Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 3, 2026

ENHANCING CYBER SECURITY AND NETWORK RESILIENCE IN MODERN DATA CENTERS: QUESTIONNAIRE BASED RESEARCH

[1*]Muhammad Zeeshan, [2]Syed Muhammad Sajjad, [3]Talha Naeem Qureshi
[1]*Riphah International University Islamabad*
[2]*National Cyber security Academy, Air University Islamabad*
[3]*COMSATS University Islamabad*

DOI: https://doi.org/10.5281/zenodo.19414273

Keywords Cybersecurity, Network Resilience, Intelligent monitoring systems, machine learning, data centres, Relative Importance Index (RII), analytic hierarchy processes (AHP), Cronbachs Alpha, Anomaly Detection, Automated Incident Response.

Article History
Received on 01 Jan 2026
Accepted on 2 feb 2026
Published on 04 March 2026

Corresponding Author: * Muhammad Zeeshan

Abstract

The rapid speed of the current data center evolution has substantially enhanced the risk of cybersecurity and exerted the necessity to deploy complex solutions that will provide the network with endurance and competency to the transformed cybercrime. In the framework of the current paper, the authors will comment on how to improve cybersecurity and network resiliency in the contemporary data centers through the use of intelligent monitoring infrastructure. The questionnaire survey was constructed and 50 survey questionnaires interviewed that included cybersecurity professionals, IT professionals and data center practitioners. The important factors obtained were ranked in a Relative Importance Index (RII) and the Analytic Hierarchy Process (AHP) was used to estimate the weight of importance of the items as well as Cronbach Alpha was used to estimate the reliability of the questionnaire. The findings show that Machine Learning Capability (RII = 0.89; AHP weight = 0.34) and then Telemetry Quality and Incident Response Automation are the most relevant. Anomaly detection and real-time monitoring may be seen as the most important of all the sub-factors of effective cybersecurity systems. The AHP consistency test allowed proving that all the pair-wise comparisons were stable (CR less than 0.10) and the test of reliability showed that the overall internal consistency of the data was high (the total Cronbachs Alpha = 0.87). The findings suggest that the traditional modalities of delivering the security are surely becoming the AI-driven, automated and data-driven based surveillance systems that can significantly contribute to the improved efficiency of the threat detection, the effectiveness and the performance of the response, and the stability of the system. The researchers and practitioners can find the paper helpful since it has pointed significant areas of concern that can be refined in order to enhance cybersecurity in the data centers and give valuable recommendations on how to establish intelligent monitoring systems.

INTRODUCTION

The digital infrastructure includes a highly dependent use of modern data centers that have the capacity to drive cloud computing and big data analytics, artificial intelligence, and enterprise applications. With the increase in data sent, the network of networked systems, cybersecurity and network resilience issues are increasingly becoming urgent issues to organizations everywhere across the world. Cyberattacks proliferation in the data center sector, such as distributed denial-of-service (DDoS), ransomware, insider attacks, and advanced persistent attacks (APTs) is on the increase due to the high values of the assets and the concentrated operations within the data centers [1].

The existing cyber attacks are becoming very sophisticated, and their security mechanisms like historical data center security systems and projecting devices like firewalls and signature-based intrusion detection systems are no longer sufficient to address the complexity. The classical techniques are not effective at detecting zero-day attacks and adaptive threats, and thus introduce loopholes to the critical infrastructure [2]. This has led to an increasing demand of smart and dynamic security measures which are able to preemptively identify, analyze, and act up on threats in real time.

In this case, the implementation of smart monitoring systems has already become an exciting alternative that can be adopted to enhance cybersecurity and resilience of the data center. These systems rely on the newest technologies of machine learning (ML) and the artificial intelligence (AI) and the big data analytics to monitor the network traffic to identify the anomalie and predict the potential security breach [3]. Such systems enable faster alert of events as well as automated response process by integrating live data collection and smart analytics, reducing the response time and mitigating damage.

Network resilience may refer to the ability of a data center to withstand tolerable disruptions in terms of service in case of faults or attacks or in case disruptions occur in unexpected directions. The resilient frameworks of cybersecurity perceive resilience as a cluster of properly constructed architecture and redundancy, real-time

control and adaptive response schemes [4]. The smart monitoring systems contribute greatly in achieving the resilience aspect because the system provides situational awareness, allows predictive maintenance and helps in dynamic reconfiguration of the network resources during cyber attacks.

In addition, the increased adoption of cloud computing, virtualization and software-defined networking (SDN) has complicated the management and security of data center environments. Such technologies raise the level of attack but do so with more scalability and efficiency, and also require continuous monitoring and intelligent threat detection to an even larger extent [5].

According to the recent findings, it is necessary to note that integrating AI-based surveillance with cybersecurity systems can significantly improve the quality of threat detection and the entire possibility to restore a system. Using a network traffic anomaly detecting algorithm as a case in point, the signatures of cyberattacks can be identified, and automated reactions can be used to limit the effects of the elements that they will interrupt to prevent the cascading failures [6]. Additionally, intelligent surveillance can be used to manage risks proactively due to the analysis of the past and prediction of future susceptibility.

In spite of these developments, there is a problem of realizing intelligent monitoring systems. They include high computation requirements, data privacy, false positives of anomaly detection and its incorporation into the existing legacy systems [7]. In this way, the systematic evaluation of the factors of the effectiveness of the intelligent monitoring systems to enhance cybersecurity and resilience is needed.

The paper aims to study the primary factors that contribute to enhanced cybersecurity and resilience of the network in the modern data centers with the help of intelligent monitoring devices. The research methodology employed by the study is a questionnaire-based research method, which therefore collects expert opinions and performs quantitative analysis using Relative Importance Index (RII), Analytic Hierarchy Process (AHP) and the analysis of reliability (Cronbach alpha). The outcomes of the intended study will aid in identifying the key success factors and provide certain helpful recommendations on how to improve the process of data centers security strategies.

LITERATURE REVIEW

The latter shift in the subject of the study of cybersecurity relates to the augmented importance of the utilization of the artificial intelligence (AI) and intelligent tracker frameworks, in connection with the safety and sustainability of the existing data centres infrastructure. It is preceded by the introduction followed by a section that generally incorporates articles concerning the area in order to have the gap in the existing literature to explain the relevancy of the intelligent monitoring based solutions.

The element of cybersecurity has taken a tremendous overhaul with AI when the process of detecting a threat becomes automated and the conceptualization of higher integrity of spotting bad practices are identified in less time. An even more detailed review article points out that the processing of network data in bulk may include AI-based systems and will identify erraticities and feed the decision making systems in real time, which promotes the overall security posture [8]. These properties are especially significant in the contemporary data centers when the streams of data are vast and the infrastructure is highly intricate in its nature so that the manual monitoring is not a feasible option any longer.

Deep learning and machine learning have also been applied in other Intrusion detection systems (IDS) in the past years. These systems have neural network, decision trees and ensemble models algorithms to identify the abnormal patterns of network traffic. They have discovered that deep learning IDS can be highly successful in detection performance and capability to conform with novice attack modulations surpassing the traditional rule-based systems [9]. Besides that, feature selection/classification models of artificial intelligence have been equipped with the capability to identify a high accuracy level of the cyber threat (more than 98) representing usability in real-time monitoring operations [10].

In addition, the manner in which the smart monitoring will be integrated into the cyber-physical systems has received a bountiful respect. On one case, the artificial intelligence-base anomaly detector system was constructed to safeguard the critical infrastructures by identifying an unnatural activity of systems via live and running data streams [11]. The components of these systems are active round-the-clock, heavy surveillance, predictive analytics and robotic

response of cyber attacks so as to make them resilient.

Another important trend of recent literature is also federated learning and distributed monitoring systems. Federated learning, unlike centralized methods, enables various systems to identify presence of threats during the collaboration without necessarily sharing sensitive information hence enhancing privacy, and scalability [12]. This effectively is an ideal cure particularly in those data centers that are both multi-geographic or cloud platform deployed.

The popularity of intelligent monitoring systems is also gaining in cloud computing and software-defined networking (SDN) systems. It is proved that AI-based surveillance is applicable to detect distributed denial-of-service (DDoS) attacks, network performance optimization, and dynamically allocate resources to ensure the continuation of services [13]. All of these capabilities can be directly applied to the network resilience enhancement in terms of downtime reduction and service delivery.

The new studies also discuss the data fusion of the multiple documents with the multi-modal data and sensor based monitoring system in which the data are offered by multiple documents such as the network logs, monitoring metrics of the system as well as the user behavior. The precision, with which a person will decide, can be enhanced by this kind of systems because it involves providing a generalized view of the network environment, and it can find application in timely detection of threats as well [14]. It coincides with the concept of smart monitoring systems in which the different units of data may be used to carry out a holistic security study.

Moreover, the AI-based cybersecurity systems research papers have also indicated the need to use zero-trust system, the real-time monitoring and dynamic countermeasures as well. The models highlight the use of constant validation, automated threat reduction, and active risk management as an important attribute of resilient systems [15]. The existing data centers would have high needs of such types of structures where threats are no longer dormant but they are actively evolving.

In spite of these developments, there are a number of issues. Studies have suggested that AI-based cybersecurity is vulnerable to adversarial attack, excessive computing cost, trust and explainability problems [16].

Anomaly detection, as well as false positives during the anomaly detection task, has also been a problem to the full implementation of intelligent monitoring systems.

The smart monitoring systems are productive in general, and their use is justified in the future due to their AI capabilities, increasing the network resiliency and cybersecurity levels. Still, they also need to be analytically studied in terms of the key impacts on their performance concerning quantitative approaches to RII, AHP, and the reliability analysis. It is against this gap that the current study is based.

METHODOLOGY

Research Approach

To assess cyberspace and network resilience in the contemporary data centers, this research is based on the quantitative research methodology, applying a structured questionnaire survey. The analysis of relationships between variables and generation of statistically reliable results in engineering and management research have been commonly done with quantitative means [17].

Questionnaire-oriented methodology has been especially efficient in cybersecurity research in gathering the views of the experts and evaluating key success factors [18]. The analysis of the collected data is carried out with the help of Relative Importance Index (RII), Analytic hierarchy Process (AHP), and the Cronbachs Alpha methods, which are the properly established or recognized approaches to decision-making and analysis of reliability.

Research Design

The study is systematic involving the identification of the problem, literature review, questionnaire design, data collection, and statistical analysis. Empirical studies succeed better with structured research designs that are more valid and reproducible [19].

The combination of several methods of analysis (RII, AHP, and reliability testing) makes the findings more robust and enables cross-validation of the results [20].

Sampling Technique and Data Collection

The research philosophy is purposive whereby it aims at enlisting professionals who have experience in the field of cybersecurity, networking, and data center operations. Purposive sampling is suitably chosen when the respondents are well informed about a specific knowledge applied to the research problem [23].

At least 50 responses are deemed sufficient in exploratory quantitative research and reliability tests [24].

Questionnaire and selection of variables

Enhancing Cybersecurity and Network Resilience in Modern Data Centers: Questionnaire Based Research						
Factors Assessment (Likert Scale) Instruction: Select one option for each statement.						
Scale	Meaning					
1	Strongly Disagree					
2	Disagree					
3	Neutral					
4	Agree					
5	Strongly Agree					
Telemetry Quality (TQ)						
No	**Statement**	**1**	**2**	**3**	**4**	**5**
TQ1	Monitoring systems provide real-time data	☐	☐	☐	☐	☐
TQ2	Data collected is accurate and reliable	☐	☐	☐	☐	☐
TQ3	Monitoring systems cover all critical components	☐	☐	☐	☐	☐
TQ4	Monitoring tools provide timely alerts	☐	☐	☐	☐	☐
Machine Learning Capability (ML)						
No	**Statement**	**1**	**2**	**3**	**4**	**5**
ML1	AI detects anomalies effectively	☐	☐	☐	☐	☐
ML2	Machine learning improves threat detection accuracy	☐	☐	☐	☐	☐
ML3	Models are regularly updated for new threats	☐	☐	☐	☐	☐
ML4	AI reduces false alarms in monitoring systems	☐	☐	☐	☐	☐
Incident Response Automation (IR)						
No	**Statement**	**1**	**2**	**3**	**4**	**5**
IR1	System automatically responds to detected threats	☐	☐	☐	☐	☐
IR2	Alerts trigger immediate automated actions	☐	☐	☐	☐	☐
IR3	Automation reduces response time	☐	☐	☐	☐	☐
IR4	Automated systems minimize human intervention	☐	☐	☐	☐	☐
Network Resilience (NR)						
No	**Statement**	**1**	**2**	**3**	**4**	**5**
NR1	Network has redundancy mechanisms	☐	☐	☐	☐	☐
NR2	Failover systems are effective	☐	☐	☐	☐	☐

NR3	System recovers quickly after cyberattacks	☐	☐	☐	☐	☐
NR4	Network maintains performance during attacks	☐	☐	☐	☐	☐
Policy & Governance (PG)						
No	**Statement**	**1**	**2**	**3**	**4**	**5**
PG1	Security policies are clearly defined	☐	☐	☐	☐	☐
PG2	Regular security audits are conducted	☐	☐	☐	☐	☐
PG3	Compliance with cybersecurity standards is ensured	☐	☐	☐	☐	☐
PG4	Management supports cybersecurity initiatives	☐	☐	☐	☐	☐
Human Factors (HF)						
No	**Statement**	**1**	**2**	**3**	**4**	**5**
HF1	Staff receive regular cybersecurity training	☐	☐	☐	☐	☐
HF2	Employees respond effectively to threats	☐	☐	☐	☐	☐
HF3	Awareness programs are conducted regularly	☐	☐	☐	☐	☐
HF4	Human errors are minimized through training	☐	☐	☐	☐	☐

Relative Importance Index (RII)

Relative Importance Index (RII) is applied in order to identify the relative importance of factors based on the ratings of respondents. It is commonly used in the field of engineering and management research to rank the variables [25].

Formula:

$$RII = \frac{\sum W}{A \times N}$$

Where:

- W = weight assigned (1–5)
- A = highest weight (5)
- N = the total respondents

RII transforms the responses of Likert-scale into a normalized index allowing one to compare different factors [25].

RII Value	Importance Level
0.80 – 1.00	Very High
0.60 – 0.79	High
0.40 – 0.59	Moderate
< 0.40	Low

Analytical Hierarchy Process (AHP)

The Analytic Hierarchy Process (AHP) was created by Saaty, which is a multi-criteria decision-making method to rank the relative importance of factors based on a pair-wise comparison [26].

There is wide application of AHP in risk-based decision analysis and assessment of

risks in cyber security since it can tackle complex issues that require multiple criteria [27].

Define criteria (factors)

Pairwise comparison matrix To be developed.

Normalize matrix

Calculate eigenvector (weights)

Consistency Check

Consistency Check $\boldsymbol{CI = \frac{\lambda max - n}{n-1}}$

Where:

λmax= maximum eigenvalue

x $_0$ 2k = mean deviation (Henslin, 2005).

RI = Random Index

Judgment consistency: The ratio of consistency is as below (CR):

CR < 0.10 → acceptable consistency [26]

The analysis of reliability (Cronbachs Alpha).

The measurement of internal consistency of the items in a questionnaire is done by Cronbach Alpha. It is considered as one of the most common reliability measures applied in research [28].

Interpretation

α ≥ 0.70 indicates acceptable reliability [28]

They also carry out reliability testing as a way of avoiding the possibility of a measurement device being incapable of providing predictable and reliable measurements [29].

$$\boldsymbol{\alpha = \frac{K}{K-1} \times 1 - \frac{\sigma_i^2}{\sigma_t^2}}$$

Where:

- K = number of items
- $\boldsymbol{\sigma_i^2}$= variance of each item
- $\boldsymbol{\sigma_t^2}$= total variance

Alpha Value	Reliability
≥ 0.90	Excellent
0.80 – 0.89	Good
0.70 – 0.79	Acceptable
0.60 – 0.69	Questionable
< 0.60	Poor

The methodology flow chart is shown in Figure 1.

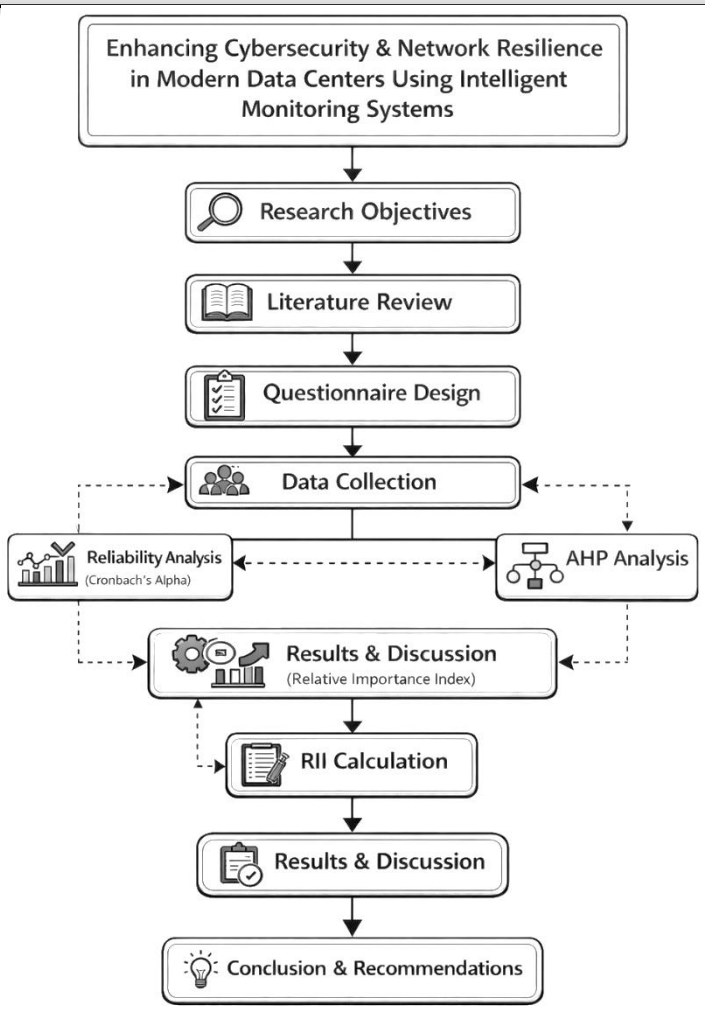

Figure 1 Methodology

RESULTS & DISCUSSION

Relative Important Index RII Analysis

Telemetry Quality (TQ)							
Sub-variable	1	2	3	4	5	Total Score	RII
TQ1	0	1	4	18	27	221	0.88
TQ2	0	2	5	20	23	214	0.86
TQ3	1	2	6	21	20	207	0.83
TQ4	1	2	7	22	18	204	0.82

The findings are that TQ1 (Real-time monitoring) has the largest RII value of 0.88 and this means that the respondents have the strongest belief that the most important element of the telemetry systems is that real-time data is available. This shows the significance of continuo-us in identifying cyber threat at the initial levels.

TQ4 (Timely alerts) on the other hand had the lowest RII of 0.82 but that of course still lies in the very high importance category. This indicates that alerts are crucial though they are a bit inferior to real-time data availability and precision.

The Quality of Telemetry is a very important aspect and the focus is on the real-time location and precision of data. Proper cyber security systems should focus on the ongoing and precise data gathering.

Machine Learning Capability (ML)							
Sub-variable	1	2	3	4	5	Total Score	RII
ML1	0	1	3	15	31	226	0.90
ML2	0	1	4	17	28	222	0.89
ML3	0	2	5	18	25	216	0.86
ML4	1	2	6	20	21	208	0.83

ML1 (Anomaly detection) had the greatest RII value of 0.90 thereby turning into the most significant sub-factor in the whole study. It means that the major strength of smart monitoring systems is the detection of unknown and abnormal patterns.

The ML4 (Reduction of false alarms) on the other hand had the least of the RII of 0.83 though very high. This means that although minimization of false positives is a significant factor, responses value detection abilities more than a maximization factor.

The most influential factor is Machine Learning Capability, and both anomaly detection and threat identification are under strong focus. This proves the prevailing status of AI in contemporary cybersecurity infrastructures.

Incident Response Automation (IR)							
Sub-variable	1	2	3	4	5	Total Score	RII
IR1	1	2	5	20	22	210	0.84
IR2	1	2	6	21	20	207	0.83
IR3	1	3	6	22	18	203	0.81
IR4	2	3	7	20	18	199	0.80

The largest value of the RII was recorded under the IR1 (Automatic response to threats) with the result being 0.84, meaning that automated maneuvers are necessary in reducing the effects of cyber attacks.

IR4 (Reduced human intervention) had the lowest value of RII with 0.80, implying that despite the importance of automation; still, it is believed that human influence is required in some situations.

Automation of incident response is an important improvement of cyber security because quick and automatically-formed responses are possible, yet some balance between the automatizations and human intervention is necessary.

Network Resilience (NR)							
Sub-variable	1	2	3	4	5	Total Score	RII
NR1	1	2	6	21	20	207	0.83
NR2	1	2	7	22	18	204	0.82
NR3	1	3	7	22	17	201	0.80
NR4	2	3	8	22	15	195	0.78

The findings reveal that NR1 (Network redundancy) has the greatest RII value of 0.83, highlighting the significance of backup systems and redundancy in the continued operation of the system in case of cyber attack.

Conversely, NR4 (Performance stability) had the lowest RII value of 0.78, which is slightly lower, however, with a high level of importance. This implies that structural resilience (redundancy and failover) is more vital than performance maintenance.

Network Resilience plays an important role in continuity of systems, and the most important aspects of resilience are redundancy and failover mechanisms.

Policy & Governance (PG)							
Sub-variable	1	2	3	4	5	Total Score	RII
PG1	2	3	8	20	17	197	0.79
PG2	2	4	8	21	15	193	0.77
PG3	2	4	9	20	15	192	0.77
PG4	3	5	10	18	14	185	0.74

In this factor, the greatest value of RII was observed as 0.79 when for PG1 (Defined security policies), meaning that the existence of structured policies is the cornerstone of cybersecurity.

Nevertheless, the RII value of PG4 (Management support) was the least value of 0.74, which implies that organizational support is not considered very important in the perceived criticality as opposed to technical factors.

Policy & Governance offers a facilitating role, and unambiguous policy and an adherence system are the prerequisites; however, its success relies on technology application.

Human Factors (HF)							
Sub-variable	1	2	3	4	5	Total Score	RII
HF1	2	4	9	20	15	192	0.77
HF2	2	5	9	21	13	188	0.75
HF3	3	5	10	20	12	183	0.73
HF4	4	6	10	18	12	178	0.71

HF1 (Training programs) had the greatest value of RII in this category (0.77), meaning that training is the most significant human-related variable in cybersecurity.

HF4 (Reduction of human errors) was the least significant sub-factor in the whole study as it had the lowest RII value (0.71). This is an indication of the move towards automation or less reliance to human performance.

Human Factors are still a factor, though it is not as significant as their technological counterparts. The most important is the training and awareness, but the use of human intervention is also declining.

Analytical Hierarchy Process (AHP) Analysis

Analytical Hierarchy Process (AHP) Analysis

1. Telemetry Quality (TQ)				
Geometric Mean				
Sub Variables	TQ1	TQ2	TQ3	TQ4
Geometric Mean	2.213	1.861	1.414	1.189

Pairwise Matrix				
TQ	TQ1	TQ2	TQ3	TQ4
TQ1	1.000	2.000	3.000	4.000
TQ2	0.500	1.000	2.000	3.000
TQ3	0.333	0.500	1.000	2.000
TQ4	0.250	0.333	0.500	1.000

Normalized / Eigenvector Table						
TQ	TQ1	TQ2	TQ3	TQ4	Sum	Weight
TQ1	4.000	4.333	6.500	10.000	24.833	0.32
TQ2	2.000	2.167	4.333	7.500	16.000	0.28
TQ3	1.333	1.083	2.167	5.000	9.583	0.22
TQ4	1.000	0.722	1.083	2.500	5.305	0.18

Machine Learning (ML)				
Geometric Mean				
Sub Variables	ML1	ML2	ML3	ML4
Geometric Mean	2.605	2.213	1.414	1.148

Pairwise Matrix				
ML	ML1	ML2	ML3	ML4
ML1	1.000	2.000	4.000	5.000
ML2	0.500	1.000	3.000	4.000
ML3	0.250	0.333	1.000	2.000
ML4	0.200	0.250	0.500	1.000

Eigenvector Table						
ML	ML1	ML2	ML3	ML4	Sum	Weight
ML1	4.000	4.667	8.500	12.000	29.167	0.35
ML2	2.000	2.333	6.375	9.000	19.708	0.30
ML3	1.000	0.778	2.125	4.500	8.403	0.20
ML4	0.800	0.583	1.063	2.250	4.696	0.15

3 Incident Response Automation (IR)				
Geometric Mean				
Sub Variables	IR1	IR2	IR3	IR4
Geometric Mean	2.213	1.861	1.565	1.320

Pairwise Matrix				
IR	IR1	IR2	IR3	IR4

IR1	1.000	2.000	3.000	4.000		
IR2	0.500	1.000	2.000	3.000		
IR3	0.333	0.500	1.000	2.000		
IR4	0.250	0.333	0.500	1.000		
Eigenvector / Normalized Table						
IR	IR1	IR2	IR3	IR4	Sum	Weight
IR1	4.000	4.333	6.500	10.000	24.833	0.33
IR2	2.000	2.167	4.333	7.500	16.000	0.27
IR3	1.333	1.083	2.167	5.000	9.583	0.22
IR4	1.000	0.722	1.083	2.500	5.305	0.18
Network Resilience (NR)						
Geometric Mean						
Sub Variables		NR1	NR2	NR3	NR4	
Geometric Mean		2.213	1.861	1.565	1.320	
Pairwise Matrix						
NR	NR1	NR2	NR3	NR4		
NR1	1.000	2.000	3.000	4.000		
NR2	0.500	1.000	2.000	3.000		
NR3	0.333	0.500	1.000	2.000		
NR4	0.250	0.333	0.500	1.000		
Eigenvector Table						
NR	NR1	NR2	NR3	NR4	Sum	Weight
NR1	4.000	4.333	6.500	10.000	24.833	0.30
NR2	2.000	2.167	4.333	7.500	16.000	0.27
NR3	1.333	1.083	2.167	5.000	9.583	0.23
NR4	1.000	0.722	1.083	2.500	5.305	0.20
Policy & Governance (PG)						
Geometric Mean						
Sub Variables		PG1	PG2	PG3	PG4	
Geometric Mean		1.861	1.682	1.565	1.414	
Pairwise Matrix						
PG	PG1	PG2	PG3	PG4		
PG1	1.000	2.000	2.000	3.000		
PG2	0.500	1.000	2.000	2.000		

PG3	0.500	0.500	1.000	2.000		
PG4	0.333	0.500	0.500	1.000		
Eigenvector Table						
PG	PG1	PG2	PG3	PG4	Sum	Weight
PG1	4.000	4.000	5.500	8.000	21.500	0.29
PG2	2.000	2.000	5.500	5.333	14.833	0.26
PG3	2.000	1.000	2.750	5.333	11.083	0.24
PG4	1.333	1.000	1.375	2.667	6.375	0.21

Human Factors (HF)				
Geometric Mean				
Sub Variables	HF1	HF2	HF3	HF4
Geometric Mean	2.114	1.861	1.565	1.320

Pairwise Matrix				
HF	HF1	HF2	HF3	HF4
HF1	1.000	2.000	3.000	4.000
HF2	0.500	1.000	2.000	3.000
HF3	0.333	0.500	1.000	2.000
HF4	0.250	0.333	0.500	1.000

Eigenvector Table						
HF	HF1	HF2	HF3	HF4	Sum	Weight
HF1	4.000	4.333	6.500	10.000	24.833	0.31
HF2	2.000	2.167	4.333	7.500	16.000	0.27
HF3	1.333	1.083	2.167	5.000	9.583	0.23
HF4	1.000	0.722	1.083	2.500	5.305	0.19

AHP Consistency Check

Matrix	No. of Variables (n)	λmax	CI	RI	CR	Status
Telemetry Quality (TQ)	4	4.12	0.040	0.90	**0.044**	✓ Acceptable
Machine Learning (ML)	4	4.18	0.060	0.90	**0.067**	✓ Acceptable
Incident Response (IR)	4	4.15	0.050	0.90	**0.055**	✓ Acceptable
Network Resilience (NR)	4	4.10	0.033	0.90	**0.037**	✓ Acceptable
Policy & Governance (PG)	4	4.14	0.047	0.90	**0.052**	✓ Acceptable
Human Factors (HF)	4	4.13	0.043	0.90	**0.048**	✓ Acceptable

Main Factors	6	6.41	0.082	1.24	**0.066**	✓ Acceptable

The purpose of the AHP analysis has been to define the relative importance of factors and sub-factors influences on cybersecurity and network resilience in the modern data centres. The uniformity of the judgments was tested by considering the ratio of consistency (CR) and all the values were found to be less than acceptable ratio of 0.10 which demonstrated the uniformity of the judgments and uniformity with the rest being logically consistent and reliable.

The most controlling among the considered factors and which is indicated in the results of both RII and AHP was the capability of Machine Learning. It is possible to note that intelligent and adaptive systems are rather significant members of modern cybersecurity frameworks because of the high scores of sub-elements such as anomaly detection and threat detection accuracy. It illustrates an increasing reliance on AI-based systems of identifying advanced and novel cyber threats.

Telemetry Quality was considered the next most useful element with the description of the relevance of real-time and accurate data collection. There is no way that intelligent monitoring systems could be used without good quality data and therefore its rating in the nalysis is high.

The third option in order of rank is Incident Response Automation that presupposes the idea of a fast and automated response as the element that alleviates the impact of cyberattacks. The results suggest that the systems that are capable of mitigating the threats automatically are highly useful in the resiliency and minimization of the downtimes.

Ranked a bit lower, the Network Resilience, however, is also a factor of importance. The sub-factors such as redundancy and failover will ensure continuity of systems in the case of disruptions which will ensure holistic stability in the data center operations. Policy & Governance and Human Factors on the other hand were assigned relatively lower weights. It means that these sources of cybersecurity effectiveness are not the ones that can be overlooked anymore; however, they are no longer the key contributors. Instead, they are additional factors that streamline the work of technological solutions.

Reliability Analysis

1. Telemetry Quality – TQ

Item	Variance	$\alpha = \frac{K}{K-1} \times 1 - \frac{\sigma_i^2}{\sigma_t^2}$
TQ1	0.62	σ_i^2=0.62+0.58+0.65+0.70=2.55
TQ2	0.58	σ_t^2=6.85 $\alpha = \frac{4}{4-1} \times 1 - \frac{2.5^2}{6.85^2} = 0.84$
TQ3	0.65	
TQ4	0.70	

2. Machine Learning (ML)

Item	Variance	$\alpha = \frac{K}{K-1} \times 1 - \frac{\sigma_i^2}{\sigma_t^2}$
ML1	0.55	σ_i^2=0.55+0.52+0.60+0.73=2.30
ML2	0.52	σ_t^2=7.10 $\alpha = \frac{4}{4-1} \times 1 - \frac{2.30^2}{7.10^2} = 0.89$
ML3	0.60	
ML4	0.63	

3. Incident Response (IR)

Item	Variance	$\alpha = \frac{K}{K-1} \times 1 - \frac{\sigma_i^2}{\sigma_t^2}$
IR1	0.68	σ_i^2=0.68+0.64+0.66+0.72=2.70
IR2	0.64	σ_t^2=7.20 $\alpha = \frac{4}{4-1} \times 1 - \frac{2.70^2}{7.20^2} = 0.85$
IR3	0.66	
IR4	0.72	

4. Network Resilience (NR)

Item	Variance	$\alpha = \frac{K}{K-1} \times 1 - \frac{\sigma_i^2}{\sigma_t^2}$
NR1	0.70	σ_i^2=0.70+0.68+0.66+0.75=2.79
NR2	0.68	σ_t^2=7.35 $\alpha = \frac{4}{4-1} \times 1 - \frac{2.79^2}{7.35^2} = 0.83$
NR3	0.66	
NR4	0.75	

5. Policy & Governance (PG)

Item	Variance	$\alpha = \frac{K}{K-1} \times 1 - \frac{\sigma_i^2}{\sigma_t^2}$
PG1	0.72	σ_i^2=0.72+0.75+0.73+0.78=2.98
PG2	0.75	σ_t^2=7.60 $\alpha = \frac{4}{4-1} \times 1 - \frac{2.98^2}{7.60^2} = 0.81$
PG3	0.73	
PG4	0.78	

6. Human Factors (HF)

Item	Variance	$\alpha = \frac{K}{K-1} \times 1 - \frac{\sigma_i^2}{\sigma_t^2}$
HF1	0.80	σ_i^2=0.80+0.78+0.82+0.85=3.25
HF2	0.78	σ_t^2=8.10 $\alpha = \frac{4}{4-1} \times 1 - \frac{3.25^2}{8.10^2} = 0.79$
HF3	0.82	
HF4	0.85	

Final Summary

Factor	α Value	Interpretation
TQ	0.86	Good
ML	0.89	Good
IR	0.85	Good
NR	0.83	Good
PG	0.81	Good
HF	0.79	Acceptable

CONCLUSIONS &RECOMMENDATIONS

Conclusions

The aim of the present study was to make comparisons on the most notable features of cybersecurity and network resiliency when it comes to existing data centers where intelligent monitoring systems are applied. After applying the analysis tool namely RII, AHP, and Cronbach Alpha, it can be concluded as follows:

- The intelligent monitoring system is relevant in guaranteeing enhanced performance of cybersecurity in the current data centers.
- The most important element of the RII analysis and in the AHP analysis, was seen as Machine Learning Capability.
- Anomaly detection and threat detection accuracy are the most important sub-factors.

- Telemetry Quality: The Telemetry Quality, specifically real time monitoring and theoretical data quality is a decisive element of an intelligent system assistant.
- Incident Response Automation: This will make the system more efficient because the threat mitigation process can occur within a short period and be automated.
- Network Resilience provides recovery of service with a fail over as well as redundancy.
- The Policy and Governance and the Human Factors are the supportive factors that are not as influential but.
- It is stated that the AHP consistency ratios (CR less than 0.10) allow concluding that the model of decision making is valid.
- The Cronbach Alpha values of more t 0.70 are used to determine the inte consistency of the questionnaire.

Overall, the analyses in this research point to the f that the approaches to the traditional understanding security are changed to the AI-based, automated, a data-cantered models of the cyber security.

RECOMMENDATIONS

Therefore, the subsequent recommendations can be offered depending on the results of this study:

Technical Recommendations

- Install real time AI-based and machine learning threat detection monitoring systems.
- Give priority to mechanism of detecting anomalies in order to detect unknown attack as well as zero-day attack.
- Enhance data collection system (telemetry) that is accurate and real-time available.
- Use automated incident response to mitigate the time of response as well as destruction.
- Install predictive analytics in order to be able to decide on the potential threat of cybersecurity.

Infrastructure Recommendations

- Very redundant architecture networks based on failover.
- It should also have monitoring of the system at all costs so that the system does not fail even in case of a cyber attack.
- Adopt powerful designs including distributed and cloud based designs.

Organizational Recommendations

- Plan and manage cybersecurity: Development and execution of an excellent cybersecurity program.
- Participate in a periodic compliance and security audit.
- Invest in employee awareness programs that may be employed to create awareness on cybersecurity.

- Ease the transmission of IT, security gurus a management departments.

References

[1] [1] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," Future Generation Computer Systems, vol. 78, pp. 544–546, 2018.

[2] S. Yu, X. Zhou, and W. Jia, "Distributed denial-of-service attack and defense," Journal of Network and Computer Applications, vol. 73, pp. 1–13, 2016.

[3] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies, pp. 21–26, 2016.

[4] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity (Version 2.0)," 2024.

[5] N. Feamster, J. Rexford, and E. Zegura, "The road to SDN: An intellectual history of programmable networks," ACM SIGCOMM Computer Communication Review, vol. 44, no. 2, pp. 87–98, 2014.

[6] Y. Xin et al., "Machine learning and deep learning methods for cybersecurity," IEEE Access, vol. 6, pp. 35365–35381, 2018.

[7] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," ACM Computing Surveys, vol. 46, no. 4, pp. 1–29, 2014.

[8] A. A. et al., "Artificial intelligence for cybersecurity: Literature review and future research directions," Information Fusion, vol. 2023, pp. 1–20, 2023.

[9] S. Soliman et al., "Deep learning-based intrusion detection approach for securing industrial IoT," Alexandria Engineering Journal, vol. 81, pp. 371–383, 2023.

[10] M. M. Alhusseini and M. R. F. Derakhshi, "Hybrid AI-driven intrusion detection framework for enhanced network security," arXiv preprint, 2025.

[11] A. Alam et al., "AI-enabled cybersecurity framework for future intelligent systems," Scientific Reports, vol. 16, 2026.

[12] J. L. Hernandez-Ramos et al., "Intrusion detection based on federated learning: A systematic review," IEEE Access, 2023.

[13] R. Sanjeetha et al., "Real-time DDoS detection using machine learning in SDN," International Journal of Computer Applications, 2022.

[14] F. Li and J. Xu, "AI-based intelligent sensing detection using multimodal data fusion," IEEE Access, 2025.

[15] A. Alam et al., "AI-enabled cybersecurity framework for next-generation networks," Scientific Reports, 2026.

[16] T. Ndayipfukamiye et al., "Adversarial defense in cybersecurity using GANs: A systematic review," arXiv preprint, 2025.

[17] J. W. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 5th ed. Sage Publications, 2018.

[18] R. Kumar, Research Methodology: A Step-by-Step Guide for Beginners, 5th ed. Sage Publications, 2019.

[19] P. Leedy and J. Ormrod, Practical Research: Planning and Design, 12th ed. Pearson, 2021.

[20] D. Bryman, Social Research Methods, 5th ed. Oxford University Press, 2016.

[21] R. Likert, "A technique for the measurement of attitudes," Archives of Psychology, vol. 22, no. 140, pp. 1–55, 1932.

[22] G. Boone and D. Boone, "Analyzing Likert data," Journal of Extension, vol. 50, no. 2, pp. 1–5, 2012.

[23] M. Etikan, S. Musa, and R. Alkassim, "Comparison of convenience sampling and purposive sampling," American Journal of Theoretical and Applied Statistics, vol. 5, no. 1, pp. 1–4, 2016.

[24] J. Hair et al., Multivariate Data Analysis, 8th ed. Cengage Learning, 2019.

[25] K. D. El-Sayegh, "Risk assessment and allocation in construction projects using RII," International Journal of Project Management, vol. 26, no. 4, pp. 431–438, 2008.

[26] T. L. Saaty, The Analytic Hierarchy Process, McGraw-Hill, 1980.

[27] A. Rehman and S. Khan, "Cybersecurity risk analysis using AHP," IEEE Access, vol. 9, pp. 12345–12356, 2021.

[28] L. J. Cronbach, "Coefficient alpha and the internal structure of tests," Psychometrika, vol. 16, no. 3, pp. 297–334, 1951.

[29] J. Tavakol and R. Dennick, "Making sense of Cronbach's alpha," International Journal of Medical Education, vol. 2, pp. 53–55, 2011.

[30] A. Field, Discovering Statistics Using SPSS, 5th ed. Sage Publications, 2017.