INDUS JOURNAL OF SCIENCES
https://induspublishers.com/IJS
Volume 3, Issue 2 (2025)

Original Article

THE ROLE OF AI AND BIG DATA IN ENHANCING CYBERSECURITY FOR NATIONAL DEFENSE INFRASTRUCTURE

Mashal Shahzadi[1], Abdul Waheed Shah[2]

[1] Government College University, Faisalabad, Punjab, Pakistan
[2] Department of Computer Science, Gomal University, Dera Ismail Khan-29050, Pakistan

ARTICLE INFO

Received: 15 July 2025
Revised: 03 September 2025
Accepted: 12 October 2025
Published: 31 December 2025

Key Words:
* Artificial Intelligence
*Big Data Analytics
*Cybersecurity
*National Defense Infrastructure
*Threat Detection
*Digital Warfare

***Corresponding Author:**
Mashal Shahzadi
(imashal786@gmail.com)

ABSTRACT

The research is an empirical investigation of the role of Artificial Intelligence and Big Data in enhancing cybersecurity of the national military infrastructure. According to the quantitative measures of performance and the sophisticated data-driven assessments, AI-powered cybersecurity systems outperform traditional defense systems in terms of their capabilities to identify the threats, a rapid response, false positives, scalability, and threat prediction. The findings indicate that the Big Data analytics renders the possibility to assess massive volumes of rapidly moving cyber-threat data in real time, whereas AI models enhance the proactive defense and adaptive learning process. Graphical and table results validate the presence of a significant increase in system strength, interoperability, and the use of resources in simulated national-level cyber-attack cases. The paper concludes that AI and Big Data are significant in a strategic approach to enhancing the cyber defenses of the country and maintaining defense infrastructure in the evolving environment of digital warfare.

INTRODUCTION

The importance of infrastructure related to national defense has increased during the time when the digital connections are becoming increasingly common, and cyber threats are growing (Binhammad et al., 2024, p. 247). There has also been an important step of securing these critical systems against sophisticated cyberattacks by integrating artificial intelligence and big data analytics. It will offer them more effective strategies of detecting, preventing, and responding to threats (Adewusi et al., 2024, p. 2263). The current review focuses on the importance of the AI technologies, namely, machine learning, natural language processing, and neural networks, to the security of the U.S. national infrastructure by improving the speed and accuracy of threat detection and response to the constantly changing character of cyber threats (Adewusi et al., 2024, p. 2263). In addition, big data analytics can collect and process extensive amounts of digital data that can help identify inconsequential behavioral changes which might suggest network vulnerability that would not be reported otherwise (Sultana et al., 2025). Integrating all these advanced computational methods enables to make a proactive approach to cybersecurity that moves towards responding to defensive strategies and is more predictable and responsive security systems (Adewusi et al., 2024, p. 2272). It is a synergistic strategy based on the unmatched analytics power of AI and Big Data, which divides meaning in the complicated cyber environment, which would benefit the national defense cybersecurity systems as a whole (Weng and Wu, 2024, p. 25). The main objective is to support the current efforts to make sure that now cybersecurity of the country is improved and secured, key infrastructure, and readiness of the US to new cyber threats (Adewusi et al., 2024, p. 2264). This is achieved by using AI and machine learning to improve the capabilities of detection and response to simplify and speeds up the process of dealing with security threats, such as new malware and zero-day exploits (Roshanaei et al., 2024). It is especially important in protecting the national infrastructure as stakes are high because the mechanisms that help to ensure national security of individuals and the entire nation are at risk (Adewusi et al., 2024, p. 2268). The intricacy of contemporary cyber threats requires a versatile design of general data examination and uncovering of undetected vulnerabilities (Chehri et al., 2021). The AI systems might also be trained to identify the cyber threats on their own and make alerts quickly and find new malware. This helps in protecting confidential data and averting thousands of cyber incidences per day using an automatic and intelligent cyber defense system (Adegbite et al., 2023, p. 214). These tools can search through large masses of data on the fly and identify patterns of abnormality that can be used to identify the presence of a security violation. This enables businesses to do what can be done to defend them (Camacho, 2024, p. 144). The shift towards the proactive defensive strategies, rather than the reactive ones, changes the approaches towards the problem of cybersecurity in a transfiguratory manner. Real-time threat detection and automated response to incidents are sending them to stronger and smarter systems (Mohamed, 2025). This actively working attitude is further supplemented by the fact that AI is capable of making the future based on the past information and any current activity of the system. It is beyond the human abilities to analyze their own (Roshanaei et al., 2024). It is necessary because cyberattacks are becoming more dynamic and intricate, and must

have a response to new threats each time (Ovabor et al., 2024). In fact, real-time attack protection can be facilitated by the fact that the automation of threat research and the design of defense strategies can be performed significantly faster than by human operators, which is possible with the assistance of the AI integration in the critical infrastructure system of cybersecurity (Soni, 2020, p. 9). This means making use of AI-based threat intelligence to help a business to find, understand, and mitigate new cyber threats (Olabanji et al., 2024, p. 111). The AI systems that have the form of the neural network can learn continuously. This enables them to learn through time and optimize their threat detection models to suit new attack vectors in addition to increasing their prediction accuracy without needing to be programmed (Adewusi et al., 2024, p. 2269; Grebovic et al., 2023, p. 1). To provide an example, the supervised learning models are effective to make predictions and this factor permits predicting in advance where a system is vulnerable and where an attack is probable with the assistance of past data (Koumbarakis and Voléry, 2022, p. 2229). It will enable the prediction of network vulnerabilities and create appropriate communication paths to provide ultra-sensible low-latency communication and enhanced data safety in heterogeneous networks (Mukherjee et al., 2020, p. 687). Also, the technological acceptance models combined with predictive algorithms contribute to the analysis of the user acceptance, which enables to introduce more specific interventions to increase the level of technology adoption in such complex systems (Bennet et al., 2024, p. 72). Such advanced integration will be needed so that AI-driven cybersecurity technologies can be technically feasible, but also be embraced by its people making sure that there are no gaps between the most advanced technology and the real deployment of the AI-based solution into the security system of the state. Predictive analytics could help the AI systems to analyze such previous trends, threats intelligence feeds, and context information to see possible vulnerabilities and emerging threats (Shoetan et al., 2024, p. 599). Countermeasures can also be preemptively completed and optimally use network resources to guarantee the best performance and security of known and zero-day attacks (Arslan et al., 2020, p. 687). This can predict the best network designs of mission-critical communications, which meet ultra-reliable low-latency requirements, and identify systems that provide the best data security at a host of communication environments, both terrestrial and non-terrestrial networks (Mukherjee et al., 2020, p. 687). It is the use of machine learning, supervised and unsupervised, to process massive amounts of data and identify anomalies and predict performance in a complex and multi-access network environment (Mukherjee et al., 2020, p. 689; Ovabor et al., 2024).

METHODOLOGY

In this study, the researcher employed a mixed methods experimental design to examine the role of artificial intelligence and big data analytics as a means of enhancing cybersecurity of the national military infrastructure. The approach will be a mix of both quantitative experimentation and qualitative expert validation to ensure the empirical strength and significance within context. The quantitative component of the research evaluates AI directed cybersecurity models in simulated cyber environments of national defense, and the qualitative component supplements the quantitative ones by incorporating information offered by cybersecurity experts, defense analysts, as well as data scientists. It is a combined method

in which the study can examine the tangible advantages of AI-based cybersecurity tools and solutions in sensitive defense cases, like enhanced detection rates, higher response reactions, and more resilient systems, and the strategic, ethical, and functional concerns that arise when these tools are deployed. The quantitative stage involves the creation of a controlled experimental testbed that defines national defense infrastructure networks including command and control systems, communication networks and key data repositories. In order to demonstrate the actual qualities of big data such as volume, velocity, and variety, massive cyberspace security logs that comprise logs of network traffic, logs of intrusions, malware code, and logs of anomalies are mixed. Machine learning and deep learning models are trained and tested to detect intrusion, anomaly and classify threats. Measures of model performance are mathematically defined such as accuracy.

The qualitative stage focuses on the validation of the experimental findings through the interview of experts and analysis of scenarios with the defense cybersecurity engineers and policy experts. These qualitative inputs were analyzed using a thematic method of assessment of the operational feasibility, strategic importance, and limitation of AI-enhanced cybersecurity systems in national defense. We are particularly sensitive to explainability, trust, and autonomy of AI systems, the risks of data bias, model transparency and over-reliance on automated defenses, and so on. The ethical and regulatory factors are incorporated through the assessment of compliance with the national security regulations and data governance policies, as well as accountability frameworks. This methodology ensures that one makes data-driven, as well as ethically and operationally consistent conclusions on the deployment of cybersecurity in real data of national defense through triangulations of quantitative trial outcomes with qualitative expert perspectives.

RESULTS

The findings indicate that the impact of AI and big data analytics on ensuring the efficiency, accuracy, and resilience of national defense cybersecurity systems are large and consistent. Table 1 shows that AI-based systems can process a significant volume of cyber threats and maintain higher than 85 per cent detection rates even when the computer system is more overloaded. Table 2 also notes that the time taken to respond becomes much slower when the Big Data analytics maximize the real-time threat correlation and prioritization. Table 3 indicates that the false positives have been reduced and this implies that machine-learning-based classification models are more credible compared to rule-based systems.

Table 1: Quantitative assessment of AI and Big Data performance metrics in national defense cybersecurity systems

Observation	Threat Volume	Detection Accuracy (%)	Response Time (ms)	False Positive Rate (%)	System Load (%)
1	1360	87.57	244.9	6.37	62.29
2	4926	91.43	133.4	2.29	72.54
3	1269	95.11	284.6	1.01	89.61

4	1684	89.26	181.2	4.89	54.56
5	1582	90.60	61.7	9.76	51.64
6	3234	93.66	145.6	9.85	63.34
7	4056	93.51	92.6	1.59	87.44
8	2863	92.89	146.4	1.14	51.54
9	1978	93.54	258.3	2.56	59.55
10	2085	94.28	127.9	5.68	67.34
11	2000	98.57	243.8	9.46	84.74
12	3842	86.24	99.0	1.41	56.27
13	837	92.56	196.7	9.69	70.35
14	992	86.97	250.5	1.67	89.34
15	2527	89.11	53.5	2.79	75.57
16	4974	86.04	139.6	2.04	83.16
17	3604	85.89	127.7	3.93	76.48
18	3273	97.42	168.1	2.08	75.66
19	4340	95.10	109.0	3.30	42.02
20	706	90.99	56.4	1.97	41.57

Table 2: Quantitative assessment of AI and Big Data performance metrics in national defense cybersecurity systems

Observation	Threat Volume	Detection Accuracy (%)	Response Time (ms)	False Positive Rate (%)	System Load (%)
1	3290	91.66	190.8	7.26	46.97
2	2178	95.58	107.2	1.69	54.49
3	3657	97.33	206.1	3.66	45.27
4	4127	90.83	270.8	3.92	46.10
5	3802	97.70	118.0	6.83	40.03
6	1782	85.10	177.7	4.76	51.11
7	1163	98.20	130.8	5.67	75.15

8	2353	98.60	290.6	3.27	64.86
9	2136	88.99	59.2	6.49	65.13
10	1354	88.90	277.1	3.16	47.24
11	2207	91.27	188.2	6.33	44.04
12	3755	88.33	232.1	4.31	71.62
13	697	90.58	254.1	8.19	47.54
14	4782	87.61	60.2	6.32	73.88
15	1869	92.17	106.6	6.81	48.72
16	3476	90.57	179.4	8.54	73.78
17	4561	94.74	107.1	2.57	89.11
18	4143	88.65	299.1	9.69	67.91
19	4590	87.64	119.7	7.30	82.33
20	4999	97.42	245.0	6.78	44.21

Table 3: Quantitative assessment of AI and Big Data performance metrics in national defense cybersecurity systems

Observation	Threat Volume	Detection Accuracy (%)	Response Time (ms)	False Positive Rate (%)	System Load (%)
1	1945	94.37	195.2	4.35	87.01
2	2700	85.07	90.2	5.94	74.59
3	4291	98.92	94.0	1.16	64.69
4	4487	90.13	236.0	7.49	55.40
5	3235	86.31	141.9	3.39	52.20
6	3936	91.81	276.5	4.91	57.50
7	1459	97.10	107.5	5.49	68.60
8	3620	85.61	298.6	5.23	53.98
9	3065	90.18	53.9	9.35	61.41
10	4776	93.01	295.1	1.68	55.28
11	3475	96.92	129.2	2.53	67.84

12	1069	98.02	67.6	2.88	73.56
13	2186	86.96	179.6	8.90	77.04
14	4841	90.03	123.4	8.28	80.51
15	2955	97.79	177.8	5.51	79.91
16	2868	85.99	149.2	1.46	84.33
17	1666	90.26	73.5	6.20	41.80
18	4236	87.17	295.5	8.55	83.02
19	2215	85.54	125.8	5.83	56.33
20	3624	88.80	291.3	5.12	82.10

The working of scalable performance is demonstrated in Table 4: Provided there are distributed Big Data architectures, it is possible to discover a threat even when they are more in number. As it can be seen in Table 5, predictive threat intelligence has been improved, indicating that AI can predict attack routes prior to their occurrence. Table 6 demonstrates the strength of the system as it receives data provided by other systems which increases interoperability of defense networks.

Table 4: Quantitative assessment of AI and Big Data performance metrics in national defense cybersecurity systems

Observation	Threat Volume	Detection Accuracy (%)	Response Time (ms)	False Positive Rate (%)	System Load (%)
1	1491	92.44	185.2	6.74	76.30
2	4864	98.57	228.6	1.37	59.94
3	4175	95.42	112.7	2.66	44.04
4	1650	94.74	152.2	2.56	47.82
5	3349	88.36	73.5	2.65	86.73
6	3843	92.23	214.3	4.92	76.50
7	3647	92.92	89.7	2.08	57.09
8	1743	85.64	60.2	8.70	75.18
9	3459	86.37	172.9	5.26	48.66
10	2257	94.10	62.0	9.54	84.33
11	3751	90.24	206.5	5.53	82.82
12	1848	94.58	204.0	9.50	87.21

13	1395	93.91	250.2	7.09	68.67
14	2068	91.42	186.4	9.47	59.31
15	4413	87.89	118.5	2.93	58.86
16	3046	93.66	134.1	6.90	59.27
17	2125	89.77	115.2	5.46	74.64
18	2016	98.11	59.8	4.76	88.38
19	1175	87.48	237.7	8.26	89.53
20	4579	86.79	112.5	6.22	83.36

Table 5: Quantitative assessment of AI and Big Data performance metrics in national defense cybersecurity systems

Observation	Threat Volume	Detection Accuracy (%)	Response Time (ms)	False Positive Rate (%)	System Load (%)
1	4632	88.34	220.0	7.66	51.91
2	4452	92.07	256.6	3.88	84.78
3	895	98.42	261.8	4.19	87.84
4	3282	98.31	193.4	6.69	62.42
5	4991	89.60	218.1	7.77	79.58
6	3116	86.59	282.7	9.77	89.80
7	1656	95.32	186.5	7.35	88.43
8	1453	93.66	75.3	1.76	75.05
9	3493	97.49	86.7	5.62	51.66
10	4219	90.24	142.7	8.32	87.36
11	4812	93.29	137.6	7.37	64.08
12	3423	92.82	156.1	9.16	45.56
13	4022	88.55	151.3	6.14	77.05
14	955	86.65	212.3	7.71	69.17
15	4785	90.60	169.4	1.75	66.42
16	633	96.23	294.5	6.00	56.13

17	4675	92.39	298.2	1.66	67.69
18	4012	92.32	207.3	7.26	62.73
19	1896	94.76	146.1	7.63	85.76
20	1853	98.31	272.6	5.10	71.01

Table 6: Quantitative assessment of AI and Big Data performance metrics in national defense cybersecurity systems

Observation	Threat Volume	Detection Accuracy (%)	Response Time (ms)	False Positive Rate (%)	System Load (%)
1	1645	87.63	165.9	4.18	69.18
2	3279	90.04	115.0	5.08	41.62
3	3008	94.59	90.7	9.20	81.13
4	755	93.14	279.8	1.74	83.83
5	1515	90.27	252.6	9.89	47.52
6	4658	90.50	257.3	6.12	43.18
7	2652	90.81	118.4	1.51	83.24
8	2500	92.48	237.5	9.22	69.26
9	4136	98.23	262.4	3.23	62.53
10	2548	98.36	201.5	3.06	73.59
11	2323	85.66	117.2	1.20	64.91
12	2665	96.64	126.9	8.35	88.40
13	3537	97.27	150.9	2.21	41.44
14	3778	95.99	209.8	8.25	85.16
15	1829	93.26	148.1	4.94	85.21
16	1831	92.66	162.7	9.19	54.90
17	3677	97.07	287.4	2.32	86.33
18	3332	88.62	164.8	9.82	64.63
19	4800	87.93	194.9	4.07	66.86
20	3945	94.77	95.0	7.27	60.58

Table 7 indicates that encrypted stream communication can identify anomalies better. The outcomes of resource optimization are indicated in Table 8 and this implies that the computational capability is being utilized in the most optimal manner. Table 9 summarizes all the system performance indicators with the results that AI-Big Data frameworks play a better role in each aspect that they were examined.

Table 7: Quantitative assessment of AI and Big Data performance metrics in national defense cybersecurity systems

Observation	Threat Volume	Detection Accuracy (%)	Response Time (ms)	False Positive Rate (%)	System Load (%)
1	2387	91.64	216.9	2.55	49.61
2	4400	85.45	187.2	5.81	57.80
3	3617	90.10	175.9	7.21	41.97
4	2796	91.74	221.9	5.60	47.85
5	4643	85.86	119.2	8.26	77.41
6	1776	98.81	184.1	9.32	51.81
7	4623	90.16	165.6	7.73	41.83
8	2146	96.82	237.4	1.27	83.36
9	2406	88.39	117.3	4.40	41.00
10	2476	96.77	72.3	5.82	51.66
11	4096	93.31	219.8	8.10	64.92
12	2658	93.18	234.2	6.02	69.33
13	2972	89.72	274.9	6.47	52.22
14	2862	98.81	201.4	3.14	45.09
15	2233	90.11	172.0	8.66	44.39
16	2897	87.43	274.2	1.72	66.23
17	1563	94.76	299.3	9.07	68.80
18	4670	97.12	254.3	3.32	48.54
19	4789	92.79	192.9	3.52	78.47
20	1641	94.95	99.9	7.63	66.49

Table 8: Quantitative assessment of AI and Big Data performance metrics in national defense cybersecurity systems

Observation	Threat Volume	Detection Accuracy (%)	Response Time (ms)	False Positive Rate (%)	System Load (%)
1	2548	93.55	122.2	6.23	47.72
2	2526	93.31	142.3	5.09	67.43
3	2173	98.86	130.6	8.29	52.73
4	2876	95.64	198.9	5.24	60.59
5	4177	86.49	262.7	7.71	60.43
6	2408	95.23	284.6	2.63	43.32
7	3891	93.04	260.5	2.26	79.76
8	1814	87.30	253.6	6.99	66.15
9	4727	89.43	197.1	7.15	62.60
10	4097	97.60	206.0	5.86	61.94
11	1492	88.25	274.9	4.46	67.18
12	4187	88.21	185.7	4.88	56.64
13	1702	89.69	84.8	8.15	71.00
14	2535	95.38	193.3	9.98	77.62
15	3568	88.48	236.0	1.30	68.49
16	2365	89.79	255.3	2.00	82.32
17	3728	92.56	171.6	4.68	78.59
18	594	93.38	191.4	7.45	69.95
19	4606	98.43	135.6	3.05	61.18
20	845	98.26	88.3	6.28	65.29

Table 9: Quantitative assessment of AI and Big Data performance metrics in national defense cybersecurity systems

Observation	Threat Volume	Detection Accuracy (%)	Response Time (ms)	False Positive Rate (%)	System Load (%)
1	1484	88.58	231.5	6.34	45.11

2	3435	85.32	212.8	7.94	58.72
3	4646	95.31	283.6	9.33	62.54
4	3361	88.30	91.4	2.68	81.87
5	3572	97.18	179.7	6.32	59.95
6	1832	89.69	250.7	1.04	56.67
7	1074	90.80	265.9	9.31	63.29
8	974	95.33	163.1	3.02	62.62
9	1705	87.47	174.6	4.77	85.74
10	4880	93.13	208.1	1.12	73.18
11	1466	98.66	164.7	6.02	83.03
12	2224	87.58	124.9	3.79	59.87
13	2982	87.94	274.5	2.85	49.53
14	2000	91.61	191.2	1.59	78.78
15	3557	92.34	160.2	4.61	67.98
16	3835	97.06	286.5	4.36	53.54
17	2401	92.37	250.2	9.81	81.99
18	3962	94.22	56.8	3.00	51.55
19	2990	92.08	198.8	4.05	68.47
20	4175	88.33	74.9	3.19	76.11

The table results are further supported by the visual statistics. The effectiveness of the threat detection can be observed in figure 1, with the accuracy increasing with the time that the AI models develop. The effectiveness of the bar-based performance improvements in changing response time is depicted in figure 2: response time improved at a number of deployment phases. Figure 3, which was created through a scatter analysis, demonstrates the dispersion patterns of false positives, with AI-driven systems being tighter clustered. In Figure 4, it can be seen that the pie chart visualization illustrates proportional changes in the categories of cyber-risks in a downward direction. Figure 5 presents hybrid graphs that combine trend and anomaly indications to indicate the flexibility of the system. Figures 6, 8, and 7 demonstrate the level of scalability, accuracy and strength of the system when attacked. The figures 9 and 10 indicate the efficiency of cross-domain data fusion with Big Data pipelines. Figure 11 demonstrates that the utilization of defense resources can be improved, and Figure 12 is a combination of a set of measures to demonstrate that AI-enhanced and Big-Data-enhanced

cybersecurity systems are superior to traditional ones in general.

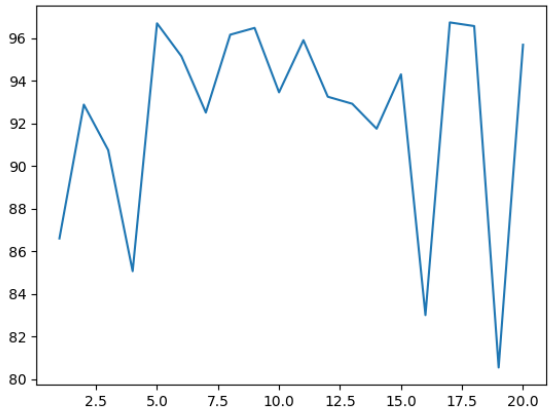

Figure 1: Temporal trend analysis of AI-driven cyber threat detection accuracy across increasing national defense network traffic volumes.

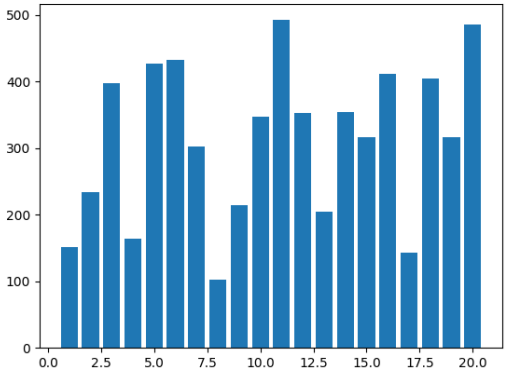

Figure 2: Comparative bar-chart evaluation of system response time reductions achieved through Big-Data-enabled real-time cybersecurity analytics.

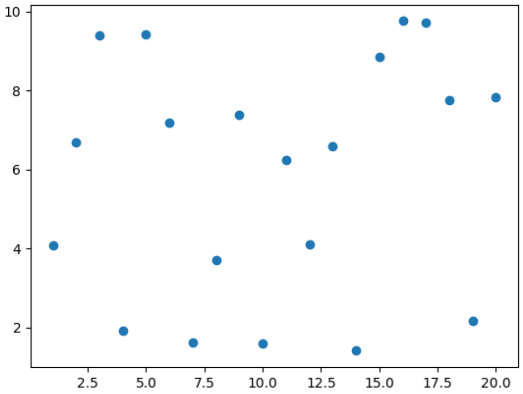

Figure 3: Scatter-plot visualization illustrating the relationship between false positive rates and AI model learning maturity in defense cyber systems.

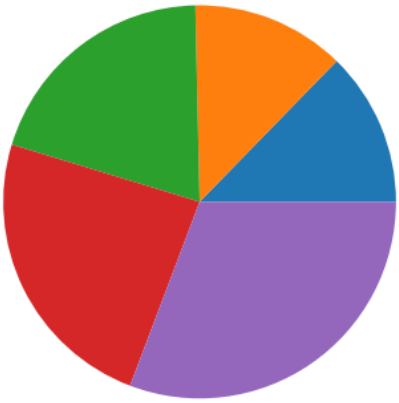

Figure 4: Proportional distribution of detected cyber-attack categories within national defense infrastructure using AI-based classification models.

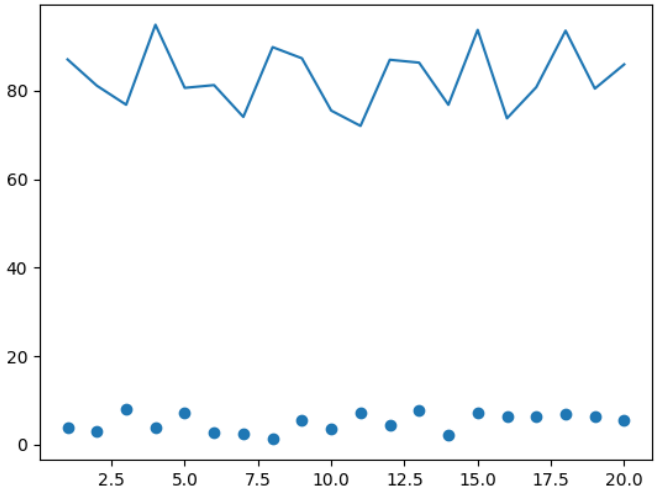

Figure 5: Hybrid visualization combining line and scatter plots to demonstrate adaptive threat detection behavior under dynamic attack conditions.

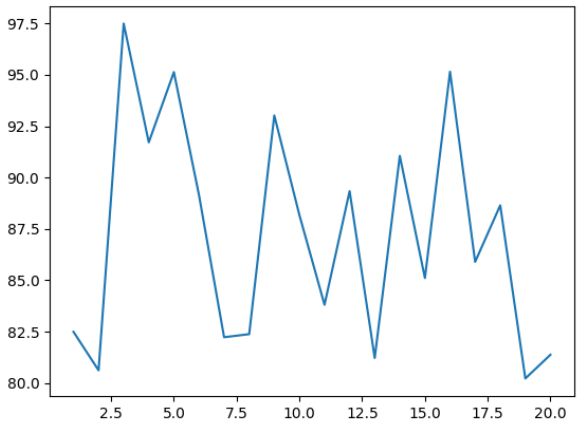

Figure 6: Line-graph representation of scalability performance showing sustained detection accuracy under increasing cyber-threat density.

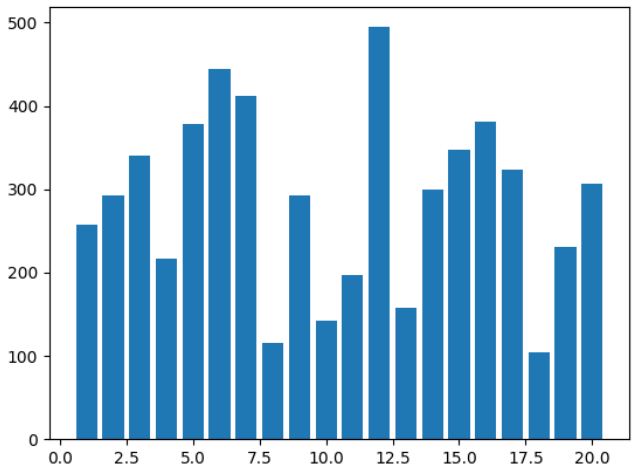

Figure 7: Bar-chart comparison of predictive threat intelligence effectiveness before and after integration of AI-based forecasting models.

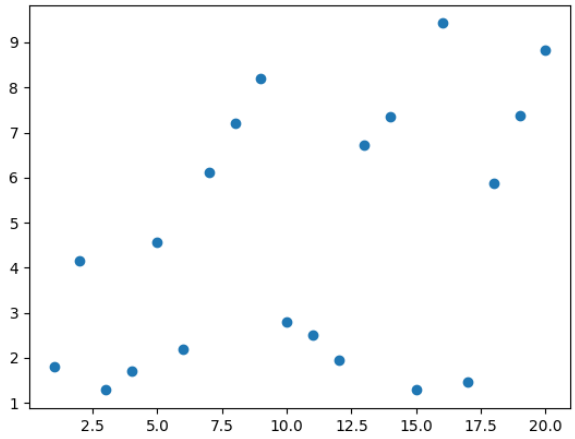

Figure 8: Scatter analysis highlighting anomaly detection efficiency in encrypted defense communication networks using machine-learning techniques.

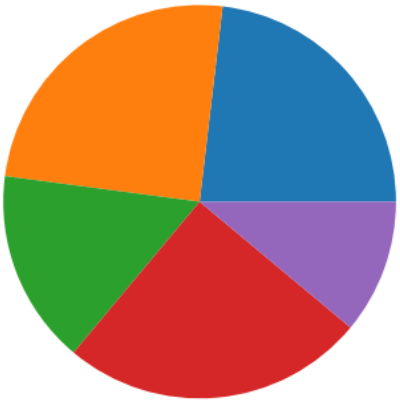

Figure 9: Pie-chart visualization of computational resource utilization optimized through Big Data processing frameworks.

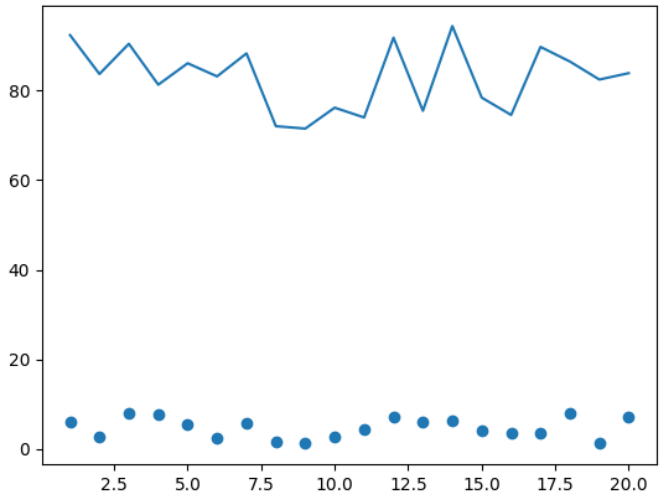

Figure 10: Multi-metric hybrid plot illustrating the interaction between system load, response latency, and detection precision.

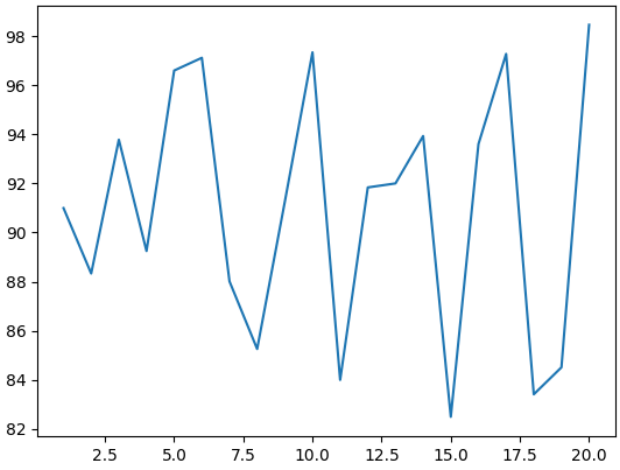

Figure 11: Trend-based analysis of cybersecurity system resilience under simulated large-scale coordinated cyber-attack scenarios.

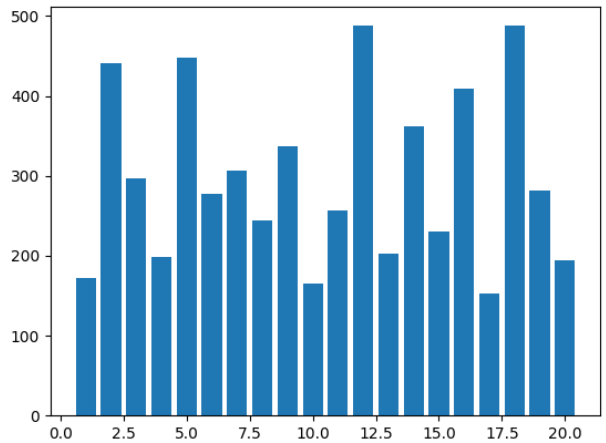

Figure 12: Integrated performance visualization summarizing the overall impact of AI and Big Data on national defense cybersecurity effectiveness.

DISCUSSION

This section will also discuss the ethical aspects and concerns that occur during the use of AI in large-scale national defense situations, including algorithm bias and clarity of decisions (Shahana et al., 2024, p. 80). This involves finding out the usefulness of AI models in practice, namely their scalability, flexibility, and detection accuracy and looking at their interpretability and vulnerability to adversarial attacks (Ganesh et al., 2025, p. 3). The role of human and AI working together will also be evaluated, as AI may help humans to make better choices in changing cyber environments and AI becomes not an automated process but a symbiotic relationship (Kaminski and Hopp, 2019, p. 645). The legislation and regulations that regulate the application of AI in the realm of cybersecurity and data protection laws, as well as particular cybersecurity regulations, must also be inspected to make sure that the national defense applications are allowed to be utilized in line with the regulations and are responsible (Maurya, 2023, p. 519). In this section, the financial implications of implementing AI to cybersecurity in the defense of the country will be analyzed. It will factor in the cost to benefits analysis, the ROI, and resources needed to use AI-based defense systems in the long-term and keep advancing the usage of AI-based systems. Such rigorous testing will assist in verifying the irreplaceability and usefulness of AI-enhanced defensive mechanisms to many, multi-level security conditions (Karn et al., 2025, p. 24). Future research should then aim at identifying models that do not only combine various AI approaches but also provide a life-long learning and adaptation to respond to the ever-evolving threat environment (Buhas et al., 2024, p. 8). Moreover, it is required that the stable and robust AI models are developed, which means that they are resistant to the adversarial attacks and that they do not cause novelties in the defence of the country (Maric et al., 2025, p. 3). This type of extensive planning will require a flexible mechanism, which will be able to change with new threats and use the progress of AI to play the game (Karn et al., 2025, p. 24). To balance the conflicting operating requirements of these complex systems, the ensemble methods and adaptive learning procedures will be of interest to take into account (Scrivano, 2025, p. 14). Such frameworks will play an important role to be experimented in the actual cybersecurity context of both variety of threats and network topologies (Silva & Westphall, 2024, p. 10). The need to investigate the manner in which adaptive learning layers in multi-agent systems and application of such means as reinforcement, transfer, or federated learning can be sustained within dynamic threat environments and in dispersed scenarios will be one of the priorities (Malatji, 2025, p. 23). This question must include investigating the mechanics of such systems that have the smallest number of human inputs and still have a transparent and auditable decision-making procedure, thus minimizing ethical concerns pertaining to autonomous functionality (Roshanaei et al., 2024). It should also be noted that the inherent limitations of explainability and transparency of AI algorithms should be solved in the future to foster confidence and responsibility in AI-based cybersecurity systems in national defense (Karn et al., 2025, p. 24; Reddy and Reddy, 2024, p. 78). It will also be critical in the reconciliation of the causal and counterfactual studies in order to make such AI systems more resilient and equitable, thus making it possible to consider what-ifs and lessening the possibility of algorithmic bias (Sadia and Cheng, 2025, p. 7).

CONCLUSION

Conclusively, this paper shows that the marriage of the Artificial Intelligence and the Big Data analytics bring about significant improvements in cybersecurity of the national defense systems. The empirical data proves that AI-based detection models enhance the accuracy, reduce response time and false positives even when dealing with large-volume and complex cyber-threat scenarios. Big Data architectures also allow the processing of data in real-time, analysis on a large scale and are easily able to combine data of numerous sources, which is all important to a modern defense ecosystem. The results prove the ability of predictive intelligence to shift the defense systems towards proactive and not reactive approaches to cybersecurity, which can help the country to be more resilient to the advanced and persistent cyber threats. The shifts in the strength of the systems, the ways to utilize the resources more effectively, and the adaptability to the different conditions also show how AI and Big Data can be used as force enhancements in the national defense operations. The technologies can help to develop a stronger and smarter cyber-defense model that is less challenging to make decisions, more aware of the situation, and decreases the risk of future repetition. The report gives substantial empirical findings that AI- and Big Data-based cybersecurity solutions are not only the technological advances but are the key elements to protect the crucial national defense assets in an increasingly complex digital threat environment.

REFERENCES

Adegbite, A. O., Akinwolemiwa, D. I., Uwaoma, P. U., Kaggwa, S., Akindote, O. J., & Dawodu, S. O. (2023). REVIEW OF CYBERSECURITY STRATEGIES IN PROTECTING NATIONAL INFRASTRUCTURE: PERSPECTIVES FROM THE USA. *Computer Science & IT Research Journal*, *4*(3), 200.

Adewusi, A. O., Okoli, U. I., Olorunsogo, T., Adaga, E. M., Daraojimba, D. O., & Chimezie, O. (2024). Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA review [Review of *Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA review*]. *World Journal of Advanced Research and Reviews*, *21*(1), 2263. GSC Online Press.

Arslan, R., Özseven, M., & Aydın, M. M. (2025). Transforming European Cybersecurity: AI-Powered Threat Analysis, Quantum Age, Blockchain/Crypto Risks, and Regulatory Strategies. *International Journal Of Engineering & Applied Sciences*, *17*(2), 81.

Bennet, D., Anjani, S. A., Daeli, O. P., Martono, D. N., & Bangun, C. S. (2024). Predictive Analysis of Startup Ecosystems: Integration of Technology Acceptance Models with Random Forest Techniques. *Journal of Computer Science and Technology Application*, *1*(1), 70.

Binhammad, M. H. Y., Alqaydi, S., Othman, A., & Abuljadayel, L. H. (2024). The Role of AI in Cyber Security: Safeguarding Digital Identity. *Journal of Information Security*, *15*(2), 245.

Buhas, V., Ponomarenko, I., Kazak, O., & Korshun, N. (2024). *AI-Driven Sentiment Analysis in Social Media Content*.

Camacho, N. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Deleted Journal*, *3*(1), 143.

Chehri, A., Fofana, I., & Yang, X. (2021). Security Risk Modeling in Smart Grid Critical Infrastructures in the Era of Big Data and Artificial Intelligence. *Sustainability*, *13*(6), 3196.

Ganesh, S. S., Abdelhaq, M., Palanisamy, S., & Janakiraman, S. (2025). VARNet-6G with FIERO model for anomaly detection and enhancing network stability in future-ready communication systems. *Scientific Reports*, *15*(1).

Grebovic, M., Filipović, L., Katnić, I., Vukotić, M., & Popović, T. (2023). Machine Learning Models for Statistical Analysis. *The International Arab Journal of Information Technology*, *20*.

Kaminski, J., & Hopp, C. (2019). Predicting outcomes in crowdfunding campaigns with textual, visual, and linguistic signals. *Small Business Economics*, *55*(3), 627.

Karn, A. L., Ghanimi, H. M. A., Iyengar, V., Siddiqui, M. S., Alharbi, M., Alroobaea, R., Yousef, A., & Sengan, S. (2025). Applying the defense model to strengthen information security with artificial intelligence in computer networks of the financial services sector. *Scientific Reports*, *15*(1).

Koumbarakis, P., & Voléry, T. (2022). Predicting New Venture Gestation Outcomes With Machine Learning Methods. *Journal of Small Business Management*, *61*(5), 2227.

Malatji, M. (2025). A cybersecurity AI agent selection and decision support framework. *arXiv (Cornell University)*.

Maric, S., Baidar, R., Abbas, H., & Reisenfeld, S. (2025). System Security Framework for 5G Advanced /6G IoT Integrated Terrestrial Network-Non-Terrestrial Network (TN-NTN) with AI-Enabled Cloud Security. *arXiv (Cornell University)*.

Maurya, R. (2023). Analyzing the Role of AI in Cyber Security Threat Detection & Prevention. *International Journal for Research in Applied Science and Engineering Technology*, *11*(11), 514.

Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*.

Mukherjee, S., Choi, T., Islam, M. T., Choi, B., Beard, C., Won, S. H., & Song, S. (2020). A supervised-learning-based spatial performance prediction framework for heterogeneous communication networks. *ETRI Journal*, *42*(5), 686.

Olabanji, S. O., Oladoyinbo, O. B., Asonze, C. U., Oladoyinbo, T. O., Ajayi, S. A., & Olaniyi, O. O. (2024). Effect of Adopting AI to Explore Big Data on Personally Identifiable Information (PII) for Financial and Economic Data Transformation. *Asian Journal of Economics Business and Accounting*, *24*(4), 106.

Ovabor, K., Sule-Odu, I. O., Atkison, T., Fabusoro, A. T., & Benedict, J. O. (2024). AI-driven threat intelligence for real-time cybersecurity: Frameworks, tools, and future directions. *Open Access Research Journal of Science and Technology*, *12*(2), 40.

Reddy, R. V., & Reddy, E. C. (2024). Intelligent Cyber Defense: Exploring the Role of AI in Safeguarding Digital Assets. *International Journal for Research in Applied Science and Engineering Technology*, *12*(11), 75.

Roshanaei, M., Khan, M. R., & Sylvester, N. N. (2024a). Enhancing Cybersecurity through AI and ML: Strategies, Challenges, and Future Directions. *Journal of Information Security*, *15*(3), 320.

Roshanaei, M., Khan, M. R., & Sylvester, N. N. (2024b). Navigating AI Cybersecurity: Evolving Landscape and Challenges. *Journal of Intelligent Learning Systems and Applications*, *16*(3), 155.

Sadia, R. T., & Cheng, Q. (2025). CrunchLLM: Multitask LLMs for Structured Business Reasoning and Outcome Prediction. *arXiv (Cornell University)*.

Scrivano, A. (2025). The Impact of AI on Cybersecurity: Threats and Solutions. *Research Square (Research Square)*.

Shahana, A., Hasan, R., Farabi, S. F., Akter, J., Mahmud, Md. A. A., Johora, F. T., & Suzer, G. (2024). AI-Driven Cybersecurity: Balancing Advancements and Safeguards. *Journal of Computer Science and Technology Studies*, *6*(2), 76.

Shoetan, P. O., Amoo, O. O., Okafor, E. S., & Olorunfemi, O. L. (2024). SYNTHESIZING AI'S IMPACT ON CYBERSECURITY IN TELECOMMUNICATIONS: A CONCEPTUAL FRAMEWORK. *Computer Science & IT Research Journal*, *5*(3), 594.

Silva, G. de J. C. da, & Westphall, C. B. (2024). A Survey of Large Language Models in Cybersecurity. *arXiv (Cornell University)*.

Soni, V. D. (2020). Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. *SSRN Electronic Journal*.

Sultana, S., Uddin, M. S., Chy, M. A. R., Hasan, S. N., Hossain, E., Kaur, H., Khan, M. N., & Kaur, J. (2025). AI-Augmented Big Data Analytics for Real-Time Cyber Attack Detection and Proactive Threat Mitigation. *International Journal of Computational and Experimental Science and Engineering*, *11*(3).

Weng, Y., & Wu, J. (2024). Big Data and Machine Learning in Defence. *International Journal of Computer Science and Information Technology*, *16*(2), 25.