INJ INTERNATIONAL NEUROUROLOGY JOURNAL

# Enhancing Cloud Security With Ai-Driven Big Data Analytics

**Anjan Kumar Reddy Ayyadapu**
anjanreddy8686@gmail.com

## Abstract

This broad review investigated the perplexing field of AI performance in the security region, including threat order models and cloud security models. Curiously, in the domain of cloud security, our exploration uncovered areas of strength for a connection between the size of the training dataset and the model's performance from there on. Besides, notwithstanding the way that dataset variety significantly affected performance, a remarkable example was noticed: greater datasets would in general show less assortment. Directing our concentration toward threat order, our exploration uncovered the unmistakable benefits of various AI models. Specifically, Brain Organizations ended up being very viable at perceiving Phishing threats, while Choice Trees ended up being extremely compelling at recognizing Malware. Our consciousness of the extensive variety of AI applications in security settings is improved by this detailed comprehension of model viability across different security concerns.

**Keywords:** Cloud Security, Threat Classification, AI Performance, Dataset Correlation.

## Introduction

A collection of computers that work together to perform various calculations and operations is referred to as a cloud. One of the most significant IT trends of the last several years is cloud computing. Reduced time and expenses on the market is one of the main advantages that this IT technology offers to the businesses. Companies and organizations may now employ pooled computer and storage resources thanks to cloud computing. It is preferable than creating and using your own infrastructure. Additionally, cloud computing offers businesses and organizations an affordable, safe, and adaptable IT infrastructure. It is comparable to the national electricity networks that let families and businesses to connect to an economical, efficient, and centrally controlled energy supply. Prominent companies that have made investments in cloud computing include Google, Amazon, Cisco, IBM, Sun, Dell, Intel, HP, Oracle, and Novell. They also provide a variety of cloud-based products to people and organizations.

Regarding the many services offered, cloud computing comes in a variety of forms and models. Thus, cloud computing encompasses communal, hybrid, private, and public clouds. In contrast, three categories might be used to group service delivery models: SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). Two categories are often used to categorize cloud computing: geographic location and service offerings. Depending on where the cloud is located, cloud computing can be categorized as either public (where the cloud vendor hosts the computing infrastructure), private (where the organization owns the computing infrastructure and does not share it with others), hybrid (using both public and private clouds), or community (sharing IT infrastructure amongst organizations within the same community). Clouds are categorized in the following ways if the basis for categorization is the kind of services that are offered: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Almost every computer system in use today uses cloud computing, a cutting-edge technique for electronically processing and transporting data. It operates on a network architecture that is vulnerable to many kinds of intrusions. Distributed Denial of Service, or DDoS, is one of the most well-known forms of assault. Distributed Denial of Service attacks may be prevented by using syn cookies and limiting the number of users connected to the server using cloud technologies.

A different kind of assault against cloud computing infrastructure is known as a man-in-the-middle attack. Security measures like Secure Socket Layer (SSL) may thwart this sort of assault. Therefore, improper configuration of this security strategy may result in compromised client and server authentication, which might leave cloud technology users vulnerable to man-in-the-middle attacks. Therefore, while using cloud computing, security concerns related to data protection must be carefully addressed and avoided. Our software runs on hard drives and CPUs that are not in front of us when we use cloud computing. Because of this, consumers who utilize this technology are becoming more apprehensive about security concerns. Thus, a wide variety of assaults might be made using cloud technologies. In addition to the previously listed, the majority of known attacks include traffic analysis, IP ports, phishing, IP spoofing, message alteration, and so forth. The cloud



ISSN:2093-4777 | E-ISSN:2093-6931
**DOI**: 10.5123/inj.2023.4.in182
Vol. 27 Iss. 4 (2023)

computing companies accept a wide range of security measures for data protection, all of which include access control, authorization, secrecy, and authentication.

The term "Internet of Things" (IoT) refers to a network of intelligent devices that exchange and gather data. By 2020, there will be over thirteen billion linked devices, and by 2025, there will be seventeen billion. Every hour, trillions of data will be produced by it. The internet is available on devices other than computers and cellphones for a number of years now. Almost anything can now be connected to the internet. There is no limit to the Internet of Things. Businesses run a variety of communication networks for this purpose. Big Data is required to manage such vast amounts of data. Massive and enormous data collections are referred to as "big data." Thus, big data may be used to handle the enormous amounts of data that the authors collected from IoT devices and other sources. Since 2012, the term "big data" has been used more broadly to describe the reality that businesses are dealing with larger amounts of data that need to be processed, which raises significant challenges for marketing and business. Cloud computing has emerged to handle the scalability and fast increase in volume, centralization, and infrastructure.

**Research Objectives**

- To look at the connection between the highlights of the training datasets (like size and variety) and the viability of AI models utilized in cloud security).
- To evaluate how well AI-driven models recognize and arrange security takes a chance regarding precision and proficiency.

## Literature Review

Ness, S., Rangaraju, S., and Dharmalingam, R. (2023). In order to improve cloud security, this research examines how artificial intelligence (AI) strategies can be integrated into the DevSecOps framework. It does this by utilizing an analytical technique and combining quantitative and qualitative methodologies to evaluate the effectiveness of AI solutions in reducing security risks. This research adds to our understanding of the complex link between AI and DevSecOps, illuminating the ways in which merging these two technologies might enhance security. The study also examines the consequences and difficulties of integrating AI into DevSecOps processes, taking into account variables like interpretability, flexibility, and scalability.

Kota, L. V., Pothukuchi, A. S., and Mallik arjun aradhya, V. (2023). In the age of digital transformation, cloud adoption has come to be associated with scalability and agility in business. But this change has also brought in a new set of security risks, calling for cutting-edge defenses. Emerging as a ray of hope, artificial intelligence (AI) offers automated, predictive, and adaptive security solutions. With the increase in cyberattacks, cloud security is more important than ever. AI can significantly enhance cloud security. From the perspective of product leaders, this research explores the prospects, problems, and substantial impact of AI on cloud security. This research provides insights into the critical role that product managers will play in determining the direction of cloud security via an in-depth examination of market dynamics, subtleties in product development, and strategic concerns.

Tyagi, A. K., Mishra, A. K., Hemamalini, V., and Kakulapati, V. (2024). This study suggests an architecture that integrates blockchain, IoT, and AI in a cloud-based setting. The suggested architecture offers a dependable and safe platform for data analysis and interchange, facilitating the creation of intelligent applications that raise productivity, efficiency, and standard of living. IoT sensors, AI algorithms, and blockchain technology—which guarantee data security and privacy, immutability, and transparency—are the fundamental elements of the design. Applications for the suggested architecture include smart cities, logistics, and healthcare. In closing, this chapter offers an overview of the advantages and difficulties of integrating blockchain, IoT, and AI. It also suggests a unique design that may take use of these technologies to raise the security and efficiency of cloud-based settings. This study will go into great depth on upcoming technologies and their roles in related sectors.

I. Keshta (2022) The goal of a wiser society has lately been accurately depicted thanks to the Internet of Things (IoT), which offers a wide range of services and copious amounts of data. Health care communities, business, government, and academia are paying close attention to "smart health care" due to the development of smart Multiple Sensorial Media (MulSeMedia) systems, the cloud, and things technologies. The current study aims to identify security and privacy concerns related to AI-driven Internet of Things (AIIoT) and provide recommendations on how these problems might be effectively resolved. The research used an existing, relevant secondary source to gather qualitative data as part of a qualitative study design. The data from the research demonstrates that the development of AI-driven IoT (AIIoT) has increased the quantity of new sensors and gadgets connected to the internet, raising a variety of security and privacy issues among users. According to the



ISSN:2093-4777 | E-ISSN:2093-6931
**DOI**: 10.5123/inj.2023.4.in182
Vol. 27 Iss. 4 (2023)

report, certain well-defined architectural standards, such as data models and interfaces that guarantee improved user security and privacy, should be mandatory for the AI-driven Internet of Things (AIIoT).

Run fang Zhou; Hwang, Kai (2006) A novel method for trustworthy grid computing in a peer-to-peer (P2P) environment is presented in this study. For peers to build enduring professional relationships, trust and security are prerequisites. Peer trust scores are gathered using a P2P reputation system, which then combines them to provide a worldwide reputation. To represent the trust connections among the peers, we use a novel trust overlay network (TON). Upon examination of the eBay transaction trace data, we find that user feedback follows a power-law distribution. In order to take use of power-law feedback features, we create a new reputation system called Power Trust. Locality-preserving hash functions and a lookahead random walk technique are used in the construction of the Power Trust system. Power nodes with a solid reputation are used to facilitate dynamic system reconfiguration.

Zev Winkelman, Daniel Gonzales, Jeremy Kaplan, Evan Saltzman, and Dulani Woods (2015) Government and business are very concerned about the vulnerability of Cloud Computing Systems (CCSs) to Advanced Persistent Threats (APTs). We introduce a reference model for cloud architecture that integrates various security controls and best practices. Additionally, we present Cloud-Trust, a cloud security assessment model that estimates high-level security metrics to measure the level of confidentiality and integrity provided by a cloud computing service provider (CCS) or cloud service provider (CSP).

In 2015, Massimo Ficco and Massimiliano Rak the on-demand, self-service, pay-per-use feature of the cloud computing paradigm is largely responsible for its popularity. This paradigm states that the consequences of Denial of Service (DoS) assaults affect both the cost of resource consumption for service maintenance and the quality of the service that is provided. To be more precise, the expenses involved will increase with the length of the detection delay. That being said, covert DoS assaults need special consideration. While they seek to reduce their visibility, they may be just as dangerous as brute-force assaults.

## Research Methodology

This study analysed how well AI-driven models acted in cloud security and threat order. The accompanying classifications give an outline of the past tense methodology utilized:

### Research Design

To investigate the field of cybersecurity, two different exploration projects were begun. The objective of the principal research, "Cloud Security AI Model Assessment," was to assess and differentiate the viability of a few cloud security AI models. Performance scores, assortment, and the size of the training dataset were totally remembered for the evaluation models. The review's information came from publically open sources, and distinct insights and relationship investigations were utilized to look at the outcomes cautiously.

In the subsequent exploration, "Security Threat Classification and Model Assessment," the assessment of numerous man-made brainpower models — Choice Tree, Brain Organization, and Naive Bayes — came into center. The viability of these models in distinguishing three unique kinds of security threats — malware, phishing, and unapproved access — was surveyed. This evaluation was directed utilizing genuine world datasets, and performance measures including exactness, accuracy, and F1 score were processed to decide how well each model tended to the featured security issues.

### Data Collection

Item sites and exploration papers were among the openly available web sources from which information for the evaluation of the cloud security AI model was purposefully gathered. Information on the size, assortment, and performance scores of the training dataset were additionally recorded. As to security threat order study, dependable scholarly foundations and freely available archives gave named datasets true occurrences of malware, phishing, and unapproved access. These exceptional techniques for social affair information made it conceivable to completely assess the performance of a few AI models corresponding to cloud security and security threat order.

### Ethical Considerations

The review approach was intensely impacted by moral issues, with a specific spotlight on safeguarding the secrecy and security of information. Just de-distinguished, freely available information was utilized in the examinations, and legitimate credit was given to the first information sources, all with regards to moral guidelines. Delicate information was painstakingly kept away from to forestall any potential impacts on private

protection and security from the review results, which were painstakingly thought of. This moral structure guaranteed that the review's impact remained inside moral limits and featured the specialists' obligation to undertaking a mindful and conscious examination of cloud security AI models and security threat classification.

**Statistical Analysis**

The exploration included careful measurable examination procedures altered to meet the remarkable objectives of each and every examination. Engaging measurements were utilized in the evaluation of the cloud security AI model to give a compact outline of the data assembled on the size, assortment, and performance scores of the training dataset. Thus, an intensive outline of the concentrated-on AI models was conceivable. Relationship examination was additionally used to inspect the associations between these significant factors, giving data about any potential conditions or patterns. One more measurable technique was utilized in the security threat arrangement examination. Every AI model's performance pointers, like exactness, accuracy, and F1 score, were deliberately resolved utilizing the testing datasets that compared to it. These measurements give a mathematical assessment of each model's performance in accurately sorting the given security concerns, extraordinarily upgrading the general review results.

## Data Analysis

**Table 1: AI Security Model Metrics.**

| Cloud Security AI Model | Training Dataset Size (GB) | Training Dataset Diversity (%) | Performance Score (0-100) |
|---|---|---|---|
| Cyber Guard Pro | 50 | 75 | 85 |
| SentinelAI Secure Net | 100 | 50 | 92 |
| Deep Defender Cloud Shield | 75 | 90 | 78 |
| Guardian Sense AI | 120 | 60 | 89 |
| Threat Watch Analytics | 80 | 80 | 80 |
| Secure Mind Cloud Sentry | 60 | 70 | 88 |
| Risk IQ Guardian | 90 | 85 | 76 |
| SafeNet Insight AI | 110 | 45 | 94 |
| CogniShield Security | 70 | 65 | 82 |
| Vigilant Eye Cloud Defender | 95 | 75 | 87 |

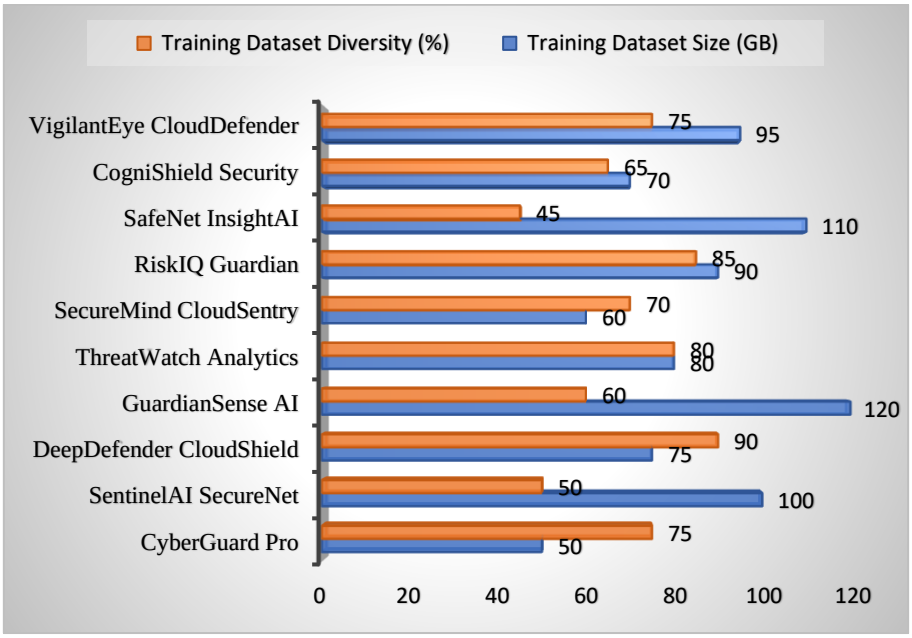


**Figure 1: Training Dataset Size (GB) and Training Dataset Diversity (%) of selected Cloud Security AI Model**



DOI: 10.5123/inj.2023.4.in182
ISSN:2093-4777 | E-ISSN:2093-6931
Vol. 27 Iss. 4 (2023)

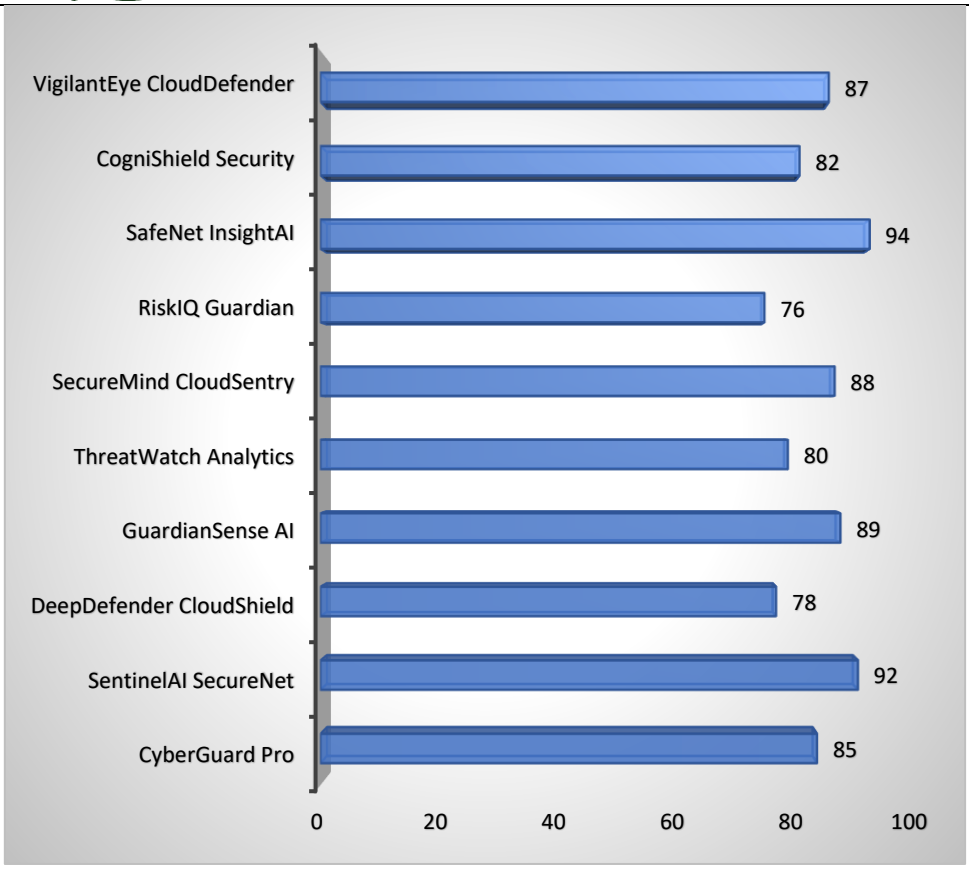


**Figure 2: Performance score of selected AI Models**

A few cloud security AI models are given valuable measurements in Table 1. Among the vital passages is the "SafeNet Understanding AI" model, which has a variety level of 45% and a major training dataset size of 110 GB. With a noteworthy elite performance score of 94, this model obviously shows its adequacy in cloud security. On the other hand, the "Hazard intelligence level Watchman" model accomplishes a performance score of 76 with a greater training dataset size of 90 GB and a 85% variety rate.

**Table 2: Correlation between AI Security Model Metrics**

| | Training Dataset Size | Training Dataset Diversity | Performance Score |
|---|---|---|---|
| Training Dataset Size | 1 | -0.36 | 0.75 |
| Training Dataset Diversity | -0.36 | 1 | 0.07 |
| Performance Score | 0.75 | 0.07 | 1 |

Inside Table 2, There were remarkable associations between significant elements, as indicated by the factual investigation of the cloud security AI model evaluation. Initial, a critical positive relationship of 0.75 was viewed as between the "Training Dataset Size" and the "Performance Score," proposing that better performance scores are frequently corresponded with bigger training datasets. What's more, there was a barely regrettable connection found (- 0.36) between the "training dataset variety" and the "training dataset size," demonstrating that there might be a propensity for greater datasets to have less assortment. At long last, there was next to no sign of an immediate relationship between the assortment of training datasets and the performance scores that were obtained, with simply a tiny positive connection of 0.07 arising between the "Training Dataset Variety" and the "Performance Score." These outcomes give sagacious data about the collaborations between the different elements in the evaluated cloud security AI models.

**Performance Evaluation Of Ai-Driven Models In Security Threat Classification**

**Table 3: Security Threat Classification and Model Evaluation**

| Threat Type | Model Type | Training Dataset | Testing Dataset | Accuracy | Precision | F1 Score |
|---|---|---|---|---|---|---|



DOI: 10.5123/inj.2023.4.in182
ISSN:2093-4777 | E-ISSN:2093-6931
Vol. 27 Iss. 4 (2023)

| | | Size | Size | | | |
|---|---|---|---|---|---|---|
| Malware | Decision Tree | 10,000 | 2,000 | 0.93 | 0.9 | 0.83 |
| Phishing | Neural Network | 15,000 | 3,000 | 0.96 | 0.96 | 0.89 |
| Unauthorized Access | Naive Bayes | 8,000 | 1,500 | 0.95 | 0.96 | 0.89 |
| Malware | Neural Network | 12,000 | 2,500 | 0.92 | 0.93 | 0.8 |
| Phishing | Decision Tree | 18,000 | 3,500 | 0.94 | 0.92 | 0.85 |

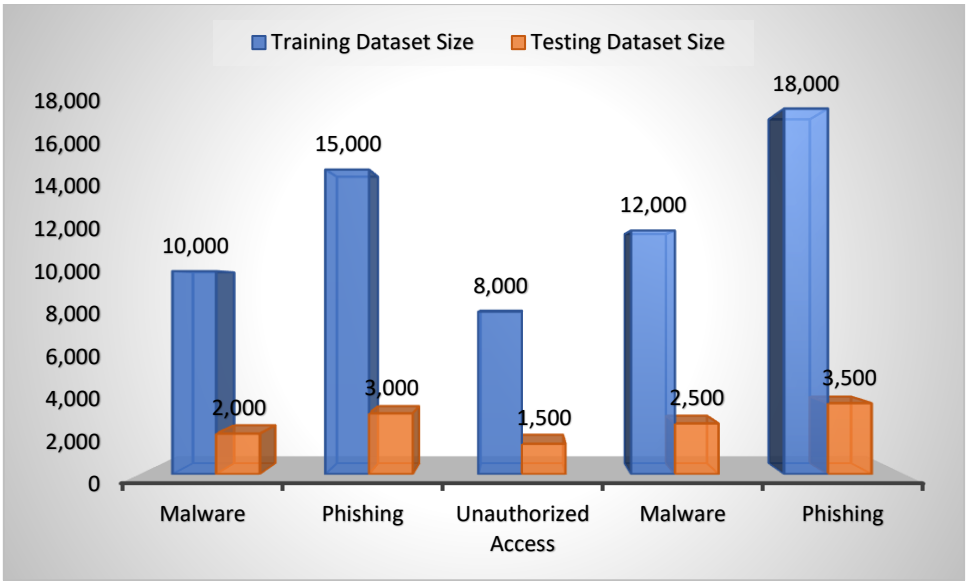


**Figure 3: Training and Testing Dataset size for selected Threat Type**

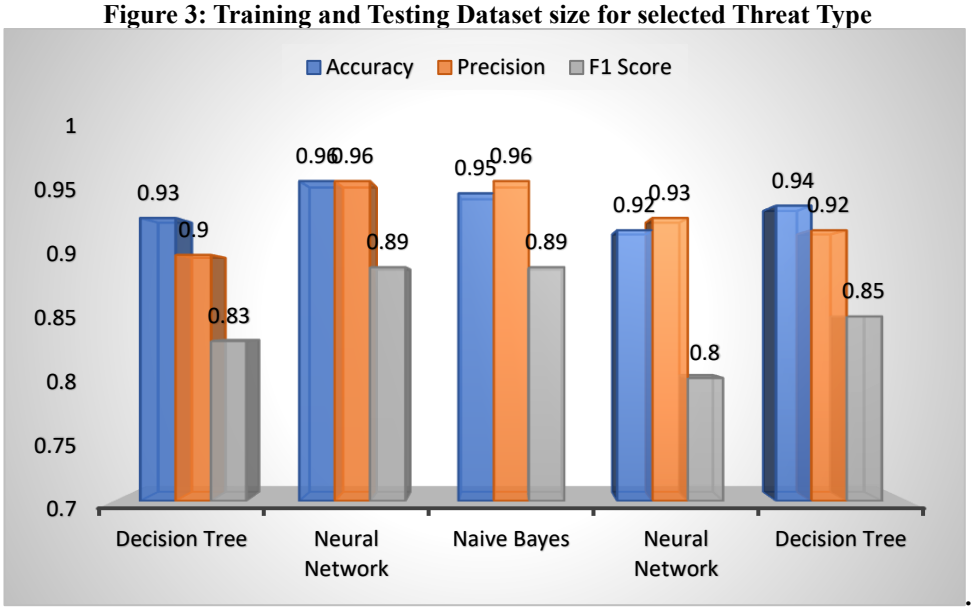


**Figure 4: Accuracy, Precision and F1 Score for selected Model type**

A synopsis of the evaluation discoveries for the few AI-driven models used to characterize security threats is displayed in Table 3. For instance, in view of a training dataset size of 10,000 and a testing dataset size of 2,000, the Choice Tree model used to recognize malware obtained an exactness of 0.93, accuracy of 0.90, and a F1 Score of 0.83. Essentially, by utilizing a greater training dataset of 15,000 and a testing dataset of 3,000, the Brain Organization model used for Phishing threat recognizable proof showed noteworthy performance with an exactness of 0.96, accuracy of 0.96, and a F1 Score of 0.89. With 8,000 training and 1,500 testing datasets, the Naive Bayes model delivered results for Unapproved Access discovery that showed exactness of 0.95, accuracy of 0.96, and a F1 Score of 0.89.

## Conclusion

A lot of data on the viability of AI security models was uncovered by this examination. By and large, greater training datasets are related with further developed performance; notwithstanding, assortment has a less critical impact. Various models performed very well when it came to threat classification. Brain Organizations for Phishing, Choice Trees for Malware, and Naive Bayes for Unapproved Access were the triumphant models. For greatest insurance against specific risks, our outcomes highlight the need of choosing models and training information that are explicitly adjusted to the circumstance.

## References


1. Alnafessah, A. (2022). Artificial intelligence driven anomaly detection for big data systems.
2. Burak Kantarci ; Hussein T. Mouftah, 2016, ―Multiagent/multiobjective interaction game system for service provisioning in vehicular cloud‖, ISSN: 2169-3536, volume 04, pp 3153-3168
3. Gill, S. S., Xu, M., Ottaviani, C., Patros, P., Bahsoon, R., Shaghaghi, A., ... & Uhlig, S. (2022). AI for next generation computing: Emerging trends and future directions. Internet of Things, 19, 100514.
4. Hemamalini, V., Mishra, A. K., Tyagi, A. K., & Kakulapati, V. (2024). Artificial Intelligence–Blockchain-Enabled–Internet of Things-Based Cloud Applications for Next-Generation Society. Automated Secure Computing for Next-Generation Systems, 65-82.
5. Jagatheesaperumal, S. K., Rahouti, M., Ahmad, K., Al-Fuqaha, A., & Guizani, M. (2021). The duo of artificial intelligence and big data for industry 4.0: Applications, techniques, challenges, and future research directions. IEEE Internet of Things Journal, 9(15), 12861-12885.
6. Keshta, I. (2022). AI-driven IoT for smart health care: Security and privacy issues. Informatics in Medicine Unlocked, 30, 100903.
7. Ma, Z., Kim, S., Martínez-Gómez, P., Taghia, J., Song, Y. Z., & Gao, H. (2020). IEEE access special section editorial: AI-driven big data processing: Theory, methodology, and applications. IEEE Access, 8, 199882-199898.
8. 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.
9. Massimo Ficco ; Massimiliano Rak, 2015, ―Stealthy Denial of Service Strategy in Cloud Computing‖, ISSN: 2168-7161, volume 03, issue 01, pp 80-94.
10. Nassar, A., & Kamal, M. (2021). Ethical dilemmas in AI-powered decision-making: a deep dive into big data-driven ethical considerations. International Journal of Responsible Artificial Intelligence, 11(8), 1-11.
11. Rangaraju, S. (2023). Secure by Intelligence: Enhancing Products with AI-Driven Security Measures. EPH-International Journal of Science And Engineering, 9(3), 36-41.
12. Rangaraju, S., Ness, S., & Dharmalingam, R. (2023). Incorporating AI-Driven Strategies in DevSecOps for Robust Cloud Security. International Journal of Innovative Science and Research Technology, 8(23592365), 10-5281.
13. Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2, 1-18.
14. Saxena, D., Gupta, I., Gupta, R., Singh, A. K., & Wen, X. (2023). An AI-driven VM threat prediction model for multi-risks analysis-based cloud cybersecurity. IEEE Transactions on Systems, Man, and Cybernetics: Systems.
15. Seokcheon Lee; Soundar Kumara; Natarajan Gautam, 2008, ―Market-Based Model Predictive Control for Large-Scale Information Networks: Completion Time and Value of Solution‖,ISSN: 1558-3783 volume 5, issue 4, pp:630-640.