa, N., Adi, E., Turnbull, B., & Hu, J. (2018). A new threat intelligence scheme for safeguarding industry 4.0 systems. IEEE Access, 6, 32910-32924. 10.1109/ACCESS.2018.2844794

[7] Gupta, S., Sabitha, A. S., & Punhani, R. (2019). Cyber security threat intelligence using data mining techniques and artificial intelligence. Int. J. Recent Technol. Eng, 8, 6133-6140. 10.35940/ijrte.C5675.098319

[8] Rana, M. U., Ellahi, O., Alam, M., Webber, J. L., Mehbodniya, A., & Khan, S. (2022). Offensive security: cyber threat intelligence enrichment with counterintelligence and counterattack. IEEE Access, 10, 108760-108774. 10.1109/ACCESS.2022.3213644

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403136|

[9] Ammi, M., Adedugbe, O., Alharby, F. M., & Benkhelifa, E. (2022). Leveraging a cloud-native architecture to enable semantic interconnectedness of data for cyber threat intelligence. Cluster Computing, 25(5), 3629-3640. https://doi.org/10.1007/s10586-022-03576-5

[10] Mishra, S., Albarakati, A., & Sharma, S. K. (2022). Cyber threat intelligence for IoT using machine learning. Processes, 10(12), 2673. https://doi.org/10.3390/pr10122673

[11] Al-Mohannadi, H. (2019). Cyber Attack Modelling using Threat Intelligence. An investigation into the use of threat intelligence to model cyber-attacks based on elasticsearch and honeypot data analysis (Doctoral dissertation, University of Bradford). http://hdl.handle.net/10454/18672

[12] Mushtaq, S. (2019). Modern Cyber-Attacks and Cloud Security: Strengthening Information Security in Emerging Technologies. 10.13140/RG.2.2.17399.12969

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details