IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AI-Powered Intrusion Detection System(IDS) In Healthcare: Necessity Or Option?

[1]Arwa Abbasali Kalyanwala, [2]Dr Divya Premchandran

[1]MSc-IT Student, [2]Assistant Professor

[1]Department of Information Technology,

[1]Keraleeya Samajam (Regd.) Dombivli's Model College (Empowered Autonomous), Mumbai, India

Abstract: Healthcare databases are increasingly becoming prime targets for cyberattacks and ransomware, leading to severe threats to patient privacy and hospital functionality. Traditional Intrusion Detection Systems (IDS) often fall short in detecting sophisticated attacks due to high false-positive rates, limited adaptability, and inability to detect novel threats. This research paper explores the growing necessity of integrating Artificial Intelligence (AI) into IDS to enhance cybersecurity in healthcare environments. By leveraging adaptive learning and intelligent decision-making, AI-powered IDS can efficiently identify anomalies, predict potential breaches, and minimize false alarms. This study highlights the limitations of traditional IDS, the potential of AI-driven solutions, and their role in safeguarding patient data. The ultimate goal is to emphasize that AI-powered IDS is not just an optional upgrade but an essential security measure in modern healthcare systems.

Index Terms - Healthcare, Cybersecurity, Intrusion Detection System, Artificial Intelligence, Ransomware, Data Privacy.

I. INTRODUCTION

The healthcare sector today depends heavily on digital systems to manage patient information, medical records, and critical operations. This dependence on technology has made healthcare a major target for cybercriminals. In recent years, numerous hospitals in India and abroad have suffered cyberattacks that disrupted medical services and compromised sensitive data. Such attacks expose a critical gap in existing security frameworks, especially within Intrusion Detection Systems (IDS).

Artificial Intelligence (AI) offers a powerful solution by enhancing the detection of unusual activities, learning from network behavior, and identifying unknown threats. This research focuses on understanding whether AI-powered IDS is necessary in the healthcare sector or merely an additional security option.

II.BACKGROUND

Healthcare organizations collect and store vast amounts of sensitive data, including patient medical histories, financial details, and digital diagnostic reports. These records, if compromised, can lead to identity theft, blackmail, and data manipulation. Traditional IDS monitor network traffic and alert administrators when malicious activity is detected. However, due to the growing complexity of cyber threats, traditional systems often fail to adapt to new or evolving attack patterns.

Recent ransomware incidents in hospitals such as AIIMS (India, 2022) and Apollo Hospitals highlight how healthcare infrastructure remains vulnerable. [1] The increasing sophistication of cyberattacks calls for more intelligent, self-learning systems capable of detecting and mitigating these threats in real-time.

III. LITERATURE REVIEW

Healthcare systems and Internet-of-Medical-Things (IoMT) devices are rapidly adopting digital services and AI-powered analytics, but that digitalization has also created a rich attack surface for cybercriminals. Several recent reviews and surveys emphasize that healthcare remains one of the most targeted sectors for ransomware and data exfiltration, and that conventional signature/rule-based IDS struggle with novel, polymorphic and zero-day attacks common in modern networks and IoMT deployments. [1]

AI in IDS for healthcare / IoMT:

AI and machine-learning approaches (classical ML, tree ensembles, deep learning) have been shown to improve detection accuracy and reduce false positives compared with simple rule/signature systems — especially for anomaly/behavioral detection in IoT/IoMT contexts. Several IoMT-focused works demonstrate high detection rates using tree-based ensembles, gradient boosted methods and feature-selection pipelines tuned for the CIC-IDS and TON-IoT families of datasets. These approaches show strong promise for IoMT environments where resource constraints and heterogeneous traffic require careful feature selection and lightweight inference. [1]

Privacy-preserving and collaborative training (Federated Learning):

Because hospital data are highly sensitive and often cannot be centralized, federated learning (FL) has become a leading technique to train IDS or threat models across institutions without sharing raw patient data. Systematic reviews of FL in healthcare report many proof-of-concept studies but relatively few real-world deployments to date; they also highlight challenges like non-IID data, communication costs, and governance — all of which impact whether an AI-IDS can be adopted across hospitals. FL is therefore a promising path for cooperative IDS models, but it introduces new concerns (model poisoning, governance, convergence).[7]

Explainability, trust and operational use:

One major practical barrier to deploying AI-IDS in healthcare is lack of explainability. Security teams and clinical administrators need human-understandable reasons for alerts (so they can make high-stakes operational decisions). Recent XAI research for IDS has produced end-to-end frameworks (SHAP, LIME, local/global explainers) tailored to network data; those works show that lightweight explanations are feasible and often come with negligible runtime cost — an important factor for real-time hospital environments. Explainability also ties directly into user trust and regulatory acceptance.[6]

Concept drift & continual learning:

Network behavior and attack patterns evolve continuously. Concept drift (changes in the underlying data distribution over time) is well documented in IDS literature; static models degrade unless updated or designed for streaming/online learning. Surveys on concept drift emphasize that anomaly/IDS systems require continual/adaptive learning strategies (windowing, incremental learning, drift detectors) to remain effective in production. This gap (how to rapidly and safely update AI-IDS in live hospital networks while avoiding catastrophic forgetting or poisoning) is a recurring research need.

Adversarial robustness and attack surface:

AI models themselves are targets: adversarial evasion, poisoning, or model-stealing attacks can reduce IDS effectiveness or even be weaponized against healthcare systems. Reviews across medical AI and NIDS document that adversarial methods degrade model performance and that defenses (adversarial training, ensembles, detection) are an active area of research. Any healthcare AI-IDS must therefore consider robustness and integrity of the learning pipeline.

Datasets, evaluation and real-world gaps:

Most IDS research uses public datasets such as NSL-KDD and CIC-IDS2017 for benchmarking, but those datasets differ substantially from real hospital traffic (IoMT heterogeneity, temporal patterns, and privacy constraints). Reviews call out the scarcity of labeled, realistic hospital/IoMT datasets and the resulting risk that high lab accuracy does not translate to operational readiness. This explains why many academically successful models fail or produce many false positives in production healthcare networks.

IV. CONCEPT OF AI-POWERED INTRUSION DETECTION SYSTEM

AI-powered IDS use advanced machine learning and deep learning algorithms to detect anomalies, identify zero-day attacks, and reduce false alarms. These systems analyze vast datasets, learn from behavior patterns, and make decisions autonomously.

Benefits include:

- Real-time threat detection and prevention
- Reduced false positives
- Ability to detect previously unseen (zero-day) attacks
- Continuous adaptation through self-learning

However, challenges such as model transparency (explainability), data privacy, and scalability still remain, which require ongoing research.

V. RESEARCH METHODOLOGY

5.1 Research Design

This study is designed to explore the need for AI-powered Intrusion Detection Systems (IDS) in the healthcare sector and assess the awareness level among students, faculty, and IT professionals regarding healthcare cybersecurity. The research aims to understand both the benefits and challenges of adopting AI-based IDS, providing a balanced perspective on its necessity versus optional adoption.

5.2 Research Approach

A mixed approach is followed, using surveys, user feedback, and secondary data from existing studies. This helps combine real user views with already available knowledge.

5.3 Data Collection Methods

Data for this research was collected using a structured online survey created via Google Forms. The questionnaire consisted of both objective and opinion-based questions designed to gather insights into cybersecurity awareness, health data privacy concerns, and acceptance of AI-based systems.

5.4 Sampling Strategy

The study used a non-probability convenience sampling method. Respondents were selected based on their relevance to the IT and AI domain. Participants included a mix of individuals with different educational and professional backgrounds, ensuring a diverse viewpoint. The variety of respondents helps in understanding how different groups perceive the role of AI in securing healthcare databases.

5.5 Data Analysis Techniques

Collected data was analyzed using descriptive statistics such as percentages and frequency distribution. The responses were visualized through charts and graphs to identify common patterns and awareness levels. Comparative analysis was performed to highlight differences in perception among students, faculty, and professionals. The study focuses on how participants view AI's capability to reduce cyber risks, improve detection accuracy, and safeguard medical information.

5.6 Tool Used

Basic survey forms, spreadsheets, and simple statistical tools are used to organize and study the data. These tools make the research process easy, clear, and understandable. Graphs, charts, and summary tables are also created to visualize trends and highlight key findings.

5.7 Ethical Considerations

All data is collected with consent, and user privacy is respected. Sensitive details are kept safe and anonymous. Care is taken to ensure that no user feels pressured or exposed. Participants are informed about the purpose of the study, and they have the right to withdraw at any time without consequences.

5.8 Limitations

The study is limited by the sample size and the respondents' familiarity with AI and cybersecurity concepts. it does not include practical deployment or real-time testing of ids in healthcare organizations due to time and resource constraints. the findings are based on perceptions and awareness rather than direct implementation. moreover, the fast-evolving nature of cyber threats and AI technology may influence the long-term applicability of the results.

VI. TARGET AUDIENCE

IT Students & Young Professionals

Individuals studying cybersecurity, AI, or healthcare IT, who represent the next generation of digital professionals.

Academic Faculty & Researchers

Experts in IT and AI domains who can provide theoretical perspectives on the adoption of AI in healthcare.

Retired and Others

A smaller portion of respondents who did not fit into the above categories but participated out of general interest or awareness of data privacy and healthcare technology trends.

VII. QUESTIONNAIRE DESIGN FOR USER PERCEPTION ANALYSIS

To complement the analysis of traditional and AI-powered Intrusion Detection Systems (IDS), a user perception survey was designed using a structured questionnaire. The goal was to assess awareness, trust, usability, and privacy concerns regarding the application of AI in securing healthcare data.

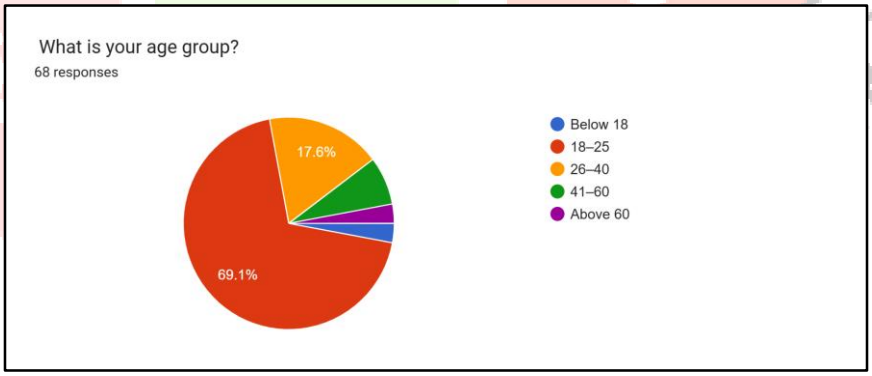
Sample Focus Areas:

- Awareness of cyber threats and IDS in healthcare
- Familiarity with the concept of AI-powered security systems
- Trust in AI for detecting and preventing cyberattacks
- Concerns about data misuse, privacy, and system transparency
- Perceived need for AI-powered IDS in hospitals and health data systems

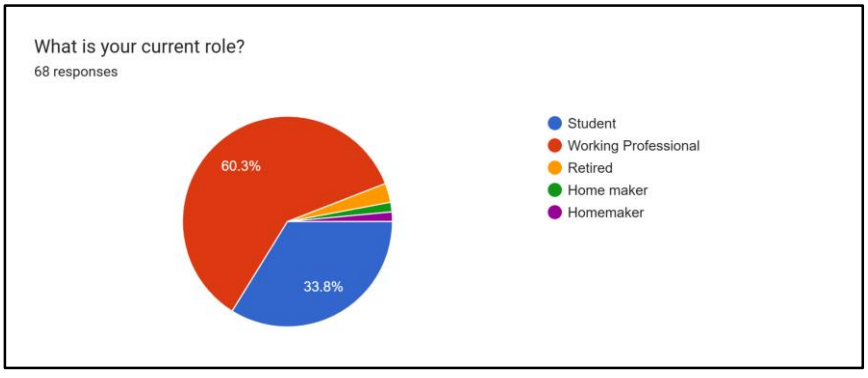
Willingness to adopt AI-based security tools in future healthcare infrastructure

VIII. SURVEY QUESTIONNAIRE AND RESULTS

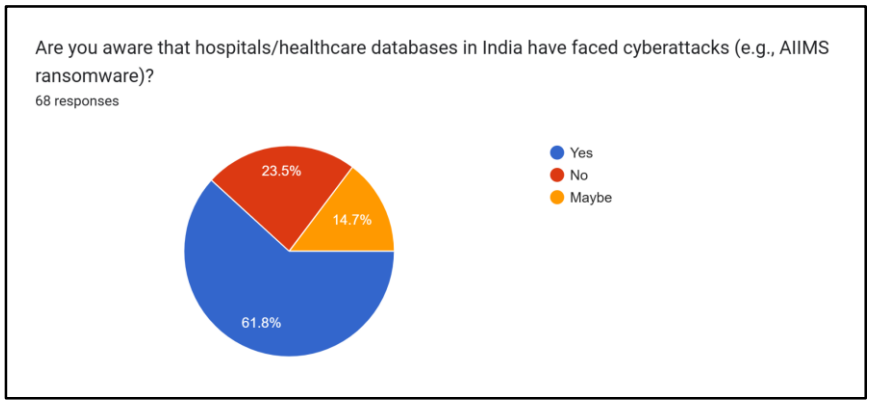
1. What is your age group?



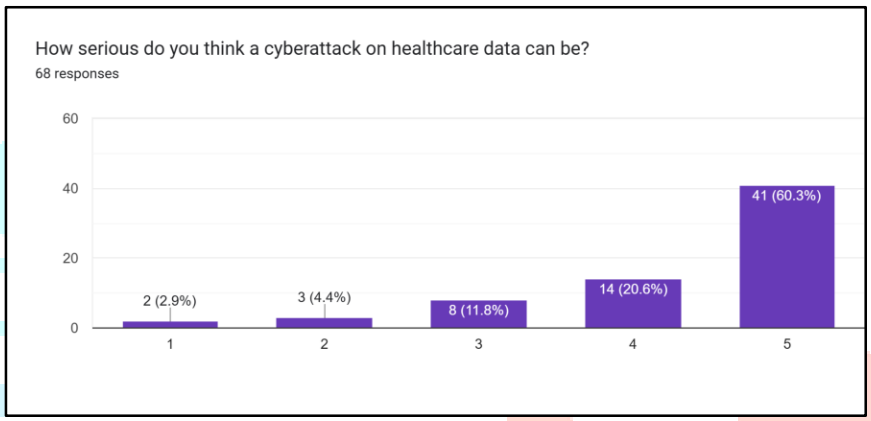
2. What is your current role?



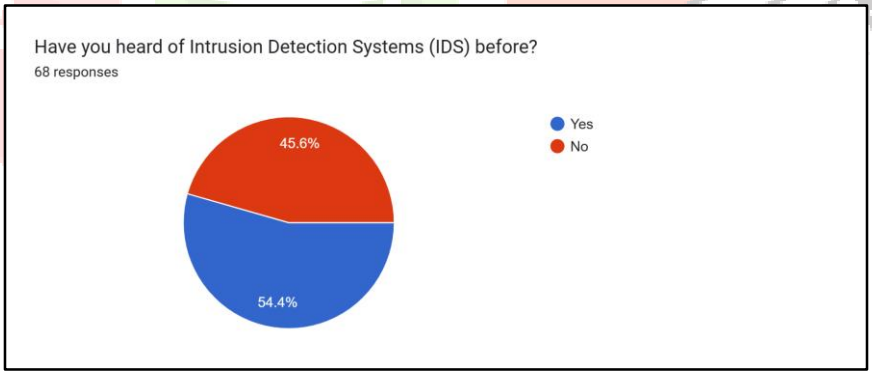
3. Are you aware that hospitals/healthcare databases in India have faced cyberattacks (e.g., AIIMS ransomware)?



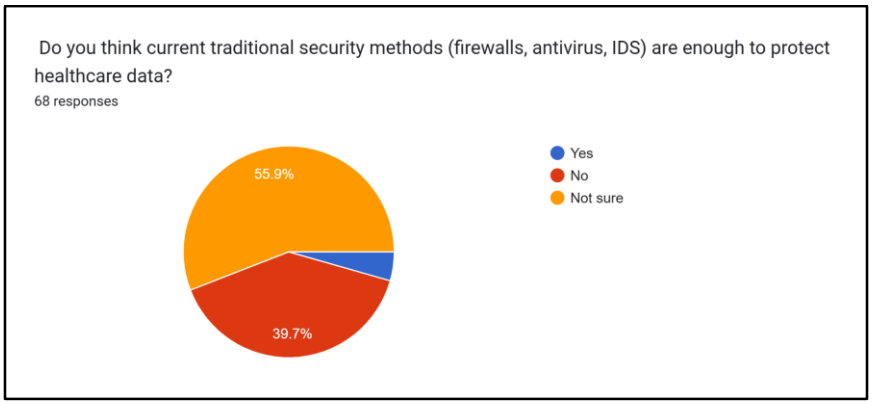
4. How serious do you think a cyberattack on healthcare data can be?



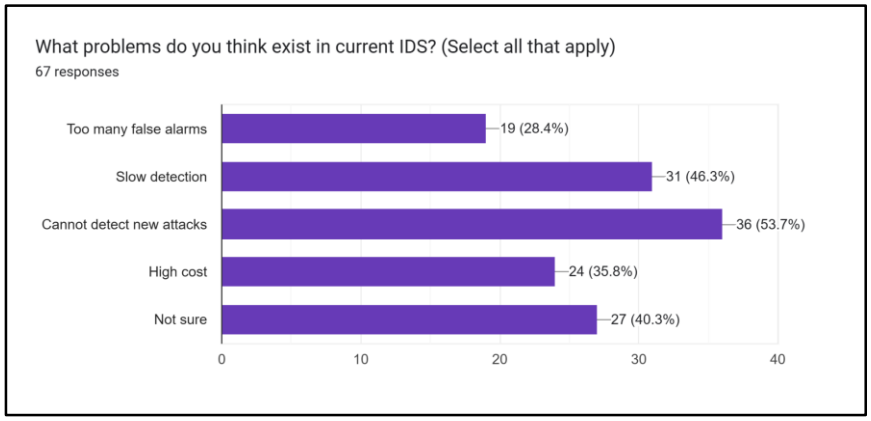
5. How concerned would you be if you found out your personal health/medical data was leaked?



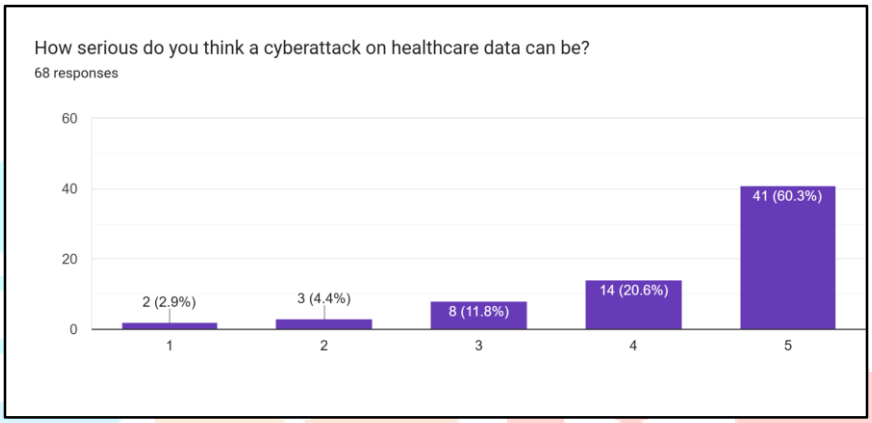
6. Do you have any idea how leaked health data could be misused?



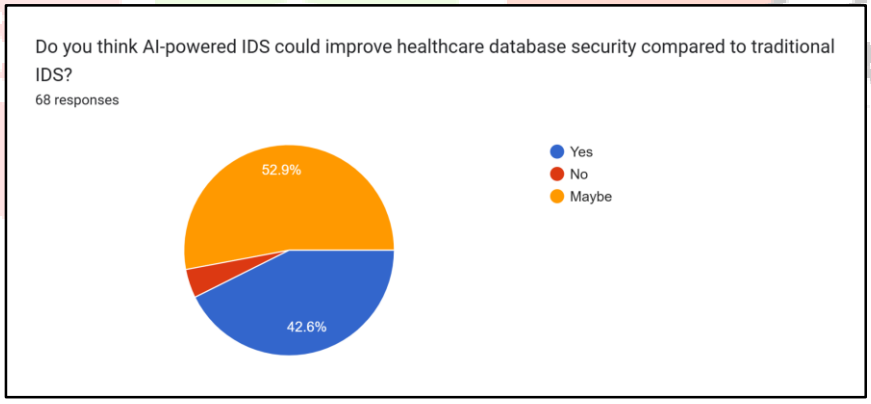
7. Have you heard of Intrusion Detection Systems (IDS) before?



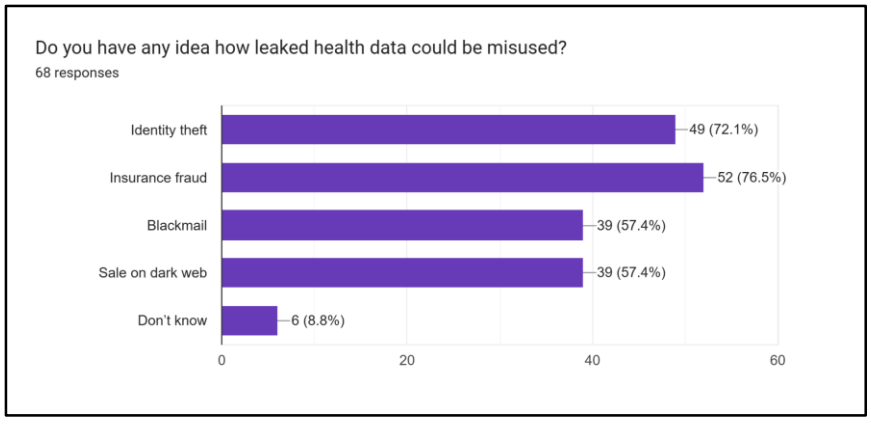
8. Do you think current traditional security methods (firewalls, antivirus, IDS) are enough to protect healthcare data?



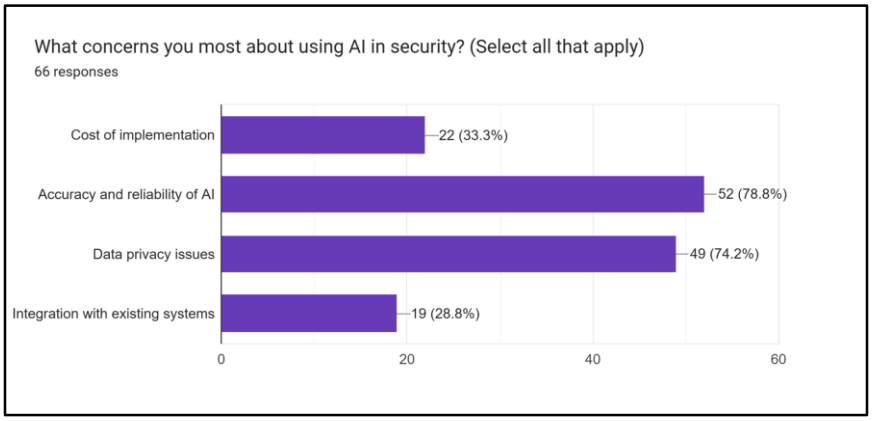
9. What problems do you think exist in current IDS?



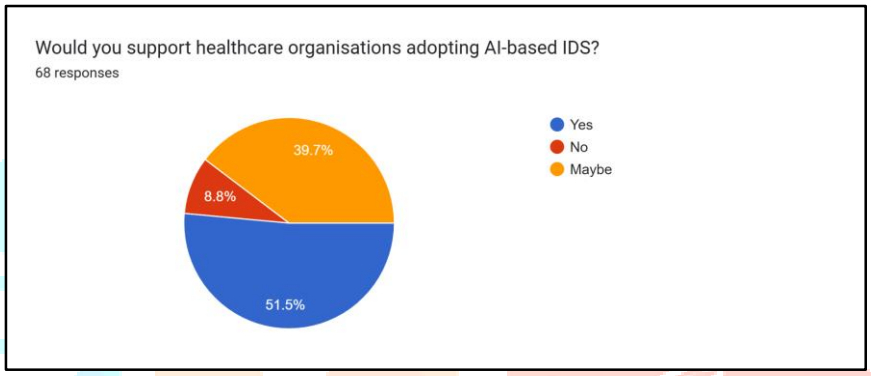
10. Do you think AI-powered IDS could improve healthcare database security compared to traditional IDS?



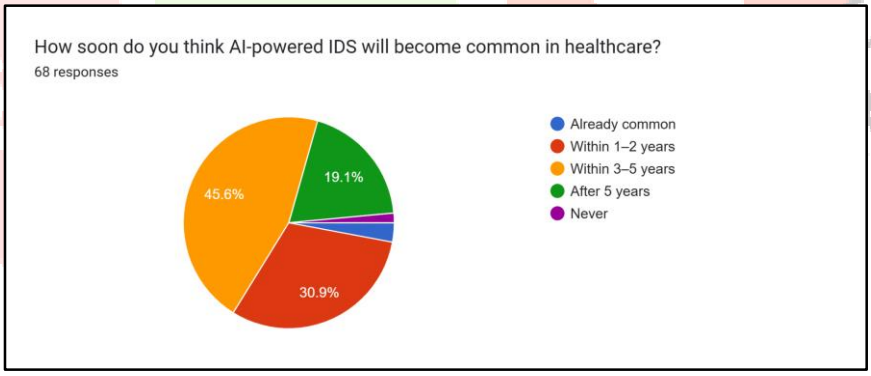
11. What concerns you most about using AI in security?



12. Would you support healthcare organizations adopting AI-based IDS?



13. How soon do you think AI-powered IDS will become common in healthcare?



IX. TESTING

9.1 Descriptive Statistics

Descriptive statistics is a means of describing features of a data set by generating summaries about data samples.

What is your age group	
Mean	3.628571429
Standard Error	0.093630321
Median	4
Mode	4
Standard Deviation	0.783367472
Sample Variance	0.613664596
Kurtosis	2.764809193
Skewness	-1.651993085
Range	4
Minimum	1
Maximum	5
Sum	254
Count	70
Confidence Level(95.0%)	0.18678738

What is your current role	
Mean	1.642857143
Standard Error	0.070595557
Median	2
Mode	2
Standard Deviation	0.590644803
Sample Variance	0.348861284
Kurtosis	0.240067876
Skewness	-0.58070738
Range	3
Minimum	0
Maximum	3
Sum	115
Count	70
Confidence Level(95.0%)	0.140834282

Are you aware that hospitals/healthcare databases in India have faced cyberattacks (e.g., AIIMS ransomware)	
Mean	1.528571429
Standard Error	0.088046262
Median	1
Mode	1
Standard Deviation	0.736647883
Sample Variance	0.542650104
Kurtosis	-0.39294779
Skewness	1.018468257
Range	2
Minimum	1
Maximum	3
Sum	107
Count	70
Confidence Level(95.0%)	0.175647488

How serious do you think a cyberattack on healthcare data can be	
Mean	4.328571429
Standard Error	0.123310829
Median	5
Mode	5
Standard Deviation	1.031692412
Sample Variance	1.064389234
Kurtosis	1.993877059
Skewness	-1.601464898
Range	4
Minimum	1
Maximum	5
Sum	303
Count	70
Confidence Level(95.0%)	0.245998372

How concerned would you be if you found out your personal health/medical data was leaked	
Mean	4.128571429
Standard Error	0.142328213
Median	5
Mode	5
Standard Deviation	1.190803268
Sample Variance	1.418012422
Kurtosis	0.810815164
Skewness	-1.3154676
Range	4
Minimum	1
Maximum	5
Sum	289
Count	70
Confidence Level(95.0%)	0.283937017

Have you heard of Intrusion Detection Systems (IDS) before	
Mean	1.457142857
Standard Error	0.059971402
Median	1
Mode	1
Standard Deviation	0.501756748
Sample Variance	0.251759834
Kurtosis	-2.027867387
Skewness	0.17585273
Range	1
Minimum	1
Maximum	2
Sum	102
Count	70
Confidence Level(95.0%)	0.119639674

Do you think current traditional security methods (firewalls, antivirus, IDS) are enough to protect healthcare data	
Mean	2.514285714
Standard Error	0.06973139
Median	3
Mode	3
Standard Deviation	0.583414665
Sample Variance	0.340372671
Kurtosis	-0.418863465
Skewness	-0.733014404
Range	2
Minimum	1
Maximum	3
Sum	176
Count	70
Confidence Level(95.0%)	0.139110316

Do you think AI-powered IDS could improve healthcare database security compared to traditional IDS	
Mean	2.1
Standard Error	0.117161035
Median	3
Mode	3
Standard Deviation	0.980239545
Sample Variance	0.960869565
Kurtosis	-1.967175421
Skewness	-0.205280824
Range	2
Minimum	1
Maximum	3
Sum	147
Count	70
Confidence Level(95.0%)	0.233729869

Would you support healthcare organisations adopting AI-based IDS	
Mean	1.898550725
Standard Error	0.115220474
Median	1
Mode	1
Standard Deviation	0.957093141
Sample Variance	0.91602728
Kurtosis	-1.911377571
Skewness	0.207807921
Range	2
Minimum	1
Maximum	3
Sum	131
Count	69
Confidence Level(95.0%)	0.229918877

How soon do you think AI-powered IDS will become common in healthcare	
Mean	2.855072464
Standard Error	0.097442493
Median	3
Mode	3
Standard Deviation	0.809418134
Sample Variance	0.655157715
Kurtosis	-0.202013805
Skewness	0.102239786
Range	4
Minimum	1
Maximum	5
Sum	197
Count	69
Confidence Level(95.0%)	0.194443466

X. Significant Outcomes

1. ***Awareness:***
   Most respondents were aware that healthcare systems are frequent targets of ransomware and data theft, but detailed understanding of Intrusion Detection Systems (IDS) was limited, revealing a moderate awareness gap.
2. ***Perception of AI in Cybersecurity:***
   The majority agreed that AI can enhance security and threat detection "to some extent," though complete reliance on automation without human verification was viewed with caution.
3. ***Concerns:***
   Key issues identified were data privacy, lack of explainability, and over-dependence on AI-based tools. Respondents highlighted risks of false alarms and system bias as major limitations of current IDS models.
4. ***Improvements Needed:***
   Participants recommended enhanced transparency, explainable AI (XAI) features, and better adaptability to evolving cyber threats as areas requiring improvement in AI-powered IDS.
5. ***Effectiveness Rating:***
   On a 1–5 scale, most rated AI's threat detection ability as "3" (moderately effective), indicating cautious optimism rather than complete trust.
6. ***Data Safety Confidence:***
   Respondents showed low to moderate confidence (rating 2–3) in the safety of their healthcare data, underlining persistent concerns about cyberattacks and information misuse.

XI. Findings

1. Most respondents were aware of rising cyber threats in healthcare, though few had a clear understanding of how Intrusion Detection Systems (IDS) and AI integration function.
2. Strong concerns were expressed about data misuse, privacy breaches, and the lack of transparency in AI-based decision-making.
3. Participants trusted AI-powered IDS only "to some extent," recognizing its benefits in improving detection accuracy while emphasizing the need for human oversight.
4. Respondents suggested that AI-based IDS should prioritize reducing false alarms, enhancing explainability, and maintaining strong data privacy standards.
5. Overall, the findings indicate that AI-powered IDS is viewed as a necessity rather than an option for ensuring robust cybersecurity and protecting sensitive healthcare data.

XII. Conclusion

This research concludes that AI-powered IDS are not optional but essential for ensuring the cybersecurity of healthcare systems. They offer improved accuracy, faster detection, and the ability to handle new and complex attacks. The hypothesis stands validated, AI can significantly enhance intrusion detection efficiency and reliability in healthcare environments.

XIII. Future Scope

- Develop lightweight AI models for IoT and medical devices.
- Integrate explainable AI to improve transparency in decision-making.
- Conduct real-world testing in hospital networks.
- Explore privacy-preserving AI models like federated learning.
- Promote cybersecurity training for healthcare staff.

XIV. ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my Research Guide, **Dr Divya Premchandran** ma'am, for her constant support, valuable guidance, and encouragement throughout this research. Her insights and feedback have been a great help in completing this paper successfully. I would also like to thank all the respondents who took part in my survey. Their honest and thoughtful responses were very helpful in carrying out this research effectively.

XV. REFERENCES

[1] Z. L. Teo, L. Jin, S. Li, D. Miao, X. Zhang, W. Y. Ng, T. F. Tan, D. M. Lee, K. Chua, J. Heng, Y. Liu, R. S. Mong Goh, and D. S. W. Ting, "Federated machine learning in healthcare: A systematic review on clinical applications and technical architecture," Cell Reports Medicine, vol. 5, no. 2, p. 101419, Feb. 2024. DOI: 10.1016/j.xcrm.2024.101419.

[2] O. Arreche, T. Guntur, and M. Abdallah, "XAI-IDS: Toward Proposing an Explainable Artificial Intelligence Framework for Enhancing Network Intrusion Detection Systems," Applied Sciences, vol. 14, no. 10, art. 4170, 2024. DOI: 10.3390/app14104170.

[3] G. Balhareth and M. Ilyas, "Optimized Intrusion Detection for IoMT Networks with Tree-Based Machine Learning and Filter-Based Feature Selection," Sensors, vol. 24, no. 17, art. 5712, 2024. DOI: 10.3390/s24175712.

[4] A. K. M. I. Newaz, A. K. Sikder, M. A. Rahman and A. S. Uluagac, "HealthGuard: A Machine Learning-Based Security Framework for Smart Healthcare Systems," arXiv:1909.10565, Sep. 2019.

[5] K. G. R. Narayan, S. Mookherji, V. Odelu, R. Prasath, A. C. T. Turlapaty and A. K. Das, "IIDS: Design of Intelligent Intrusion Detection System for Internet-of-Things Applications," arXiv:2308.00943.

[6] M. A. Shyaa, "Evolving cybersecurity frontiers: A comprehensive survey on concept drift and feature dynamics aware machine and deep learning in intrusion detection systems," Eng. Appl. Artif. Intell., 2024. (survey on drift and IDS).

[7] J. Doménech et al., "Ensuring patient safety in IoMT: A systematic literature review," (ScienceDirect/Elsevier), 2024. (systematic review on IoMT safety and security).

[8] F. Zhang et al., "Recent methodological advances in federated learning for healthcare applications," (review), 2024. DOI/Publisher page: see the review on SciDirect / AIP (methodological FL advances).

[9] S. G. Finlayson et al., "Adversarial attacks on medical machine learning," Science, vol. 363, no. 6433, pp. 1287–1289, 2019. DOI: 10.1126/science.aaw4399.

[10] S. Sharma, "A Systematic Study of Adversarial Attacks Against Network Intrusion Detection Systems," Electronics, 2024.

[11] Canadian Institute for Cybersecurity, "CIC-IDS2017: Intrusion Detection Evaluation Dataset," University of New Brunswick (UNB).

[12] Explainable AI IDS survey / arXiv surveys on XAI for IDS and Industry 5.0; • Adversarial NIDS surveys (arXiv 2024).