Journal of Information, Technology and Data Science

Cybersecurity and Artificial Intelligence of Things (AIoT) in Education: Enhancing Security in Smart Learning Environment

Sharaf M. Kannooz & Preethi E.

ISSN: 2617-3573

Stratford Peer Reviewed Journals and Book Publishing
Journal of Information, Technology and Data Science
Volume 10||Issue 1 ||Page 35-55||May|2026|
Email: info@stratfordjournals.org ISSN: 2617-3573

Cybersecurity and Artificial Intelligence of Things (AIoT) in Education: Enhancing Security in Smart Learning Environment

[1*]Sharaf M. Kannooz & [2]Preethi E.
[1]Research Scholar; kannoozvision@gmail.com
[2]Research Faculty, British Training Centre, UAE; preethiebi@gmail.com
***Corresponding author: Sharaf M. Kannooz**

How to cite this article: **Kannooz, S. M., & Preethi, E. (2026). Cybersecurity and Artificial Intelligence of Things (AIoT) in Education: Enhancing Security in Smart Learning Environment.** ***Journal of Information, Technology and Data Science, 10*** **(1), 35-55. https://doi.org/10.53819/81018102t5429**

Abstract

Cybersecurity (CS), Artificial Intelligence (AI), and the Internet of Things (IoT) are revolutionizing education by enabling adaptive learning systems and smart educational tools. The integration of AI and IoT, known as Artificial Intelligence of Things (AIoT), offers transformative possibilities but also introduces significant cybersecurity risks. Protecting AIoT-enabled devices and systems is essential to ensure secure and efficient educational environments. This research aims to address cybersecurity challenges in AIoT-enabled educational tools and adaptive learning systems. It investigates user security behaviours, evaluates threats, and compares the effectiveness of AIoT-based and traditional cybersecurity approaches. The study utilized a mixed-methods approach, collecting data by qualitative analysis of archival data, opinion & guidelines of industrial experts and via online and offline surveys of 10,024 educational participants around the globe to understand the relationship between user behaviours and cybersecurity threats in education. A machine learning-based AI model was developed to detect anomalies with high precision, and case studies were conducted to analyse real-world cybersecurity scenarios in educational contexts. The study proposed a Cyber-AIoT Solution for a Smart Learning Environment (SLE). The results demonstrated that the AI model effectively mitigates cybersecurity threats, ensuring intelligent mobility and secure operations within educational systems. The findings highlight the applicability of AIoT in creating robust and secure educational ecosystems. The research emphasizes the importance of safeguarding AIoT-enabled tools in education, providing a practical framework to address vulnerabilities and enhance security in smart learning environments. Future work should focus on developing globally scalable cybersecurity solutions, enhancing AI-driven threat detection, and fostering collaboration among educational institutions and technology providers to build secure and resilient smart Learning systems.

Keywords: *Cybersecurity, Artificial Intelligence of Things, Education, Security, Smart Learning Environment*

1.0 Introduction

The term "S.M.A.R.T" stands for Showing, Manageable, Accessible, Realtime Interactive, and Testing (Huang, Su, & Pao, 2019) and refers to a setting carefully constructed digital tools and resources to encourage student connection on enhanced face-to-face, online, virtual reality interactions in real time, and record the collective knowledge of the entire class (Lui *et al* 2014) to make smart learning environment. A smart learning environment is defined as a combination of several high-end technologies that aim to assist educators and students in optimising their overall leaning experiences (Mircea, Stoica, & Ghilic-Micu, 2021). Although a smart learning environment combines technology with other elements, such as teaching strategies and classroom models, in this paper is focus our attention on the technological dimension of a smart learning environment. The Artificial Intelligence (AI) combined with emerging technologies having the form of interactive, remote, and mobile computing in physical and virtual environments constitutes an evident trend in the development of the concept of smart learning environment. The term "Artificial Intelligence" (AI) was first mentioned by John McCarthy in 1956 and refers to the ability of computer systems to undertake human tasks (like learning and thinking) that frequently can only be attained through human intelligence. Focusing on IoT, the lessons from AI education gaps can improve IoT teaching methods. This approach prepares students for a future where AI and IoT are intricately linked within society and industry (Abichandani *et al*., 2022).

Cybersecurity means enhancing the awareness and knowledge of non-expert end users. The term "cybersecurity awareness" refers to "an approach to train internet users to be sensitive to the different kinds of cyberattacks and the vulnerability of data and computers to these threats ". Cybersecurity is a technological issue that is exacerbated by non-expert end users who interact with internet content (Zhang-Kennedy, & Chiasson, 2021). Despite this, many netizens are still not sufficiently aware of the numerous internet threats. This is even though internet consumption is rising drastically as a result of information technology advancements (Maurseth, P.B.2018). Cybersecurity Triad: The concept of cybersecurity triad [CIA] derived from Chalubinska - Jutkiewicz (2021), Kesan & Zhang (2019), Norris and (2021). According to them CIA having three parts though which we can protect and secure data from attackers. They are, Confidentiality**:** Which includes safeguarding sensitive data from unauthorised access to ensure privacy and protection. Integrity**:** Maintaining the authenticity, accuracy and consistency of data

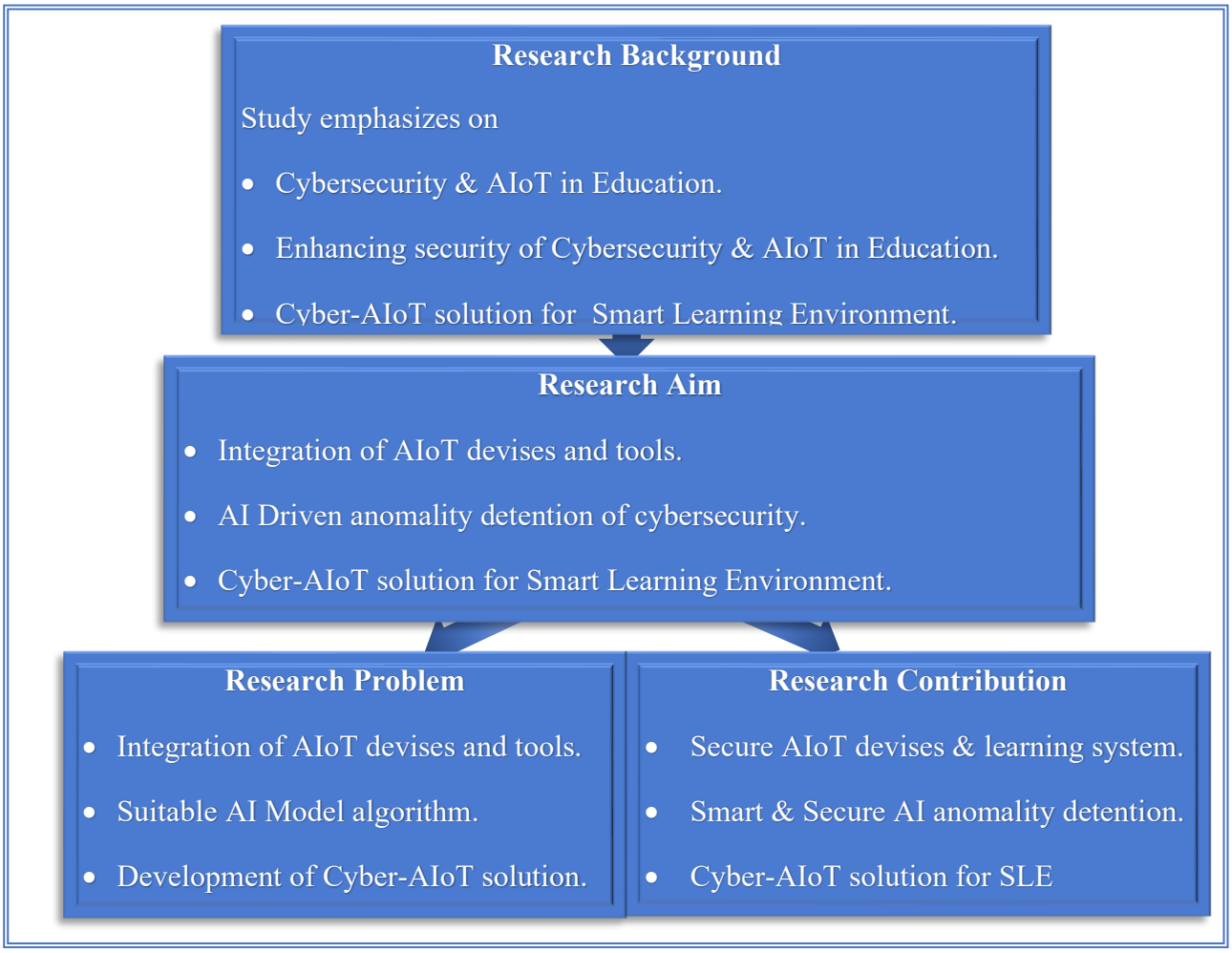
over its entire lifecycle. Availability: Ensuring timely and reliable access to data and resource for authorised users when needed.

Artificial Intelligence (AI) and the Internet of Things (IoT) have emerged technologies in recent times, transforming various industries and revolutionising the way we interact with the world. In the field of education, these technologies hold immense potential to reshape traditional learning and teaching methodologies, opening up new possibilities for personalised and efficient education (J. Robert *et al*., 2022). The convergence of AI and IoT has given rise to the concept of Artificial Intelligence of Things (AIoT), which combines the power of intelligent decision making with the vast network of interconnected devices and sensors AIoT, and these technologies to create intelligent systems capable of making autonomous decisions and interacting with the environment (A. Arsenio *et al*., 2014). The threats to AIoT**:** Thread AI emerge from stealth to help enterprises design, implement, and manage AI Workflows. Thread to AIoT may developed from all the process of data, application, networks and storage stages of an organisation. The unauthorized access to systems, data leakage, or physical harm, have a great influence. One of the major threats involves unauthorized access to AIoT devices and networks. This means access to the system through exploited software vulnerabilities, poor passwords, or no encryption, attackers would successfully get hold of it, after which they can steal information, disrupt devices, or use them as a part of a botnet to attack other systems.

The key technologies related to smart learning environment are, AIoT Architecture, Smart school, Smart Classroom, Computer vision-based surveillance, E-learning platforms, Smart student performance assessment/prediction, The role of AI for VR, AR and MR in education etc. Educational institutions are prime targeted for cybercriminals on a number of reasons, primarily for the amount of personal student data that they handle, along with student loan information, confidential research data, and a lack of adequate cybersecurity. Data must then be protected in order to maintain confidentiality, integrity and availability. Protecting against data manipulation, fraudulent user authentication and compromises in confidentiality are important security issues in e- Learning. Education is a prime target for cybercriminals. Educational institutions worldwide have become a hotbed for cybercrime, with a 75% year-over-year increase to 3,574 weekly attacks according to Check Point's the State of Cyber Security 2025 report.

Research Background

The picture No. 1 explains the summary of research background with the following, research background, Research Aim, Research problem and research contribution. Research background emphasis the studies, research surveys and case studies with real world scenarios and industrial expert's opinion about this research. The research aim focused on the output which the research is expecting throughout the research. Research problem emphasises on the difficulties faced during the research and research contribution is the final result of the research.



Picture No. 1: Research Background

This research emphasizes on Cybersecurity & AIoT in education, enhancing security of cybersecurity & AIoT in SLE and develop a Cyber-AIoT solution in Smart Learning Environment. Research Aim: Integration of cybersecurity & AIoT devises and tools, AI- driven anomality detention of cybersecurity& AIoT, Through the case studies to analyses real-world cybersecurity scenarios in education and develop a Cyber-AIoT solution in Smart Learning Environment. Research Problem: Integration of AIoT devises and tools, Suitable AI Model

algorithm. Secure Cybersecurity & AIoT Architecture and Development of Cyber-AIoT solution. Research Questions: QR1A: What are the prevalent cybersecurity threats, vulnerabilities, and risks in Smart Learning Environment, and QR1B: How do AI based approaches compare to traditional methods in addressing these challenges? QR2: What are the key ethical and technical challenges and considerations related to integrating AIoT devices and tools into traditional cybersecurity methods in education? QR3A: What are the most effective AI techniques for promoting cybersecurity in SLE, QR3B: How do integrate AIoT devices and tools without any vulnerability and QR3C.Which way to evolve a smart Cyber-AIoT solution in a Smart Learning Environment? Research Contribution: Secure AIoT devises & learning system, Smart & Secure AI driven anomality detention, Cyber-AIoT solution in Smart Learning Environment & Smart & Secure Smart Learning Environment.

As concerns about malicious threats and violence in Smart learning Environment become more common (Cohen, 2021), more comprehensive approaches are necessary to enhance safety and security in a variety of educational settings, including smart classrooms (Lamoreaux & Sulkowski, 2019, 2020). As crime and violence become growing concerns in educational settings (Casteel & Peek-Asa, 2000), applications examining threat reductions of this type separate from those examining system function or behavioural learning standards are necessary for comprehensive threat risk management and security enhancement efforts (Blokland & Reniers, 2019). The major key technologies related to Smart Learning Environment are AIoT Architecture, Virtual reality, Smart classroom, E-learning platforms, E-learning platforms, Robotics, Educator performance assessment, Computer vision-based surveillance, Smart student performance prediction etc.

2.0 Literature Review

Despite the promising potential of AIoT platforms in improving teaching and learning at various educational levels of a smart learning environment (Tsai *et al*., 2022; Zhang *et al*., 2021), they also present unique challenges. This study specifically focuses on university-level technology students, who are pivotal in advancing AIoT technology. This study explored a novel AIoT educational platform tailored to enhance the AI. This platform provided an interactive learning environment that integrates practical AI applications, effectively addressing the educational gaps often found in traditional AI adequately link theoretical knowledge to real-world applications. Given the growing industry demand for AI and IoT proficient professionals, an innovative AIoT

educational platform is crucial. It merges theoretical knowledge with practical application, promising transformative educational and operational capabilities.

Research Gap: In recent years the importance of security enhanced cybersecurity & AIoT has been a hot topic in the field of smart learning environment. Although a lot of study has been done in this field there are still some big questions that need to be answered. In particular the relationship between cybersecurity & AIoT and security enhancement for smart learning environment has received little attention from researchers. Research gap with research findings and Research gap with research citation of cybersecurity and were studied during this research.

Research hypothesis: Research hypothesis is the emphatical formulate of the entire research in which every step of process is mentioned and analyses to filter the result. Research hypothesis plays a crucial part of every research. Hypothesis related to cybersecurity & AIoT in education] AI-Driven cybersecurity effectiveness, AIoT vulnerabilities and solutions & Educational outcomes and ethics] Hypothesis related to cybersecurity Algorithms & AIoT model and Hypothesis related to security enhanced smart learning environment. Theoretical framework: The theoretical framework is based on a synergistic combination of multidisciplinary theories. These were carefully selected to thoroughly investigate how AI-enabled anomaly detection affects cybersecurity in the complex setting of smart learning environment. Theory of complex adaptive systems (CAS) (Holland, 1995) and the three other theories: TAM, or Technology Acceptance Model (Davis, 1989), Theory of Planned Behaviour (Ajzen, 1991), and the theory of socio-technical systems (Emery & Trist, 1960).

Understanding of Security Enhanced Cybersecurity & AIoT in Education is one of the major tasks to know the capabilities and benefits of security enhancement on this field. This study presents some defined study models for the understanding of security enhanced cybersecurity and AIoT through smart learning environments. This research investigates user security behaviours, evaluates threats, and compares the effectiveness AIoT based cybersecurity approaches.

- Artificial intelligence in cybersecurity [Automated Thread Detention, Enhanced Risk Management, Phishing Prevention, Incident Response, User Behaviour Analytics & Security Intelligence.]
- Machine learning application for thread detention [Anomaly Detention, Behavioural Analysis, Automated Response, Spam Filtering, Malware Classification, Data Breach Prediction& Security Score analysis.]

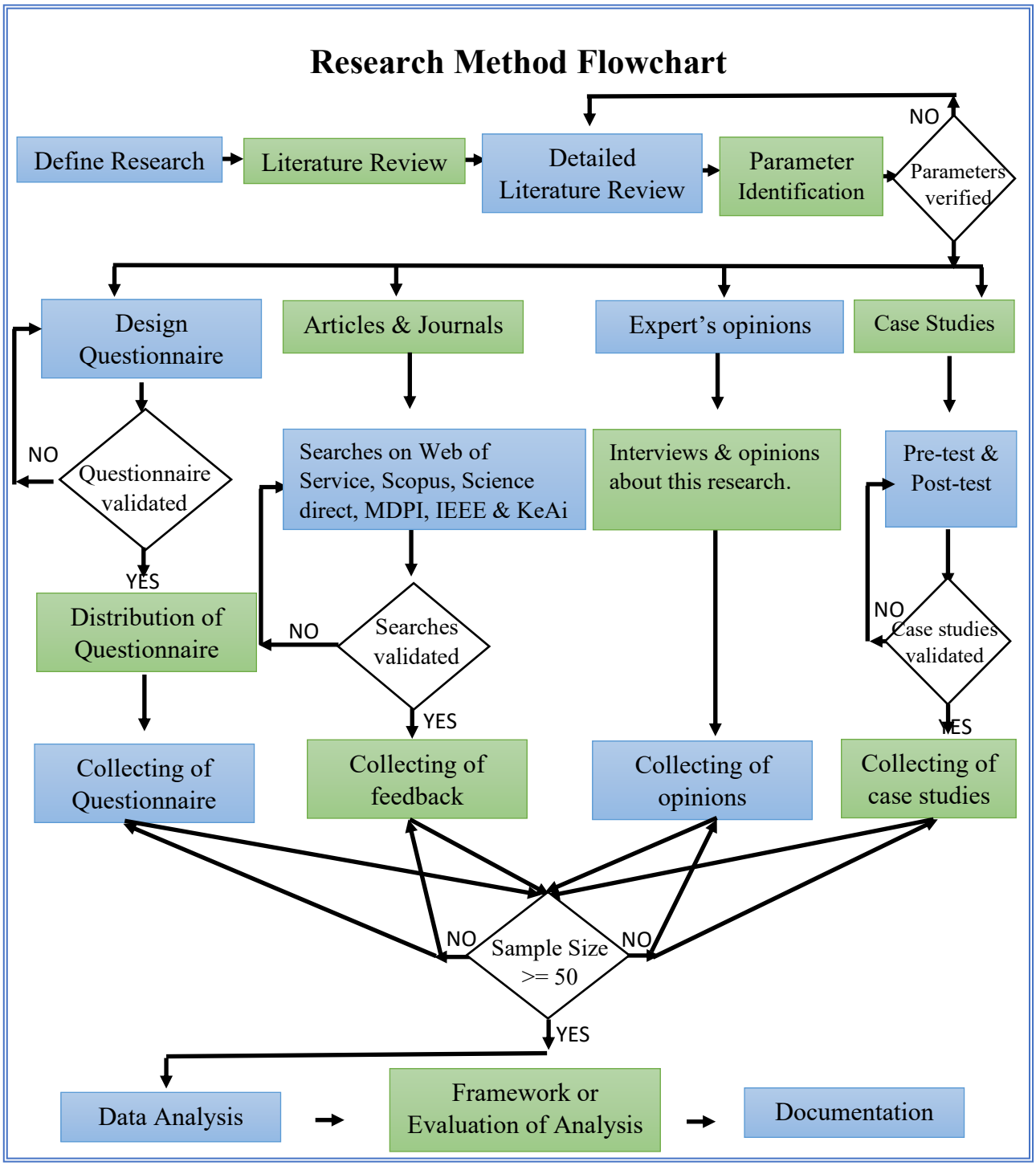
- Cybersecurity Risk Management Strategies [Cybersecurity risk management strategies involve a continuous cycle of identifying assets, assessing risks, implementing controls to mitigate threats, and monitoring for effectiveness.]
- Vulnerability Assessment and penetration test] Go beyond surface-level scans with penetration testing that combines AI-powered offensive scanning with in-house certified expert-led pen tests that cover all APIs under the same domain.]
- Incident response and management Framework [An incident response and management framework are a structured process that guides organizations handling cybersecurity events, from preparation and detection to containment, eradication, and recovery.]
- Role of training and awareness program [Training and awareness programs are crucial for equipping employees with the necessary knowledge and skills to perform their jobs effectively and safely, fostering a positive organizational culture, and protecting company assets.]

Before going to select the AI-Model, we must understand and provide security of the following; Artificial Intelligence in cybersecurity Enhanced Threat Detection, AI can quickly analyse data and identify potential threats by detecting patterns and anomalies, such as unusual network traffic or suspicious user behaviour, often indicating malware, phishing, or other cyber-attacks (Zhang, Chen, Hu, & Wang, 2022). AIoT has revolutionized the educational sector, by integrating AI, encompassing both ML and DL techniques. The data generated from various processes, devices, sensors, and machines are processed for intelligent decision-making. This processing includes activities such as data analysis, modelling, and labelling. AI techniques, particularly ML and DL, are crucial in this context. Specifically, ML techniques can be classified into supervised, unsupervised, and semi-supervised learning, which mainly solves the clustering, regression, and classification problems (Xu, Yu, Griffith & Golmie, 2018).

The most crucial part of this research is how to integrate AIoT tools, system and its protection. As educational institutions increasingly integrate Artificial Intelligence of Things (AIoT) into their learning systems, security for these devices becomes paramount. AIoT-enabled educational devices like smartboards, VR headsets, AI tutors, and connected learning tools provide innovative teaching methods but also introduce unique cybersecurity challenges (Bajaj & Sharma 2018). Smart educational environments powered by Artificial Intelligence of Things (AIoT) leverage connected devices and AI to create personalized, efficient learning experiences. (Baidoo Anu & Owusu Ansah, 2023).

3.0 Research Method

The research method refers to the overall strategy that this research is carried out and also explains the step by step process of this entire research of cybersecurity and AIoT in Education; Enhancing security in smart learning environment & picture No.2 explains in details.

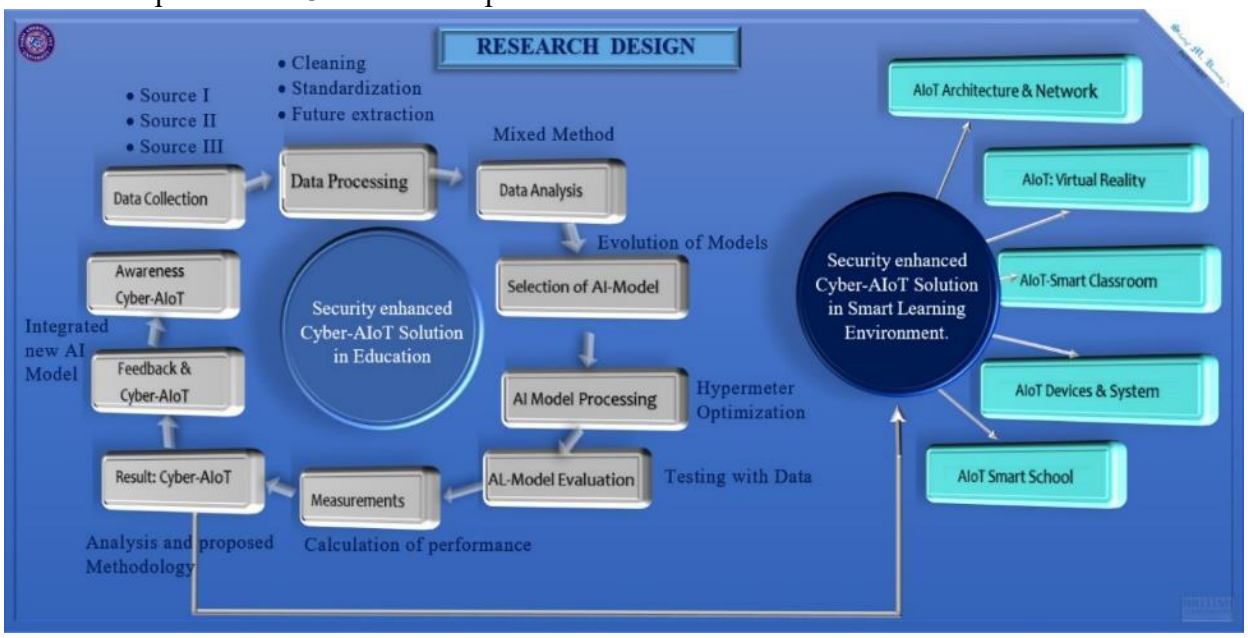


Picture No. 2: Research method flowchart.

Stratford Peer Reviewed Journals and Book Publishing
Journal of Information, Technology and Data Science
Volume 10||Issue 1 ||Page 35-55||May|2026|
Email: info@stratfordjournals.org ISSN: 2617-3573

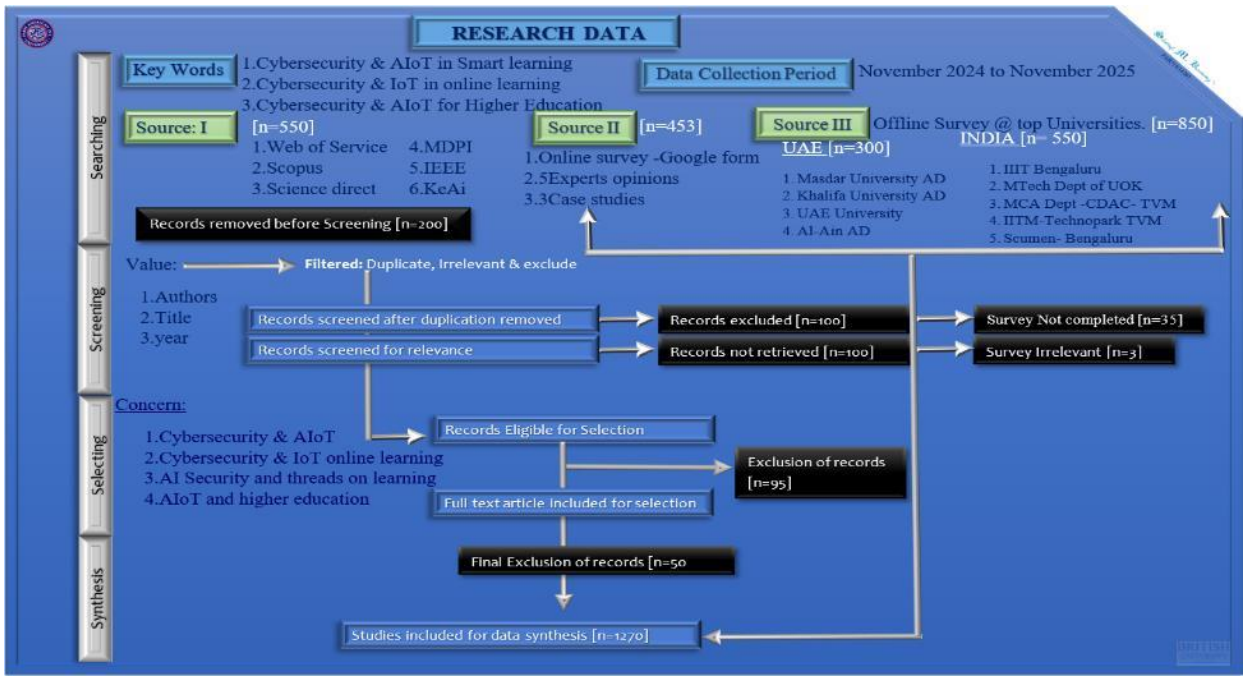
Research Design

The research design refers to the overall strategy that you choose to integrate the different components of the study in a coherent and logical way, thereby, ensuring all effectively address the research problem; it constitutes the blueprint for the collection, measurement, and analysis of data and picture No. 3 shows each process in details.



Picture No. 3: The research design of Cybersecurity and AIoT in SLE.

Data Collection procedure



Picture No 4: The data Collection of Cybersecurity and AIoT in SLE.

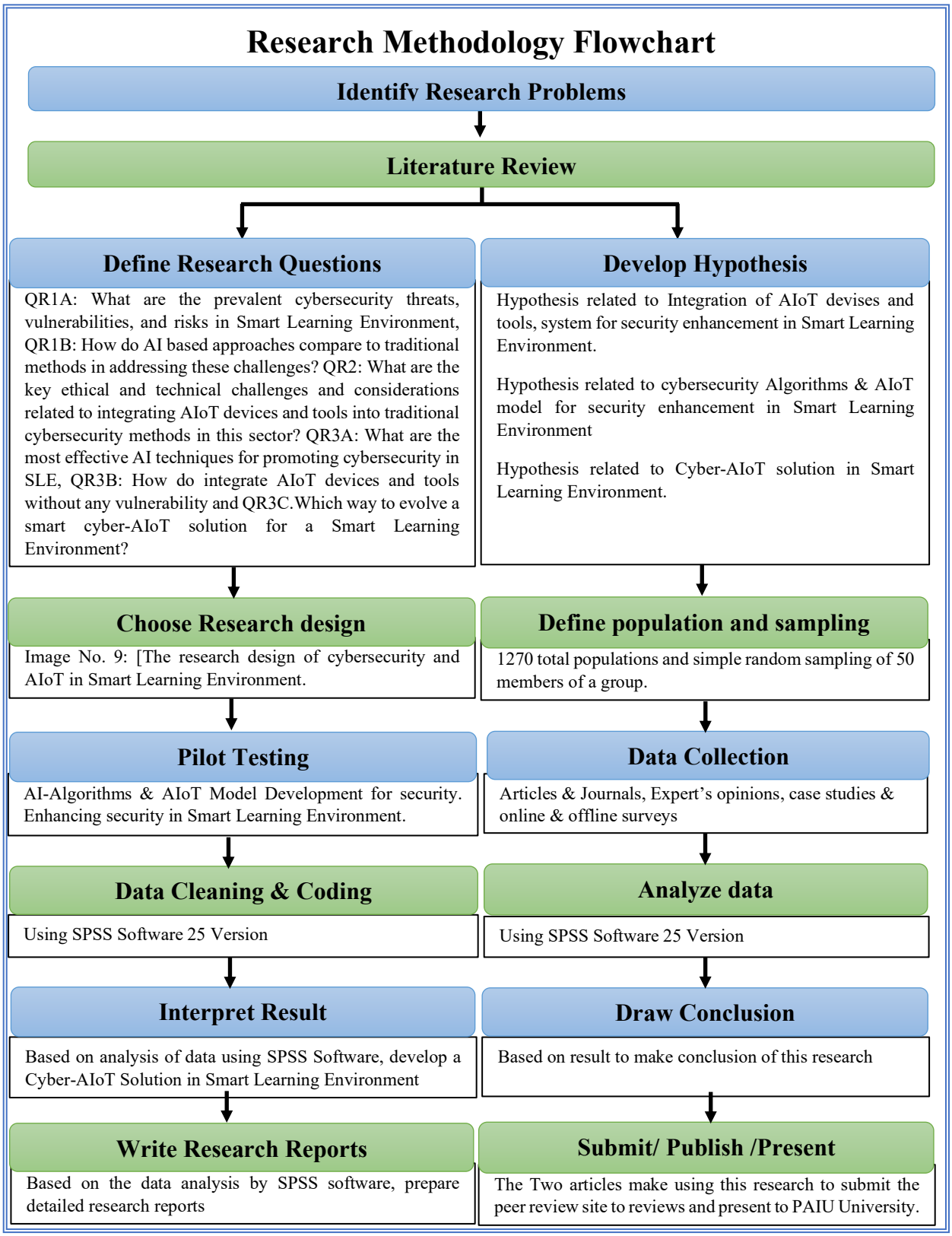
Data collection is the process of gathering and measuring information on variables of interest in an established systematic fashion that enables one to answer stated research questions, test hypotheses, and evaluate outcomes. For this research study the data gathered by different approaches of sources. The pictures No. 4 & 5 explained the details of data collection.

Data Collection	Selection based on research methods			
	Articles & Journals	Expert's opinions	Case Studies	Surveys
	Searches from Web of Service, Scopus, Science direct, MDPI, IEEE & KeAi	Interviews & professional experiences and opinions about this	Pre-test & Post-test of case studies.	Sampling surveys, Questionnaire development & Full-fledged surveys
	Theoretical study	Pilot study	Pilot study	Pilot study

Source I: Search	Cybersecurity & AIoT in Smart learning, Cybersecurity & IoT in online learning & Cybersecurity & AIoT for Higher Education.
Source II: Expert's opinion, Case studies & Online Survey.	ADCO, HCT & Masdar university's expert's opinions were collected, studied, analysed and developed a Cyber-AIoT solution.
	Case Study I: Cybersecurity in AIoT enabled learning devises Case Study II: Cybersecurity in AIoT of educational tools and adaptive learning systems
	https://docs.google.com/forms/d/1Ga6lFndH2Ygeq8VDkKysm63zzzVQalXmEZ7NINAOX04/viewform?pli=1&sharingaction=ownershiptransfer&ts=677a94dc&pli=1&edit_requested=true
Source III: Offline	IND: Scumen- Bengaluru, IIIT Bengaluru, MCA Dept -CDAC- TVM, IITM-Technopark TVM & UAE: Khalifa University, Al-Ain University &Masdar

Picture No.5: The data collection process of Cybersecurity and AIoT in SLE

The picture No. 6 explains details about this research's research methodology steps by step. Which includes research problem identification, literature review, methodology design, data analysis and AI modelling, solution development,



Picture No 6: Research methodology Flow chart.

Population and sampling: Sampling Method: We used simple random sampling to select a representative group of respondents. This method ensured that every member of the population

had an equal chance of being included, enhancing the study's external validity. Sample Size: The sample size included 50-100 students, both male and female, aged 18-32 years. Population: Total 2000 records were collected by data collection method, among these 1270 population records were selected for the analysis.

Data analysis. Data Analysis is the process of systematically applying statistical and/or logical techniques to describe and illustrate, condense and recap, and evaluate data. In this research, data collected were done by Mixed method and data analysed by using SPSS software version 25.

Statistical Techniques: We employed various statistical techniques, including: ANOVA: To compare mean scores across different groups. Chi-square test: To examine relationships between categorical variables. Correlation analysis: To measure the strength and direction of relationships between variables. Regression analysis: To predict outcomes based on independent variables. Frequency table: The normal statistical techniques for data.

Data analysis by SPSS software Ver.25

1. Frequency Table	**Demographic information**
2. Chi-Square Test	Hypotheses related to the cybersecurity strategies aligned with AIoT in SLE, Hypotheses related to the Benefits of AI in Security Automation in SLE & Hypothesis related to the roll and Impact of AI & Cybersecurity in SLE.
3. Pearson Correlation Analysis	Hypothesis related to Cybersecurity & AIoT in Education, Hypothesis related to AIoT powered enhancing security in SLE & Hypothesis related to the Cyber-AIoT Solution in SLE.
4. Two-way ANOVA Test	Hypothesis of AI Algorithms & AIoT Model based real time protection in SLE & Hypotheses related to AI Transparency, AI attacks on Data poisoning & Traditional data process methods of enhancing security in smart learning environment.
5. Multiple Linear Regression Test	Hypotheses related to Cybersecurity & AIoT in Education: Enhancing security by Slicing & Scheduling techniques in SLE.
6. Independent Samples Test	Hypotheses related to Cyber-AIoT solution in Smart learning environment.
7. One-way ANOVA Test	Hypothesis related to the combined impact of virtual reality devices, e-learning platforms, virtual reality educators in SLE.
8. Mean Square analysis	The hypotheses related to the overall context of Cybersecurity & AIoT in Education: Enhancing security in Smart Learning Environment.

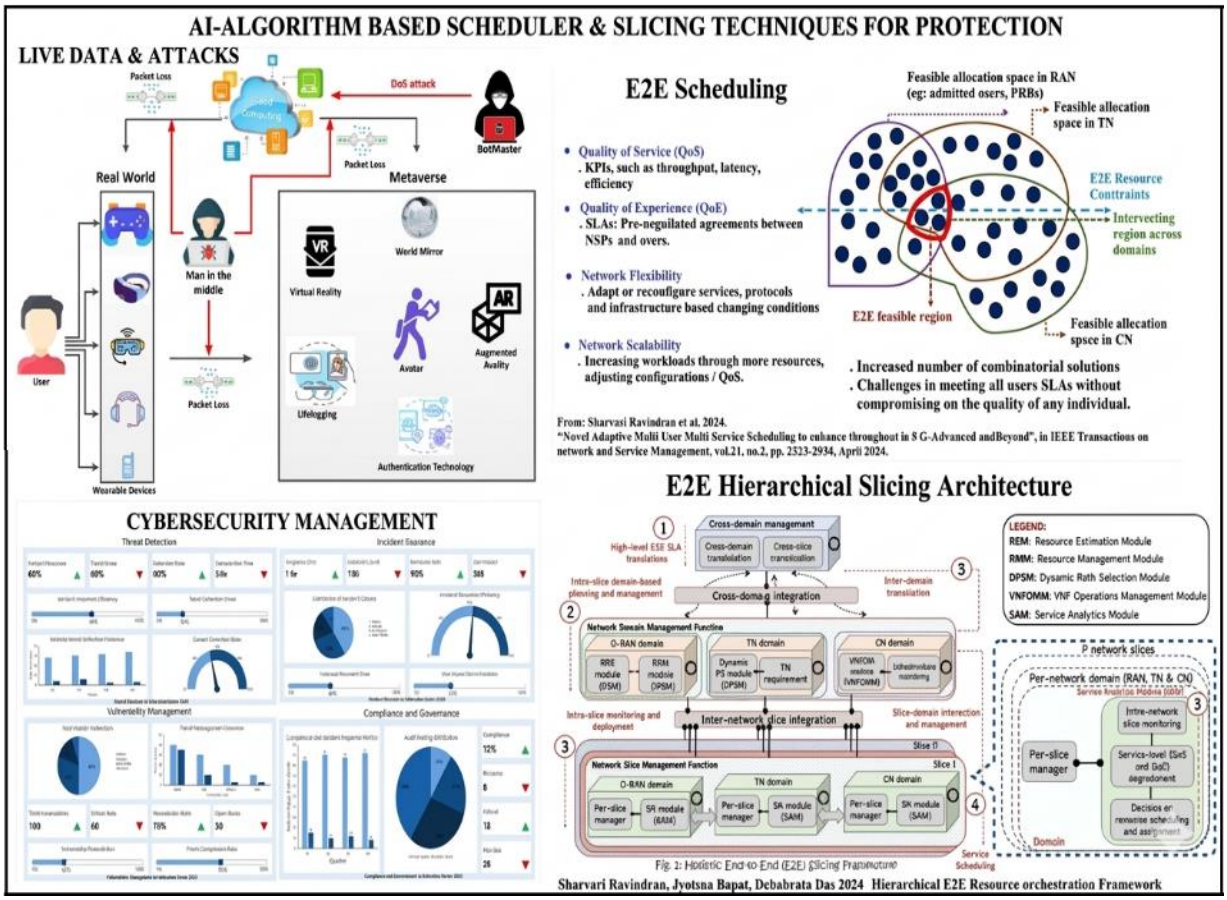
Picture No 7: Data Analysis by SPSS software Ver.25

Stratford Peer Reviewed Journals and Book Publishing
Journal of Information, Technology and Data Science
Volume 10||Issue 1 ||Page 35-55||May|2026|
Email: info@stratfordjournals.org ISSN: 2617-3573

4.0 Findings

Mechanism of security enhancement in smart learning environment by AI-algorithm based Scheduler & Slicing techniques

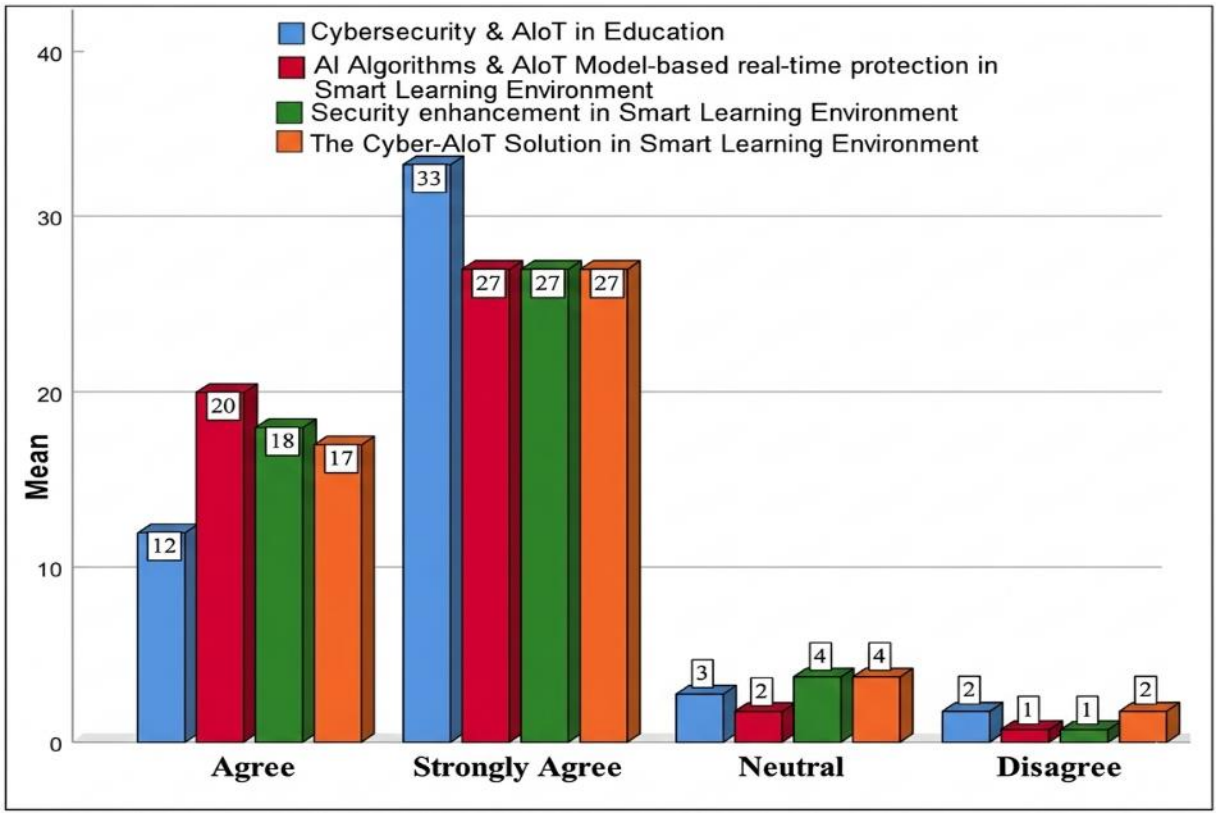
The Network slicing is an architecture technique that creates multiple, isolated virtual networks on top of a single shared physical infrastructure.It enables tailored, end-to-end logical networks each optimized for specific performance needs like latency, speed, and capacity to run simultaneously on the same hardware. A Scheduler is ensuring that network packets are transmitted vis the system network resources in the most efficient manner for maintaining quality of services (QoS), quality of experience (QoE), Network flexibility & Network scalability? It includes.. AI algorithm based scheduling and slicing techniques for protection, Scheduling mechanism in virtualisation of shared resources. Scheduling algorithm for propositional fair with rate guarantee (PF-RG) &Joint schedule with buffer of data flow is handled. The picture No.8 explained the Live data and its protection, Cybersecurity management during live data transmission, how the seducing of data packets transmitted and sliding hierarchical architecture (Sharvari Ravindren *et al*, 2024).



Picture No.8: AI-algorithm based Scheduler & Slicing techniques for protection

The hypotheses related to the overall context of cybersecurity & AIoT in Education: Enhancing security in smart learning environment.

Null Hypothesis (H0): There is not a significant factor in the overall context of cybersecurity & AIoT in Education: Enhancing security in smart learning environment. Alternative Hypothesis (H1): There is a significant factor in the overall context of cybersecurity & AIoT in Education: Enhancing



Picture No.9: Respondents' Perceptions of Cybersecurity and AIoT-Based Security Enhancement in Smart Learning Environments

The provided mean square group statistics test results compare the responses of male and female participants on four different statements related to Cybersecurity & AIoT in Education: Enhancing security in Smart Learning Environment.

- Do you agree that Cybersecurity & AIoT in Education play a crucial role in Enhancing security in Smart Learning Environment?
    - Male (N=30): Mean = 21.13 Std. Deviation = 1.103 Std. Error Mean = 0.207
    - Female (N=20): Mean = 21.40 Std. Deviation = 1.503 Std. Error Mean = 0.43
- Do you agree that AI Algorithms & AIoT Model based real time protection play a crucial role in Enhancing security in Smart Learning Environment?

Stratford Peer Reviewed Journals and Book Publishing
Journal of Information, Technology and Data Science
Volume 10||Issue 1 ||Page 35-55||May|2026|
Email: info@stratfordjournals.org ISSN: 2617-3573

- Male (N=30): Mean = 21.93 Std. Deviation = 1.143 Std. Error Mean = 0.209
- Female (N=20): Mean = 21.80 Std. Deviation = 1.543 Std. Error Mean = 0.0.43

- Do you agree that Security enhancement in Smart Learning Environment play a crucial role?
  - Male (N=30): Mean = 18.93 Std. Deviation = 0.943 Std. Error Mean = 0.109
  - Female (N=20): Mean = 20.70 Std. Deviation = 1.243 Std. Error Mean = 0.503
- Do you agree that The Cyber-AIoT Solution play a crucial role in Smart Learning Environment?
  - Male (N=30): Mean = 19.91 Std. Deviation = 1.042 Std. Error Mean = 0.105
  - Female (N=20): Mean = 20.30 Std. Deviation = 1.441 Std. Error Mean = 0.243

Age Experience * Cybersecurity & AIoT in Education

Report

Cybersecurity & AIoT in Education		Age	Experience
Agree	N	12	12
	Mean	22.50	1.67
	Std. Deviation	1.087	.778
Neutral	N	4	4
	Mean	21.50	1.50
	Std. Deviation	1.000	1.000
Strongly Agree	N	33	33
	Mean	21.67	1.45
	Std. Deviation	1.362	.869
Disagree	N	1	1
	Mean	23.00	3.00
	Std. Deviation	.	.
Total	N	50	50
	Mean	21.88	1.54
	Std. Deviation	1.304	.862

Measures of Association

	Eta	Eta Squared
Age * Cybersecurity & AIoT in Education	.309	.095
Experience * Cybersecurity & AIoT in Education	.266	.071

ANOVA Table

		Sum of Squares	df	Mean Square	F	Sig.
Age * Cybersecurity & AIoT in Education		7.947	3	2.649	1.62	.198
		75.333	46	1.638		
		83.280	49			
Experience * Cybersecurity & AIoT in Education		2.572	3	.857	1.16	.333
		33.848	46	.736		
		36.420	49			

Age Experience * Security enhancement in Smart Learning Environment

Report

Security enhancement in Smart Learning Environment		Age	Experience
Agreee	N	21	21
	Mean	22.24	1.57
	Std. Deviation	1.136	.746
Neutral	N	1	1
	Mean	21.00	1.00
	Std. Deviation	.	.
Strongly Agree	N	27	27
	Mean	21.59	1.48
	Std. Deviation	1.394	.935
Disagree	N	1	1
	Mean	23.00	3.00
	Std. Deviation	.	.
Total	N	50	50
	Mean	21.88	1.54
	Std. Deviation	1.304	.862

Measures of Association

	Eta	Eta Squared
Age * Security enhancement in Smart Learning Environment	.289	.083
Experience * Security enhancement in Smart Learning Environment	.264	.070

ANOVA Table

		Sum of Squares	df	Mean Square	F	Sig.
Age * Security enhancement in Smart Learning Environment		6.952	3	2.317	1.397	.256
		76.328	46	1.659		
		83.280	49			
Experience * Security enhancement in Smart Learning Environment		2.536	3	.845	1.148	.340
		33.884	46	.737		
		36.420	49			

Stratford Peer Reviewed Journals and Book Publishing
Journal of Information, Technology and Data Science
Volume 10||Issue 1 ||Page 35-55||May|2026|
Email: info@stratfordjournals.org ISSN: 2617-3573

Age Experience * AI Algorithms & AIoT Model based real time protection in SLE

Report

AI Algorithms & AIoT Model based real time protection in SLE		Age	Experience
Agree	N	20	20
	Mean	22.3	1.60
	Std. Deviation	1.13	.754
Neutral	N	2	2
	Mean	21.0	1.00
	Std. Deviation	.000	.000
Strongly Agree	N	27	27
	Mean	21.6	1.48
	Std. Deviation	1.39	.935
Disagree	N	1	1
	Mean	23.0	3.00
	Std. Deviation	.	.
Total	N	50	50
	Mean	21.9	1.54
	Std. Deviation	1.30	.862

Measures of Association

	Eta	Eta Squared
Age * AI Algorithms & AIoT Model based real time protection in SLE	.321	.103
Experience * AI Algorithms & AIoT Model based real time protection in SLE	.281	.079

ANOVA Table

		Sum of Squares	df	Mean Square	F	Sig.
Age * AI Algorithms & AIoT Model based real time protection in SLE	Between Groups	8.561	3	2.854	1.76	.169
	Within Groups	74.719	46	1.624		
	Total	83.280	49			
Experience * AI Algorithms & AIoT Model based real time protection in SLE	Between Groups	2.879	3	.960	1.32	.281
	Within Groups	33.541	46	.729		
	Total	36.420	49			

Age Experience * the Cyber-AIoT Solution in SLE

Report

Cyber-AIoT Solution in SLE		Age	Experience
Agree	N	19	19
	Mean	22.26	1.58
	Std. Deviation	1.147	.769
Neutral	N	3	3
	Mean	21.67	1.33
	Std. Deviation	1.155	.577
Strongly Agree	N	27	27
	Mean	21.59	1.48
	Std. Deviation	1.394	.935
Disagree	N	1	1
	Mean	23.00	3.00
	Std. Deviation	.	.
Total	N	50	50
	Mean	21.88	1.54
	Std. Deviation	1.304	.862

Measures of Association

	Eta	Eta Squared
Age * Cyber-AIoT Solution in SLE	.277	.077
Experience * Cyber-AIoT Solution in SLE	.256	.065

ANOVA Table

		Sum of Squares	df	Mean Square	F	Sig.
Age * Cyber-AIoT Solution in SLE	Between Groups	6.411	3	2.137	1.279	.293
	Within Groups	76.869	46	1.671		
	Total	83.260	49			
Experience * Cyber-AIoT Solution in SLE	Between Groups	2.381	3	.794	1.073	.370
	Within Groups	34.039	46	.740		
	Total	36.420	49			

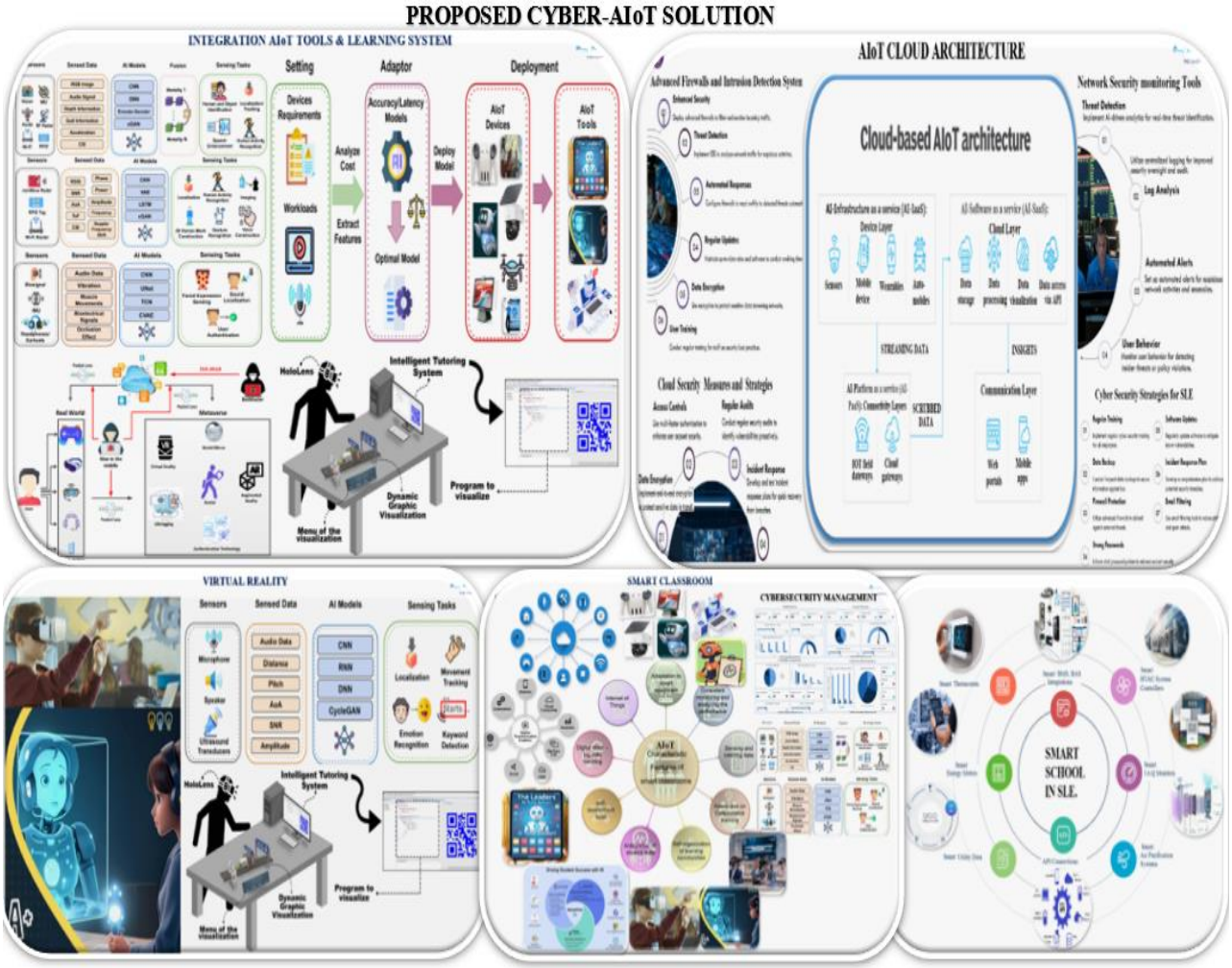
Picture No.10: Age and Experience-Based Perceptions of Cybersecurity and AIoT Security Solutions in Smart Learning Environments

The results of the mean, standard deviation, measures of association, and ANOVA indicate generally positive responses toward Cybersecurity and AIoT in Education, security enhancement in Smart Learning Environments, AI algorithms and AIoT model-based real-time protection, and Cyber-AIoT solutions. The descriptive results show that most respondents agreed or strongly agreed with the statements, suggesting favourable perceptions of the role of Cybersecurity and AIoT in enhancing security in Smart Learning Environments. Nevertheless, the measures of association between age, experience, and the study variables were weak, as shown by the low Eta and Eta Squared values. In addition, the ANOVA results were not statistically significant since all p-values were greater than 0.05. This means that age and experience did not significantly

influence respondents' perceptions of Cybersecurity and AIoT in Education. Therefore, based on these results, the null hypothesis is not rejected, and the alternative hypothesis is not supported statistically. The findings only confirm positive perceptions among respondents, but they do not confirm a statistically significant relationship based on age and experience.

Cyber-AIoT Solution in Smart Learning Environment

Based on the data analysis and case studies, this research is proposed a secure cyber-AIoT solution in Smart Learning Environment. The output of this research is the solution for Smart Learning Environment. The critical part of the research is the integration of AIoT devices and tools based on the advance AI algorithm model (Chinju Paul and Amal Ganesh C. Sunitha 2018). This research proposed following Cyber-AIoT solutions in Smart Learning Environment. The Picture No.11 explained the details of the Cyber-AIoT solutions in Smart Learning Environment.



Picture No.11: Cyber-AIoT Solution for Smart Learning environment.

- **Cyber-AIoT integrated devises & learning System.** Based on the study, it proposed Zero-attacked & protected AI-powered learning tablets, HoloLens, Adaptive system devices, Student performance tracking system etc.
- **Cyber-AIoT Cloud Architecture:** Zero-attacked AI powered protected Cloud architecture for a smart learning environment. This includes AI based advanced firewall & instruction detection system, AI based network monitor tools, Cloud based strategies and measurements& Cyber strategies for cloud architecture.
- **Cyber-AIoT Smart Classroom:** A smart classroom include AIoT devices and learning system, AI based cybersecurity management, classroom surveillance cameras, AI tutoring systems, program for visualisation, virtualisation of shared resources, high-speed internet & connectivity and the scheduling and slicing techniques for protection.
- **Cyber-AIoT Smart Virtual Reality**: CAVE (Cave automatic virtual environment) and HMDs (Head-mounted displays), Interactive school desk and there are different VR accessories which can combine with HMDs and CAVEs, such as gloves, suits or controllers which can offer more exciting experience.
- **Cyber-AIoT Smart School:** Protected Smart Cloud architecture, Smart AL System, Smart BMS, Smart HVAC system, Smart IAQ Monitor System, Smart AP System, Smart API Connectivity, Smart UD System. Smart EM System & Smart TC system for better SLE & future generation.

5.0 Conclusion

The research introduces the research topic, emphasizing the significance of cybersecurity and AIoT, AI model effectively mitigates cybersecurity threats, ensuring intelligent mobility and secure operations within educational systems outcomes. The study provides an overview of the research problem, key objectives, and questions that guide the study. Additionally, this research outlines the scope and rationale behind the study, establishing the groundwork for the subsequent researches. The findings highlight the applicability of AIoT in creating robust and secure educational ecosystems. The Cyber-AIoT solutions in Smart Learning Environment steamed the future research as well as the changing of the teaching aspects of future generation.

REFERENCES

Abichandani, P., Sivakumar, V., Lobo, D., Iaboni, C., & Shekhar, P. (2022). Internet of things curriculum, pedagogy, and assessment for stem education *A review of literature. IEEE Access, 10, 38351–38369*. https://ieeexplore.ieee.org/abstract/document/9749084

Aloul, F.A., The need for effective information security awareness. Journal of advances in information technology, 2012. 3(3) p. 176-183. https://doi.org/10.4304/jait.3.3.176-183

Arsenio A, H. Serra, R. Francisco, F. Nabais, J. Andrade, E. Serrano, Internet of intelligent things *Bringing artificial intelligence into things and communication networks, in Interco operative Collective Intelligence* Techniques and Applications, Springer, 2014, pp. 1–37. https://doi.org/10.1007/978-3-642-35016-0_1

Baidoo Anu, L. Owusu Ansah, Education in the era of generative artificial intelligence (AI) *Understanding the potential benefits of ChatGPT in promoting teaching and learning, 2023*, Available at SSRN 4337484. https://doi.org/10.2139/ssrn.4337484

Bajaj, V. Sharma, Smart Education with artificial intelligence-based determination of learning styles, Procedia Compute. Sci. 132 (2018) 834–842. https://doi.org/10.1016/j.procs.2018.05.095

Blokland, P., Reniers, G., 2019. An ontological and semantic foundation for safety and security science. Sustainability 11 (21), 6024. https//doi.org/10.3390/ su11216024

Casteel, C., Peek-Asa, C., 2000. Effectiveness of crime prevention through environmental design (CPTED) in reducing robberies. Am. J. Prev. Med. 18 (4), 99–115. https://doi. org/10.1016/s0749-3797(00)00146-x.

Chakraborty P, Dizon-Paradis RN, Bhunia S (2022) ARTS a framework for AI-rooted IoT system design automation. IEEE Embed Syst Lett 14(3)151–154.

Chałubinska-Jentkiewicz, K. (2021). Access to the ICT network as a public task of local government. Lex Localis, 19 (1), 175–195.10.4335/19.1.175-195(2021).

Chinju Paul and Amal Ganesh C. Sunitha, "An IoT-Based Smart Classroom", *Lecture Notes on Data Engineering and Communications Technologies*, vol. 15, pp. 9-14, Sept 2018. https://doi.org/10.1007/978-981-10-8681-6_2

Cohen, J., 2021. School safety and violence research and clinical understandings, trends, and improvement strategies. Int. J. Appl. Psychoanal. Stud. 18 (3), 252–263. https//doi.org/10.1002/aps.1718.

Hilgurt SY. 2022. Pattern handling for quantifying hardware components of signature-based cybersecurity systems.

Huang, L. S., Su, J. Y., & Pao, T. L. (2019). A context aware smart classroom architecture for smart campuses. *Applied Sciences, 9*(9), 1837. https://doi.org/10.3390/app9091837

Jalali, M.S., M. Siegel, and S. Madnick, Decision-making and biases in cybersecurity capability development Evidence from a simulation game experiment. The Journal of Strategic Information Systems, 2019. 28(1) p. 66-82. https://doi.org/10.1016/j.jsis.2018.09.003

Kesan & Zhang, (2019) An empirical investigation of the relationship between local government budgets, IT expenditures, and cyber losses 20

Kumar V, Sinha D. 2022. Hybrid approach using deep autoencoder and machine learning techniques for cyber-attack detection. *International Journal of Ambient Computing and Intelligence* 13(1)1-21 https://doi.org/10.4018/IJACI.293098

Lahat, T. Adali and Jutten, "Multimodal Data Fusion an Overview of Methods Challenges and Prospects", *Proceedings of the IEEE*, vol. 103, pp. 1449-1477, Sept 2015. https://doi.org/10.1109/JPROC.2015.2460697

Lamoreaux, D., Sulkowski, M.L., 2019. An alternative to fortified schools Using crime prevention through environmental design (CPTED) to balance student safety and psychological well-being. Psychol. Sch. 57 (1), 152–165. https//doi.org/10.1002/ pits.22301

Liu, S., Chen, Y., Huang, H., Xiao, L., & Hei, X. (2018). Towards smart educational recommendations with reinforcement learning in classroom. In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering* (pp. 1079–1084). https://doi.org/10.1109/TALE.2018.8615217

Liu, Y., Zhang, P., & Zhou, J. (2018). Using AI to enhance the security of Internet of Things. *Sensors, 18*(2), 403.

Maurseth, P.B., The effect of the Internet on economic growth Counter-evidence from cross-country panel data. Economics Letters, 2018. 172 p. 74-77. https://doi.org/10.1016/j.econlet.2018.08.034

Mircea, M., Stoica, M., & Ghilic-Micu, B. (2021). Investigating the impact of the internet of things in higher education environment. IEEE Access, 9, 33396–33409. https://doi.org/10.1109/ACCESS.2021.3060964

Norris, D. (2021). A new look at local government cybersecurity in 2020. Public Management (PM), 103 (7), 15–20. https//www.proquest.com/docview/ 2561966386?accountid = 13380&forcedol = true

Olawale OP, Ebadinezhad S. 2023. The detection of abnormal behavior in healthcare IoT using IDS, CNN, and SVM. In: Lecture Notes on Data Engineering and Communications Technologies. Cham: Springer. https://doi.org/10.1007/978-981-99-0835-6_27

Qin, M., Hu, W., Qi, X., & Chang, T. (2024). Do the benefits outweigh the disadvantages? Exploring the role of artificial intelligence in renewable energy. *Energy Economics, 131*, Article 107403. https://doi.org/10.1016/j.eneco.2024.107403

Robert, C. DicksonDeane, C. Guevara, L. Koster, M. SanchezMendiola, N. Arbino, w. AlFreih, L. Skallerup Bessette, J. Stine, Pelletier, M. McCormack, J. Reeves, 2022 EDUCAUSE *Horizon Report Teaching and Learning Edition, Technical Report,* EDUCAUSE, 2022.

Sharvari Ravindran, Saptarshi Chaudhuri, Jyotsna Bapat, Debabrata Das (2024) Novel adaptive multi-user multi-services scheduling to enhance throughput in 5G-advanced and beyond IEEE Transactions on Network and Service Management. https://doi.org/10.1109/TNSM.2024.3351669

Singh, A.P. (.2023). AI in Cyber Security Advantages, Applications and Use Cases. Retrieved from https//www.analyticsvidhya.com/blog/2023/02/future-of-ai-an d-machine-learning-in-cybersecurity/.

Tsai, W.-T. (2022). Cloud-based virtual laboratory for network security education. IEEE Transactions on Education, 57(3), 145–150. https://doi.org/10.1109/TE.2013.2282285

Xu, W. Yu, D. Griffith, and N. Golmie, ‘‘A survey on industrial Internet of Things: A cyber-physical systems perspective,’’ IEEE Access, vol. 6, pp. 78238–78259, 2018. R. https://doi.org/10.1109/ACCESS.2018.2884906

Zhang, J., Wang, Y., Li, S., & Shi, S. (2021). An architecture for IoT-enabled smart transportation security system: A geospatial approach. *IEEE Internet of Things Journal, 8*(8), 6205–6213. https://doi.org/10.1109/JIOT.2020.3041386

Zhang, Q., Wang, K., & Zhou, S. (2020). Application and practice of vr virtual education platform in improving the quality and ability of college students. *IEEE Access, 8*, 162830–162837. https://doi.org/10.1109/ACCESS.2020.3019262

Zhang, X.; Chen, Y.; Hu, L.; Wang, Y. The metaverse in education Definition, framework, features, potential applications, challenges, and future research topics. *Front. Psychol.* 2022, *13*, 108233. https://doi.org/10.3389/fpsyg.2022.1016300

Zhang-Kennedy, L. and S. Chiasson, A systematic review of multimedia tools for cybersecurity awareness and education. ACM Computing Surveys (CSUR), 2021. 54(1) p. 1 39. https://doi.org/10.1145/3427920