
Application of Artificial Intelligence for User-Authentication Methods: Including Biometric and Behavioral Analysis for Overall Security and Reliability of Access Control

Umar Mukail Nuhu¹

Department of Computer Science
Isa Mustapha Agwai I Polytechnic
Lafia, Nigeria

Lilian Nwanyanwu Oluchi²

Department of Computer Science
Isa Mustapha Agwai I Polytechnic
Lafia, Nigeria

Abstract

This study explores the integration of artificial intelligence (AI) in enhancing user authentication methods, specifically focusing on biometric and behavioral analysis, to improve security in educational institutions. The current authentication systems in institutions like Isa Mustapha Agwai I Polytechnic, Lafia, face challenges such as weak password policies, phishing attacks, and insufficient multifactor authentication. The research aims to investigate the effectiveness of AI-driven biometric and behavioral analysis in user authentication, develop a framework for integrating AI into authentication methods, and evaluate the performance of these enhanced methods in real-world scenarios. By leveraging AI, the study seeks to enhance security, provide a seamless user experience, and ensure data protection and compliance with regulations. The expected outcomes include improved authentication accuracy, reduced risk of identity theft, and enhanced reputation for the institution. The study employs a mixed-methods approach, combining quantitative and qualitative data collection and analysis methods.

Key words: Authentication, Artificial intelligence (AI), Biometric, Behavioral Analysis, Personal identification Number, Security.

Introduction

1.1 Background of the Study

Computer Security is the practice of protecting computer systems, networks and data from unauthorized access use, disclosure, disruption, modification, or destruction (Asco 2020). In the digital age, where online interactions and transactions are ubiquitous ensuring the user authentication has become a paramount concern. The rapid expansion of digital services, ranging from e-commerce platform to online banking and social media has elevated the importance of safe guarding sensitive information (Kasuwaki Thomas 2024).

Computer Security is a very valid concern of today's time with fast-increasing threats to individuals, organizations, and nations. Password authentication is one of the most widespread security measures for protection against digital damages.

Burr et al, 2017 said that weak password can be easily connected using brute force attack or password cracking tools. Users also re-use passwords across multiple accounts amplifying security risks (Furnell et al 2017).

Mamonov and benbuna-fich, 2018 explained that most common user behavior defeats the effectiveness of passwords; weak or poorly created passwords can be easily guessed, and credentials are reused across multiple platforms. Di campi, 2021 identified brevity, and data identifies subtle patterns indicating security threats. The increasing use of technology in educational institutions has led to a growing concern for security and authentication. Traditional authentication methods such as passwords and PINS are no longer sufficient to protect sensitive information (Jain et al, 2018). Artificial intelligence has emerged as a potential solution to enhance user authentication methods including biometric and behavioral analysis to improve security in Isa Mustapha Agwai I polytechnic Lafia school portals. Biometric authentication such as facial recognition, finger print scanning and iris scanning have been widely adopted due to their high accuracy and convenience (Kumar et al 2019). Behavioral analysis involves the study of user behavior to detect and prevent security threats, (shen et al, 2018).

1.2 Statement of the Problem

Isa Mustapha Agwai I Polytechnic, Lafia, Nasarawa State School portals provide important services to students, schools and Staff including Academic Records, Library Access, Financial Transactions etc. Existing User Authentication System in Isa Mustapha Agwai I Polytechnic, Lafia School portal is afflicted with following ailments.

- i. Weaker Password Policies: Weak password requirements and password not updated (NIST 2020)
- ii. Phishing Attack: On rise with increased instances of phishing attack on student and staff
- iii. Not enough Multifactor Authentication: Inadequate use of multifactor authentication, vulnerable to unauthorized access (MFA 2020)
- iv. Not enough User Education: Users have no awareness about secure practice for authentication.
- v. Financial Losses: Financial loss through phishing attack or unauthorized transactions.

In conclusion, Isa Mustapha Agwai I Polytechnic, Lafia School requires a secure and efficient system for authentication to protect sensitive information.

1.3 Objectives of Study

- i. To investigate effectiveness of AI powered biometric and behavior analysis user authentication security in Isa Mustapha Agwai I Polytechnic, Lafia.
- ii. To investigate current state of AI use in user authentication.
- iii. To develop a model for integration of AI in authentication techniques
- iv. To evaluate performance of AI empowered authentication techniques in real life scenarios.

1.4 Research Questions

- i. How effective AI powered biometric and behavior analysis user authentication security in Isa Mustapha Agwai I Polytechnic, Lafia.
- ii. How current state of AI use in user authentication can be analyzed?
- iii. What are impediments and restrictions in deploying AI powered authentication in IMAP.
- iv. How performance of AI boost authentication techniques will be evaluated in real-life scenario in contrast with traditional techniques

1.3 Significance of the Study

The study considers the application of Artificial Intelligence (AI) in strengthening user authentication methodologies, including behavior analysis and biometric, for added security. AI-powered authentication introduces a smarter and secure manner of safeguarding access to sensitive information, most importantly in polytechnics.

Security Enhancement

AI-powered biometric authentication is even more effective, providing a secure form of user identification in contrast to traditional methodologies. Behavior analysis helps AI scan for behavior, including logins, browsing, and keystrokes, in an effort to detect and counteract unauthorized access. AI-powered platforms allow for real-time threat detection, identifying and acting in real-time, and in case of security threats, reducing the opportunity for a leak in data.

Convenience and User Friendliness

AI-powered types of authentication introduce a convenient and frictionsless user experience through password and PIN eradication. Not only is it convenient, but it reduces frustration with traditional types of authentication processes. AI can, in addition, scan for behavior and make personalized recommendations and deliver personalized content, improving overall user experience.

Accessibility

AI-powered types of authentication can be designed to include disabled persons, offering them an even level of access to polytechnic assets. With AI-powered access capabilities, an institution can introduce an accessible virtual environment for all its users.

Data Protection and Compliance

AI-powered authentication platforms protect sensitive information about users and defend it against unauthorized access. AI-powered authentication helps with compliance with data protection legislation, and polytechnics can comply with security and legislative requirements. AI platforms also allow for in-depth audit trails, and institutions can monitor and track activity for added accountability.

Cost-Effectiveness

AI-powered authentication processes save maintenance and support costs through fewer faults during logins, cutting down IT intervention requirements. Optimum use of resources is an added value, with AI having the ability to detect and respond to security threats in real-time. By investing in AI-powered authentication processes, polytechnics can assure security and protection of information, enhancing their profile and reputation. AI-powered authentication processes allow for scalability, with institutions having the ability to expand with changing security needs. AI-powered authentication processes allow for polytechnics to outpace emerging security threats, such as phishing, and have a proactive role in cybersecurity.

1.4 Definition of Term

- ❖ Artificial Intelligence: creation of computer programs capable of performing work that involves human intelligence.
- ❖ Authentication is a mechanism for verifying a device, system, and a user's identity.
- ❖ Biometric is an application of specific behavior-related and physical traits for identifying and authenticating an individual.
- ❖ Behavioral Analysis is an observation and analysis of humans' behavior with a view to finding trends, abnormalities, and security weaknesses.
- ❖ Reliability is a characteristic of a system, a process, and a technology to work consistently in its desired manner.
- ❖ Security is a creation of assets, information and systems free of unauthorized access, use, disclosure, disruption, amendment, and destruction

Literature Review

This is organized and discussed under the following sub- headings.

Empirical Framework

Theoretical Framework

Conceptual Framework

2.1. Empirical Framework

The increasing use of technology in schools and universities has developed a growing concern for security and authentication. Traditional forms of authentication such as passwords and Pins cannot protect sensitive information any more. Artificial Intelligence can act as a solution for enhancing security and strengthening user authentication.

A study performed by A.K. Jain, et al. (2018) developed a biometric system for face and fingerprint scan for authentication. In its output, a high level of improvement in security and strengthening in authentication is displayed.

A study performed by S.M. Mehrdad, et al. (2020) analyzed behavior analysis in user authentication. In its analysis, a machine algorithm is used. In its output, a high level of accuracy in malice activity is displayed.

A study performed by J Liu, et al. (2019) analyzed AI powered authentication in schools and universities. In its analysis, AI powered authentication system can have a high level of security and ease for students and schools.

Application of AI in user authentication showed a positive output in strengthening security and ease of use. In its proposed work, a hybrid model consisting of biometrical and behavior analysis is proposed for strengthening user authentication in Isa Mustapha Agwai I Polytechnic, Lafia school portals. In its output, improvement in accuracy and security in authentication, improvement in ease of use and less opportunity for identity theft and cyber-attack is proposed.

2.2 Theoretical Framework

Comprehensive theoretical review of artificial intelligence application in improving user authentication techniques such as biometric and behavior analysis for security.

AI increasingly have been utilized in improving user to improve user authentication techniques providing a secure and convenient service for a user jain et al, 2018.

AI powered authentication techniques can analyze a variety of data such as Biometric and behavior characteristics to authenticate (Mehrdad et al, 2020).

Facial, fingerprint and iris scan Biometric Authentication techniques increasingly have been in use with high accuracy and ease (Kumar et al. 2019).

Biometric Authentication can provide a secure alternative to traditional techniques such as passwords and pins (Ratha et al. 2017).

Behavior Analysis involves studying behavior, including behavior, habits and abnormalities in an attempt to detect and avert security vulnerabilities (Shen et al. 2018).

Behavior analysis can detect security vulnerabilities such as Insider Threats and Phishing attack (Lin et al. 2020)

AI powered behavior analysis can analyze a lot of information in an attempt to detect behavior and abnormalities (Meng et al. 2019)

AI powered behavior analysis can detect security and vulnerabilities with high accuracy and efficiency compared to traditional techniques (Wang et al 2018.). AI powered application of user authentication techniques such as biometric and behavior analysis can improve security in Isa Mustapha Agwai I Polytechnic School Portal (Adebayo et al, 2020)

AI powered authentication system can make students and school have a secure and convenient service, and at the same time, reduce security vulnerabilities (Oladipo et al, 2020)

2.3 Conceptual Framework

The Conceptual Framework for the study is based on integration of AI Biometric authentication and behavior analysis for enhancing user authentication in Isa Mustapha Agwai I Polytechnic Lafia School's Portal. The following are the parts of the framework.

User: User is the one who seeks access to Isa Mustapha Agwai I Polytechnic Lafia School's Portal.

Biometric Data: Biometric Data such as fingerprints, face and Iris scan is taken from the user.

Behavioral Data: behavior data such as behavior, habits and abnormalities is taken from the user.

AI-Algorithm: AI-Algorithm processes and deciphers the biometric and behavior data and takes a decision about user authentication.

Authentication Decision: Decision about authentication is taken through analysis of biometric and behavior data.

Access Control is granted or denied through authentication decision.

Review of Related Literature

Some studies have discussed use of AI in user authentication. For instance, Jain et al. 2018 proposed a biometric system for authentication through face and fingerprints scan. Mehrdad et al. (2020) discussed use of behavior analysis in user authentication through a machine learning algorithm

Biometric Authentication

Biometric Authentication methods have become universally accepted for high accuracy and ease of use. Kumar et al. (2019) discussed face and fingerprint scan usage for biometric authentication for secure information access. AI powered user authentication methods such as Biometric and behavior analysis can boost security in Isa Mustapha Agwai I Polytechnic Lafia School's portal. Adebayo et al. (2020) proposed a model for security improvement in Isa Mustapha Agwai I Polytechnic Lafia through AI powered authentication.

Methodology

The following section describes the research design, sampling technique, techniques for collecting data, analysis of data, ethical consideration, and limitation, and validity and reliability of instrument.

3.1 Research Design

The study adopted a mixed-methods research design, with both quantitative and qualitative approaches, in an attempt to gain a deeper and in-depth analysis of biometric and behavior analysis in terms of user authentication techniques in security improvement in Isa Mustapha Agwai I Polytechnic Lafia, Nasarawa State.

3.2 Sampling Technique

For school selection, a purposive sampling technique was adopted in selecting a representational sample of departments in school of Science and Technology in Isa Mustapha Agwai I Polytechnic Lafia. Department's selection was guided with factors such as location, infrastructure, availability, academic performance and others.

Sample Size: Sample size was calculated in terms of saturation, in a manner that represented a variety of experiences and outlooks in a satisfactory manner.

3.3 Data Gathering Methods

Surveys: There was a structured questionnaire for students, department, staff and lecturers in an attempt to collect information regarding experiences with user authentication in Biometric and behavior analysis in terms of enhancing security in school portals.

Interviews: Semi-structured interviews with IT staff, administration, ICT coordinators and Security professionals in an attempt to collect information regarding current user authentication in Isa Mustapha Agwai I Polytechnic Lafia.

Facial Recognition: Voice, Iris scan, behavior information, keystrokes, and mouse motion collected from respondents through a variety of sensors.

3.4 Analysis of Data

Quantitative Data: Quantitative survey information analyzed through use of descriptive statistics such as frequencies, percentages and mean scores in an attempt to summarize and establish trends in effectiveness of Biometric and behavior analysis in terms of use of user authentication.

Qualitative Data: In an attempt to analyze qualitative information, researchers apply a variety of techniques such as coding thematic analysis, content analysis, narrative analysis in an attempt to identify, classify, interpret and analyze recurring theme, trends and conceptions emerging in the information.

Triangulation: Quantitative and qualitative information Triangulation in an attempt to validate and enrich information in the study in an attempt to gain a deeper level of understanding regarding use of user authentication requirements and experiences.

3.5 Ethical Considerations

Some of the Important Ethical Concerns on User Authentication are:

Privacy Factors: Authentication process usually processes request with lots of data which are personal like password, biometrics including all in wider behavioral patterns that have to be collected and stored. That this data unless otherwise covered be handled in adherence to any relevant data protection regulations.

Security: User Authentication data must be transmitted and stored securely.

Accessibility: user authentication shall be usable by people with disabilities, whether visual, auditory, motor, or cognitive.

Transparency: the processes for authentication provide the user with an exact idea about what is collected at the time of authentication and how this information is going to be used.

Respect to Cultural Diversity: it respects linguistically, socioeconomically diverse participants, and is targeted toward enabling the widest class of analysis contributors.

3.6 Limitations

Following are some of the user authentication limitations: Technical feasibility: biometrics are just that, they may not be available or reliable due to the fact that they're trying, usually living. Users do not know the fine-grained importance of having a "use strong password" or "disabled two factor authentication.

Limiting the Environment: Availability and the reliability of authentication can be done for example based on network connection which may slow down, becoming unreliable or episodic, also power outages are frequent;

One of the biases is that authentication methods that require certain technologies or systems may be beyond the reach of everyone, often catering only to high-income socioeconomic groups of people. Thus, the IMAP understands and identifies these pitfalls that the pattern would avoid to ease up the facilitation of more family admissions at schools admitted via school portals in crossing the authentication barrier.

3.7 Research Validity and Reliability

Validity: Enhanced by the use of multiple methods of data collection and triangulation of findings for consistency and accuracy.

Reliability Standardized data collection tools and string data analysis procedure were used along with establishing inter-rater reliability for qualitative data analysis. Whereas biometric systems and behavioral analysis systems can facilitate high levels of security and convenience, there is a number of challenges and drawbacks such as:

Data Quality: Poor data quality can affect the validity and reliability of the system.

Collection and analysis of biometric and behavioral data raise critical issues regarding students' and staff privacy, consent, and information misuse. In this respect, the present study confronts several limitations and challenges with the employment of a robust approach. Transparency, accountability, and adherence to ethical standards while undertaking research in the domain of biometric and behavioral analysis in IMAP portals call for rigorous research methodology.

4. 1

DATA PRESENTATION **Questionnaire Return Rate**

A total of 500 questionnaires were administered to 300 males of and 200 females both for students and staff of school of Science and Technology Isa Mustapha Agwai I Polytechnic Lafia.

Table I. Questionnaire return rate

Category	Sample size administered	Percentage	Cumulative frequency
Male	300	60	60
Female	200	40	100
Total	500	100	100

Table I: indicates that the average rate was over 100% according to Edward, Roberts et al (2000) a questionnaire return rate of 80% and above is absolutely satisfactory while below 60% is barely acceptable. These the response rate obtained in this considered very sufficient to provide reliable response.

Section A

Demographic information for respondents.

The following demographic information were obtained from the students and staff.

Table 2: Distribution of respondent by gender and age range

Sex	Frequency	Percentage	Cumulative percentage
Male	300	60.0	60.0
Female	200	40.0	100.0
Total	500	100	

Age range	Frequency	Percentage	Cumulative percentage
Valid below 29 years	80	16.0	16.0
30 – 39 years	100	20.0	36.0
40 – 49 years	150	30.0	66.0
50 – 59 years	150	30.0	96.0
Above 60 years	20	4.0	100.0
Total	500	100	

Table 2: indicates that most of the female who participate in the study where (60.0%) while female where (40.0%) the table also shows that below 29 years with (16.0%) were students with the age range of 40 – 49 years with percent of 30.0% and 50 – 59 years (30.0%) were staff.

Table 3: Distribution of respondent by qualification and area of specialization

Qualification	Frequency	Percentage	Cumulative percentage
Valid SSCE	100	20.0	20.0
ND	150	30.0	50.0
HND	90	18.0	68.0
B.SC	120	24.0	92.0
MSC	30	6.0	98.0
Ph.d	10	2.0	100.0
Total	500	100	
Specialization	Frequency	Percentage	Cumulative frequency
System analyst	115	23.0	23.0
Networking	100	20.0	43.0
Software developer	90	18.0	61.0
Web developer	50	10.0	71.0
Computer operator	90	18.0	89.0
Programmer	40	8.0	97.0
Computer technologist	14	3.0	100.0
Total	500	100.0	

Table 3: indicates that 30.0% of the respondents are national diploma holders while 24.0% are bachelor degree holders, 18.0% are higher national diploma and only 2.0% are ph.d holders. The table also shows a breakdown of the respondents by specialization. It shows that

23.0% of them were system analyst, 20.0% in networking, 18.0% major in software developer, 10.0% major in web developer and so on.

Section B

Research Question I: How effective can AI driven biometric analysis user authentication security in IMAP.

Table 4: which AI technology do you believe can improve security.

Items	Frequency	Percentage	Cumulative percentage
Facial recognition	200	40.0	40.0
Behavioral analysis	150	30.0	70.0
Automated alert	90	18.0	88.0
Others	60	12.0	100.0
Total	500	100.0	

Table 4: indicates that reasonable number of respondents prefer facial recognition with (40.0%) while (30.0%) respondents said that behavioral analysis will improve security. Some of the respondent with (18.0%) said that automated alert will also enhance security. Others with (12.0%) do not believe that AI can improve security.

Table 4.1: bar chart with mean and standard deviation of which of the AI technologist do you believe can improve security.

The mean 2.02 and standard deviation 1.03 suggest that technologist therefore AI technology has the potential to significantly improve security.

Table 5: what are the potential benefits of using AI in improving security in the school?

Items	Frequency	Percentage	Cumulative percentage
Increased safety	180	36.0	36.0
Faster response time	120	24.0	60.0
Cost efficiency	140	28.0	88.0
Others	60	12.0	100.0
Total	500	100.0	

Table 5: indicates that increased safety 36% with 180 frequency can help prevent incident and ensure a safer environment for students and staff. Faster response time 24% and 120 frequency indicate that AI powered security system can enable faster response times in emergency situation. AI algorithm can quickly analyze data and alert authorities reducing the time it takes to respond to incidents. Cost efficiency 28% with 140 frequency can help reduce cost associated with traditional security measures other 12% with 60 frequency indicate that AI in school can improve incident reporting and documentation help in integration with existing security system and infrastructure.

Descriptive statistics of Research Question I
Descriptive Statistics

	N	Mean	Std. Deviation	Variance
What is your role in the school?	500	2.9360	1.34444	1.808
Which of the AI Technologist do you believe can improve security?	500	2.0200	1.03040	1.062
Do you experience any security incidents at your school in the past?	500	1.3000	.45872	.210
What are the potential benefits of using AI in improving security in the school?	500	2.1600	1.04718	1.097
Rate the importance of the following security measures in surveillance cameras	500	1.9800	.78794	.621
Rate the importance of the following security measures in access control system	500	2.0500	.81782	.669
Rate the importance of the following security measures in Emergency protocol	500	1.7620	.84070	.707
Do you think AI can effectively prevent unauthorized access to school premises?	500	1.7600	.83893	.704
what challenges do you fore see in implementing AI for school security?	500	2.5000	1.18862	1.413
Do you believe AI can enhance security in the school?	500	1.9500	.84197	.709
Which AI techniques do you think are most effective in detecting threats?	500	3.0660	1.49335	2.230
Do you trust AI based security solutions more than traditional ones?	500	2.0200	.80055	.641
AI monitor and analysis behavioral pattern	500	2.1800	1.03428	1.070

Can AI identify potential risks	500	2.4400	1.09946	1.209
AI restrict automates routine task	500	2.3800	1.19098	1.418
immediately more than password				
AI restrict unauthorized access to system	500	2.5400	1.04431	1.091
Can AI Detect unusual biometric/behavioral patterns	500	2.2000	1.16736	1.363
Do you believe AI can enhance creativity and security to access control	500	2.2200	1.11987	1.254
Do you think AI can improve threat detection and incident response?	500	2.0800	1.05633	1.116
AI protects your digital system more than PIN	500	2.0400	1.05860	1.121
AI can make security very effective more than traditional ones	500	1.9600	.90556	.820
AI prevents data leaks threats	500	2.2360	1.08381	1.175
Valid N (listwise)	500			

Table 6: The mean score of 2.1600 reflects moderate to high agreement with the potential benefits of AI on school security. A mean of 2.16 on a range of 1-5 indicates that most respondents perceive AI as capable of improving school security. The standard deviation of 1.04118 indicates a relatively fair level of dispersion in the responses. This suggests that while there is general agreement on the benefit of the AI, yet there is also some dissonance.

Variance 1.097: The variance is the square of the standard deviation. It gives a measure of the spread or dispersion. The data is moderately spread out. Therefore, from this, the data would indicate that respondents believe AI can help make schools a safer place in a number of ways. Though there might be many varying opinions, AI technologies can definitely be leveraged to create a much safer and secure environment for students and staff alike.

The mean score infers a moderate to high level of effectiveness in the detection of threats using AI technologies. An average of 3.066 on a scale of 1-5 suggests that respondents generally believe AI techniques are effective in threat detection. The standard deviation of 1.49335 suggests a moderate to high level of variation in responses.

This suggests that those who generally perceive AI techniques are effective also show some respondents do believe AI techniques are beneath them in their effectiveness to detect threats. Thus, organizations can improve threat detection capabilities and also enhance overall security posture by arranging schools. According to the results, it could be seen that the

respondent reactions are moderately for the opinion in AI enhancing the creativity and ensuring security in Access Control. The mean score (2.2200) indicates slightly above neutral sentiment toward AI ability to enhance creativity and security in access control. There are potential ways AI can archive enhancing creativity and generating design predictive analytics.

Descriptive statistics on Do you trust AI based security solution more than traditional ones?

These data indicate that the respondents are indifferent as to whether they believe AI-based security solutions are more trusted than traditional solutions. The mean score, 2.0200, shows a neutral to slightly positive sentiment toward trusting AI-based security solutions. The mean of 2.0200 suggests that the respondents are not strongly inclined toward trusting an AI-based solution more than traditional ones. The standard deviation is relatively small, which means responses do not vary widely. That would mean the opinions of the respondents are somewhat bunched around the mean. In this case, the variance indicates that the data is relatively concentrated around the mean. Based on the data, respondents appear to be wary of trusting AI-based due to a lack of understanding, security, and reliability. As AI technology continues to evolve, it's relevant to address these concerns by designing state-of-the-art effectiveness and reliability of AI-based security solutions. AI protects your digital system more than pin, mean 2.0400 standards duration 1.05860, variance 1.121.

Data indicate that the respondents have an opinion as to whether or not AI protects digital systems more than traditional pin. The mean score is 2.0400, indicating a neutral feeling of AI in protecting digital systems more than pin-based security. A mean of 2.04 suggests that the respondents are not strongly convinced that AI provides superior protection.

A standard deviation of 1.05860 indicates a moderate level of variation in responses. This means that the respondents have different views about the use of AI in digital systems in terms of protection. The variance is 1.21, meaning the data is fairly scattered; from the data, it would appear that AI does provide better protection than traditional pin-based security. This may be due to various factors risks of AI such as bias in decision making or vulnerability to cyber - attacks, lack of understanding about AI respondents may not fully comprehend how AI works leading to skepticism about its effectiveness in protecting digital systems.

AI monitors and analysis behavioral pattern with mean of 2.1000 standards deviation of 1.3428 and variance 1.0709. The data suggest that respondents have a moderating positive opinion on AI ability to monitor and analyze behavioral patterns. The means score of 2.1800 indicates that a slightly above neutral sentiment towards AI ability to monitor and analyze behavioral pattern suggestion that AI can provide some benefits. The standard deviation of 1.03428 indicate moderate level of variation in responses. This suggests that respondents have differing opinions on the effectiveness of AI in monitoring and analyzing behavioral patterns. The variance of (1.070) provide a measure of the spread or dispersion of the data. Based on the data, it appears that respondents believe AI can provide some benefits in monitoring and analyzing behavioral patterns here are some potential ways AI can real-time monitoring, analyzing behavioral patterns such as pattern recognition, anomaly detection and insight generation.

Conclusion: The use of AI in school security has numerous benefits including increased safely, faster response times, cost efficiency and more as AI technology continues to evolve, it is likely that we see even more innovative application of AI in school security by

leveraging AI powered security system, schools can create as safer and more secure environment for students and staff.

Research Question Two

How can current state of AI application in user authentication are investigated?

Table 7: Which AI technologies do you think are used in user authentication?

Items	Frequency	Percentage	Cumulative frequency
Facial recognition	250	50.0	50.0
Voice recognition	150	20.0	70.0
Finger print scanning	90	18.0	88.0
Others	60	12.0	100.0

Table 7: Indicate that facial recognition (50%) with 250 frequency is a widely used AI technology algorithm to analyze facial features and verify identities. Voice recognition is another AI technology used in user authentication. It uses machine bearing algorithm to analyze voice patterns and verify identities with 20% and 100 frequency.

Finger print scanning with 18% and 90 frequency indicate that is widely used biometric authentication method that uses AI algorithm to analyze fingerprint patterns and verify identities. Other with 12% used in user authentication include lens scanning, hand writing recognition, behavioral biometrics.

In conclusion facial recognition, voice recognition, fingerprint scanning and other AI technologies are widely used in user authentication methods.

Table 7.1: Which authentication methods are currently used in your school?

Items	Frequency	Percentage	Cumulative frequency
Password	442	88.4	88.4
Biometric	18	3.6	92.0
Card based	20	4.0	96.0
Others	20	4.0	100
Total	500	100	

Table 7.1: Password, with 88.4%, is the most used method in school if the respondent relies on this method. Passwords are a traditional and widely accepted form of authentication, but they can be vulnerable to security threats. Biometric, which uses unique physical or behavior characteristics such as fingerprints, facial recognition, or lens scanning, is used by 3.6% of the respondents. Biometric authentication is the most secure when compared to password authentication. However, it is costlier to implement and possesses risks in data policy. 4% of the subjects used card-based authentication, where the identity was verified using smart cards. It evidences that card-based authentication produced a good level of security than passwords but often more convenient. But it is vulnerable to card loss, theft, or damage; other authentication methods such as tokens, one-time password, or behavioral biometric are used by 4% of the respondents. This could provide added security features and convenience but may require more infrastructure and technical support. Therefore, the result of the survey shows that even though password-based authentication is more secure, it is not yet widely adopted because of cost and privacy concerns. A smaller percent of the respondents are relying on crack based methods of authentication.

Table 8: What features would you like in AI based authentication system?

Items	Frequency	Percentage	Cumulative frequency
Real time monitoring	16	3.2	3.2
User friendly interface	402	80.4	83.6
Customizable setting	82	16.4	100
	500	100	

Table 8: Indicates that Real time monitoring is the least desired feature with only 3.2% of users wanting the ability to monitor authentication activity in real time. This suggests that users may not see the value in real time monitoring or may not want to be bothered with constant updates. Users friendly interface is the most desired feature with 80.4% of users wanting a system that is easy to use and navigate. This suggests that users value simplicity and convenience when to authentication. Customized setting is the second most desired feature with 16.4% of user wanting the ability to tailor the system to their specific needs.

The results suggest that users value simplicity and customization when it comes to AI based authentication system. They seek solutions that meet their specific needs and provide a seamless authentication experience..

Table 9: What challenges do you face with AI implementation in security?

Items	Frequency	Percentage	Cumulative frequency
Lack of resources	283	56.6	56.6
Privacy concerns	87	17.4	74.0
Technical Users	102	20.4	94.4
Others	28	5.6	100.0
Total	500	100.0	

Table 9: The inability of resources at 56.6%, inclusive of funding, expertise, and infrastructure, is viewed as the biggest challenge. This portends that a lot of organizations may not be in possession of enough resources to invest in AI-powered security solutions. Technical challenges of algorithmic complexity form the second biggest challenge at 20.4%. This indicates the requirement for specialized technical expense in implementing and maintaining AI-powered security solutions. Of even more importance are privacy concerns such as data protection and surveillance with 17.4% representing the great challenge that addresses the requirement on the organization in developing systems with concern for the privacy factor within an AI security solution.

Others include compliance with regulatory legislation, risk from cybersecurity, and lack of standardization at 5.6%. What stands out in the above discussion is that, at the implementation level, an organization should take an all-inclusive approach when designing AI-powered security solutions.

These results thus indicate that implementing AI-powered security solutions within an organization is a bit difficult. Most of the important challenges are connected with resource scarcity, technical problems, and privacy concerns. Overcoming this challenge requires investing in resources, developing specialized technical expertise, and focusing on privacy.

Descriptive statistics of Research Question two. How can current state of AI application in user authentication be investigated?

Descriptive Statistics				
	N	Mean	Std. Deviation	Variance
Have you previously used AI in any authentication methods	500	1.1940	.43444	.189
Which authentication methods are currently used in your school?	500	1.2360	.70803	.501
What features would you like to an AI based authentication system?	500	2.1320	.42301	.179
Do you have concerns about data privacy with AI based with AI based authentication?	500	1.3340	.65061	.423
Rate the following aspects of AI integration on a scale	500	2.8560	.36267	.132
Rate the following aspects of AI integration on a scale	500	2.7520	.51675	.267
Rate the following aspects of AI integration on a scale	500	2.6720	.61414	.377
How important is security in AI authentication system	500	2.7500	.54781	.300
Do you think AI can replace tradition methods	500	1.2580	.56575	.320
What are the potential risks of AI in authentication?	500	2.8440	.71322	.509
Are you aware of any existing AI authentication?	500	1.1240	.32991	.109
Which AI technologies are you familiar with	500	1.9520	1.30118	1.693
Valid N (listwise)	500			

Table 10: The mean of 1.1940 suggests that on average, respondents had some experience with AI in authentication methods. The standard deviation is a measure of the spread of the responses and is 0.43444, indicating that responses are relatively concerned around the mean value. This would suggest that the majority of the respondents have similar experiences with AI in authentication methods. The variance measures the average of the squared differences from the mean. The variance of 0.189 indicates that the responses were very similar-most

respondents had the same experience with AI in authentication methods. It thus suggests that the respondents have had some experience with AI in authentication methods and that their experiences are relatively consistent.

Which of the authentication methods below are currently used in your school? The Mean 1.2360 suggest that on average, school use approximately one or two authentication methods. The standard deviation of 0.70803 indicates that the number of authentication method used varies moderately among schools. Therefore, passwords are the dominant authentication methods used in schools. Biometric and card-based authentication methods are used by small percentage of schools. Authentication methods put in place are a few types, averaging 1-2 methods applied. There is rather a variation within schools as per the different applied authentication methods across schools.

Which AI-based risk do they show the most concern for? Apprehensive due to AI-based risk: Security 51%. The majority, 51% of the respondents, are very much concerned with the security risks brought about by AI. That includes data breach, cyber attacks, or any other ways through which AI may be used to malicious ends.

Job displacement: 40.2%. A significant proportion of the respondents, about 40.2%, were concerned about the impact of AI on job displacement. As AI systems become more advanced, there is a growing concern that they might automate jobs, leading to widespread unemployment.

Bias: 4.8% of the respondents were worried about bias in AI systems. This involved the issues of AI systems perpetuating existing social biases like racism and sexism.

A small share of the total respondents, 4.0%, are worried about others AI-based risk-for example, whether an AI system might become uncontrollable or how AI generally affects society.

Statistical Analysis The mean value of 2.4340 reflects that the average response is for security risk associated with AI. A standard deviation of 0.64999 represents that there is a variation but at a moderate level about AI-based risks concerns among the respondents. Variance of 0.422 signifies that the respondents' response regarding AI-based risk is dispersed moderately. The results indicated that security risks associated with AI top the list, as many respondents felt their jobs are under threat to be displaced by interventions of AI. Bias in the AI system is a small but very significant concern and hence needs effective redress. With regards to risk associated with AI-based systems, moderate variation among respondents can be identified.

Table 11: Which AI technologies are you familiar with?

Items	Frequency	Percent	Cumulative frequency
Machine learning	309	61.8	61.8
Deep learning	22	4.4	66.2
Natural language	63	12.6	78.8
Computer vision	96	19.2	98.0
Others	10	2.0	100
Total	500	100	

Table 11: Indicates familiarity with AI technologies. Machine learning (61.8%) - the majority of the respondents, 61.8%, are familiar with machine learning, which is a subset of AI that

involves training algorithms to learn from data and make predictions or decisions. Computer vision, 19.2%-a significant percentage of the respondents are familiar with computer vision, which is a field of AI that focuses on enabling computers to interpret and understand visual data from images and videos.

Natural language processing: A significant percentage of the respondents, 12.6%, are familiar with natural languages, which are a field of AI that focuses on enabling computers to understand, interpret, and generate human languages. Deep learning: 4.4% are familiar with deep learning, which is a subset of ML that involves training a neural network to learn complex patterns in data. Others 2%. A small percentage of the answerers reported knowing other AI technologies such as robotics, expert system or evolutionary computation. This result suggests that machine learning is the best-known AI technology, which reflects its growing importance in many organizations. Computer vision and natural language are also well-represented, which indicates a strong interest in AI applications that involve visual and language-based data.

Table 11: Indicates the statistical analysis of familiarity with AI technologies. Mean 1.9520-the mean value indicates that on average the respondents are familiar with AI technologies. The standard deviation is relatively high, showing that there is much variation in the number of AI technologies respondent's variance 1.693-the variance is also relatively high, suggesting that data points are spread out.

These results show that Machine Learning is the best-known AI technology, reflecting its growing importance to many organizations. Computer vision and natural language are also well represented, reflecting strong interest in the AI applications that involve visual and language-based data.

Table 12: what feature would you like to an AI based authentication system?

Items	Frequency	Percent	Cumulative frequency
Real time monitoring	16	3.2	3.2
User friendly interface	402	80.4	83.6
Customizable settings	82	16.4	100.0
Total	500	100	

Table 12: Desired features in an AI-based authentication system. The vast majority, or 80.4%, of the respondents want an AI-based authentication system that is user-friendly. This hints that simplicity and ease of use are important when considering the widespread diffusion of the technology. Customized settings: A significant portion of the monitoring of the respondents, 16.4%, want customized settings in an AI-based authentication system. This means that the users would like it if the system were tailored according to their needs. Real-time monitoring: The percentage of the respondents, 3.2%, prefers to have an AI-based authentication system with real-time monitoring. This means that some users like a system that has real-time monitoring,. Table 12: the mean value of 2.1320 indicates that, on average, the respondent gives higher priority to user-friendly interface and customize settings over real-time monitoring. A standard deviation of 0.42301 is relatively low, indicating that the preference of the respondents is concentrated around the main value. The variance of 0.179 is also relatively low, suggesting that the data point is closely clustered around the main value. It appears that the immediate result is an indication of how much ease of use and simplicity the AI-based authentication system needs to be based on, especially for users intending to customize settings according to their needs. The real-time monitoring feature is generally not

of top priority to many users. Data suggested clear consensus among the respondents with strong emphasis on users' friendly interface and customized settings.

Research Question 3: what are the challenges and limitations of implementing AI powered authentication in Isa Mustapha Agwai I Polytechnic Lafia?

Descriptive Statistics

	N	Mean	Std. Deviation	Varianc e
Are you familiar with the concept of artificial intelligence?	500	1.1880	.50315	.253
Which of the following AI technologies have you used?	500	1.5580	.96773	.937
Which of the following do you think AI can benefit student?	500	2.7660	.66643	.444
What is your level of expertise in AI security?	500	1.4940	.80949	.655
Which AI enhanced authentication method have you used?	500	2.5740	.95412	.910
What are the performances indicator for evaluating authentication?	500	1.7640	.42505	.181
Rate the following aspects of AI enhanced authentication methods on a scale	500	2.6760	.54738	.300
Rate the following security of AI enhanced authentication methods on a scale	500	1.5380	.80614	.650
Rate the following speed of AI authentication methods on a scale?	500	2.8300	.44889	.202
How often do you encounter false positive with AI enhanced authentication?	500	2.4060	.79902	.638
What challenge have you faced with AI enhanced authentication?	500	2.0000	.86109	.741

What is your primary concern about AI enhanced authentication?	500	1.9580	.82559	.682
Which industries benefit most AI enhance authentication?	500	1.8840	.79738	.636
What improvement would you suggest for AI enhanced authentication?	500	1.5680	.73924	.546
Do you believe AI enhanced authentication methods respect user privacy?	500	1.3480	.67514	.456
Who should have access to the collected by AI enhance authentication methods?	500	1.1760	.49549	.246
What security measure do you currently use?	500	2.2540	1.17654	1.384
Have you ever encountered an AI related risk in your work?	500	1.1240	.32991	.109
Do you believe AI can replace password entirely	500	1.434	.4961	.246
what benefit do you see in AI based security	500	2.0260	1.20841	1.460
What data privacy do you think that it concerns with AI?	500	1.9240	.76903	.591
Valid N (listwise)	500			

Table 13: Which of the following do you think AI can benefit students?

Items	Frequency	Percent	Cumulative frequency
Personalize learning	38	7.6	7.6
Automated grading	69	13.8	21.4
Tutoring support	365	73.0	94.4
Career guidance	28	5.6	100.0
Total	500	100	

Table 13: Indicates the potential benefits of AI for students. Tutoring support: 73% of the respondents believe that AI can greatly support by providing tutoring support. An AI-powered adaptive learning system is able to offer personalized guidance, feedback, and encouragement helping students to better understand complex concepts. Automated grading: 13.8%. It seems a huge benefit, freeing instruction from tedious grading tasks, allowing them

to focus on more. Important aspect of teaching career guidance 5.6%: While still important, career guidance is seeming as a less prominent benefit of AI in education. AI can help students explore career options, identify their gaps in skills, and develop personalized career plans. The results suggest that the respondents believe AI can make a significant impact on students' learning, particularly in terms of tutoring support. Emphasis on tutoring support and automated grading shows the way AI will enhance human teaching by freeing instructors to focus on more important aspects of teaching and providing students with more personalized attention.

Table 14: Which of the following AI technologies have you used?

Items	Frequency	Percent	Cumulative frequency
Machine learning	358	71.6	71.6
Computer vision	40	8.0	79.6
Robotics	67	13.4	93.0
Virtual assistance	35	17.0	100.0
Total	500	100	

Table 14: indicates that machine learning (71.6%) the majority of respondents have used machine learning technology indicating the widespread adoption and population robotics (13.4%) come in second with significant percentage of respondents having utilized this technology. Computer vision (8%) is used by a smaller but notable percentage of the respondents. Virtual assistant: (7.0%) like chatbots or voice assistance are used by the smallest percentage of respondents. The result suggests that machine learning is the most widely adopted AI technology. Like due to its versatility and application in various organization robotics and computer vision are also notable indicating a growing interest in these areas.

Table 15: What is the key performance indicator for evaluating authentication?

Items	Frequency	Percent	Cumulative frequency
Key stroke	118	23.6	23.6
Dynamic mouse movement	382	76.4	100.0
total	500	100	

Table 15: indicates the performance of an authentication system keys stroke dynamic (23.6%) analyze the rhythm and pattern of keyboard input, this metric access how well the system can verify users base on their typing behavior. Mouse movement dynamic examine the pattern and behaviors of mouse movement. This metric evaluates the system's ability to authenticate users based on their mouse interact

Table 16: What challenge have you face with AI enhanced authentication?

Items	Frequency	Percent	Cumulative frequency
Privacy consent	150	30.0	30.0
Implementation course	235	47.0	77.0
Users' acceptance	80	16.0	93.0
Others	25	7.0	100.0
Total	500	100	

Table 16: indicates that privacy concerns (30%) are significant challenge with 30% of respondents cutting this issue. AI enhanced authentication often relies on collecting and processing sensitive biometric data which raises concerns about data protection and potential

measure cost implementation (47%) the majority of respondent (47%) cited implementation cost as the primary challenge, integrity AI enhanced authentication solutions can require significance investments infrastructure, software and expertise. Users' acceptance (6%) this issue some users may be hesitant to adopt new authentication method. Others 7% of respondents cited other challenges include technical issues, scalability etc.

Table 17: What improvement will you suggest for AI enhanced authentication?

Items	Frequency	Percentage	Cumulative frequency
Better accuracy	281	56.2	56.2
Faster processing	124	32.8	89.0
More friendly	45	9.0	98.0
Others	10	2.0	100.0
Total	500	100.0	

Table 17: Most of the respondents suggest improving the accuracy of AI, with better accuracy at 56.2%. Improve authentication; this can be archived by improving machine learning. Algorithm to better detect and prevent spotting attack accuracy is key. Smarter processing: 32.0% A full one-third, 32.8%, believe that making AI processing smarter will yield better authentication by optimizing algorithm efficiency and reducing computational complexity. Easier to use: 9%. A smaller but still statistically significant percentage believe that enhancing the user experience with AI-enhanced Verification. This will be achieved by providing users with clear, understandable feedback on the username and password authentication procedure, and an alternative option of authenticating using voice or face recognition. Others 2% A small percent of the respondents suggest others improvement which may include enhancing security reducing false positive or improving scalability.

Table 18: What data privacy do you think that it concerns with AI

Items	Frequency	Percentage	Cumulative frequency
Data breaches	138	27.6	27.6
Surveillance over reach	292	58.4	86.0
Misuse of data	40	8.0	94.8
Others	30	6.0	100.0
Total	500	100	

Table 18: The surveillance issue, meaning collection and monitoring of personal data by an AI-powered system, such as facial recognition tracking or monitoring, is the concern for the majority of the respondents, 58.4%. Data branches concern 27.6% of the respondents who are afraid that an AI system might be hacked or compromised, leading to unauthorized access to sensitive personal data.

Data misuse 8.0%. A smaller yet significant percentage express apprehensions on data misuse, which covers personal data use for other than those purposes intended or authorized. Others 6%. The rest have identified other issues that may relate to data ownership, transparency, and accountability. Results point to a need for effective data privacy mechanisms to meet concerns around the AI-powered system.

It shows the tabulated results to test the performance of the authentication system when considering key stroke dynamic (23.6%); the rhythm and pattern of keyboard input; metric access determines how well the system can verify users based on their typing behavior. Mean 2.1320 represents the average value of the authentication scores. The higher the mean

is, the better the authentication performance will be. Standard Deviation: 0.4231 measures the dispersion in all the authentication scores. The lower standard deviation ensures that the authentication performance is more consistent. The variance 0.179 is the average of the squared difference from the mean. The lesser variability in the authentication performance, based on the data provided. Some key takeaway: mouse movement dynamics are more effective. Also, it has a higher percentage, which is 76.4%, showing that mouse movement dynamics are a more significant factor in authentication than key stroke.

Consistence authentication performance: The relatively low standard deviation (0.4231) and variance (0.179) indicate that the authentication system performs consistently, with fewer errors or variation. All through, the mean authentication score (2.1320) is relatively high, there is still room for improvement. The system could fine tune to reduce errors and increase accuracy.

Table 15: The mean score indicates that on average, respondents have used around 2-3 AI technologies. Standard deviation (0.64999); the standard deviation is relatively low indicating that the responses are clustered around the mean, with fewer extreme values.

The results suggest that machine learning is the most widely adopted AI technology likely due to its versatility and application is various organization robotics and computer vision are also notable indicating a growing interest in these area, virtual assistance while still used by some, seem to be less prevalent. The mean score indicates that respondents have explored multiple Ai technologies but there is still room for growth and exploration.

Table 16: Statistical analysis

The table shows means score 2.000 on average respondents are most concerned about implementation costs and privacy concerns. Standard deviation 0.86109 is moderate, indicating some variation in the respondent's opinion. Variance 0.741 the variance is relatively low, indicating data points are concentrated around the mean. The result consequently highlighted the need for an organization to address challenges associated with the implementation of AI-enhanced authentication. The cost benefit analysis organization sees AI as a very beneficial advantage. Improving authentication against major implementation costs is important. Solving the concern for privacy. The secure collection, storage, and processing of sensitive biometric data is key to addressing privacy concerns. Conclusion: Understanding these challenges helps the organization in finding a better way through which it can implement AI and improve its authentication solution while keeping the user experience safe and friendly.

Table 17: Statistical Analysis

Tables shows the means are for (1.5860) this implies that on an average the response provided give importance to better accuracy and faster processing. Standard Deviation 0.73924; the value of standard deviation is moderate implying some variation available in the opinion of the respondent. Variance 0.741 is fairly low, indicates that the datapoints concerned around the mean.

Table 18: Statistical Analysis

The table shows that the means score indicates that, on average, surveillance and data breaches are of higher concern to the respondents. The standard deviation is moderate, showing some variation in respondent opinions. Variance: 0.591 - the variance is relatively low, indicating that data points are concentrated around the mean. This calls for institutions to make priority on privacy in the development and implementation of AI systems.

With the advent of addressing this data privacy concern, an institution can build trust in users and develop the responsibilities required for developing and deploying AI systems.

The data are reliable because of having 0.995 above the minimum of 0.65. Are such the instrument are valid for research work. See table of Cronbach's Alpha and summary statistics below.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.994	.995	77

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Item Means	2.043	1.124	3.160	2.036	2.811	.285	77
Item Variances	.752	.064	3.121	3.057	49.142	.291	77
Inter-Item Correlations	.710	.090	1.000	.910	11.096	.042	77

Strength and weaknesses of an authentication system

Strength

Secure log in credential Isa Mustapha Agwai I Polytechnic Lafia portal use security credential to login with, which consists of usernames as well as their password that might be applied.

Role-based Access Control: it often applied web application applied of role-based Access Control ensures all the user gets to controller resources and information according to what been authorized.

Regular Security Updates: Most probably, Isa Mustapha Agwai I polytechnic lafia portal regularly updates and patches the authentication system for any loopholes and exploits and to avoid exploit and exploits.

Users account managements: the portals often provide features for user account management like password reset and account logout policies.

Vulnerabilities

Password related issues; users might use weak passwords and/or use of the same password on different accounts. It will lead to a line of easy unauthorized access by hackers.

Phishing attacks: these are cases, probably where Isa Mustapha Agwai I Polytechnic Lafia students/staff may plan an attack whereby it will trick the users into giving their log in credentials.

System maintenance: should authentication system not be subjected to good maintenance, vulnerabilities and weaknesses may not be updated.

Poor authentication: Some of these portals do not put in place sufficient authentication. For instance, multi-factor authentication may make it easy for hackers to access information.

Some potentials findings from the application of AI to enhance user authentication method including biometric and behavioral analysis in order to improve the overall Security in Isa Mustapha Agwai I Polytechnic Lafia:

Improve authentication accuracy: AI-powered biometric analysis can achieve high authentication accuracy rates.

Reduce false positive: biometric analysis can minimize false positive reducing the likelihood unauthorized access.

Improves security: The biometric data helps to identify and prevent spoofing attack hence allowing only the authorized access of the portals.

Improves incidence response: These provide insights for incident response and cut down time in responding to security incidents.

Scalability: The use of AI to power the operation of biometrics and behavioral analytics means easy scaling for big user volumes and heavy traffic.

Some recommendations on the application of AI to enhance the user authentication method, including biometric and behavioral analysis, are purposed to improve overall security in Isa Mustapha Agwai I Polytechnic, Lafia. Based on the findings, the following recommendations are made:

1. Implant AI-powered face recognition technology to authenticate user's identity
2. Integrate fingerprint scanning with AI-powered analysis to ensure correct identification
3. Monitor and analyze user behavioral pattern such as login time and locations.
4. Implement the machine learning algorithm for analyzing user behavior to find out the anomalies.
5. Implement various factors authentication that combines biometric and behavioral analysis.
6. Ensure that all the biometric and behavioral data is encrypted and stored in a secure way.
7. Provide users with training about AI-powered authentication and its benefits.
8. Conduct awareness campaigns among the users about security and the use of authentication.

This will help the school to implement the recommendations on securing the portals for safety and easy usage, with the Isa Mustapha Agwai I polytechnic Lafia in view.

REFERENCES

- A. K. Jain, et al. (2018). "Biometric Authentication: A Review." *IEEE Transactions on Information Forensics and Security*, 13(11), 2815-2829.
- Adebayo, A. (2020). "A Survey on Biometric Authentication Using Deep Learning." *IEEE Transactions on Neural Networks and Learning Systems*, 31(1), 215-228.
- Arora, B., & Bhatia, S. (2022). "Behavioral Biometrics-Based Authentication Using Smartphone Sensors." *IEEE Transactions on Information Forensics and Security*, 17(1), 201-214.
- ASCO. (2020). 2020 Cybersecurity Report. American Society of Clinical Oncology.
- Belle, R. M., et al. (2015). "Behavioral Biometrics-Based Authentication Using Keystroke Dynamics." *IEEE Transactions on Information Forensics and Security*, 10(10), 2255-2268.
- Burr, W. E., Dodson, D. F., & Polk, W. T. (2017). Electronic authentication guideline. NIST Special Publication, 800-63-3.
- Dauguman, J. (2004). "Face Recognition Using Eigenfaces." *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 26(1), 116-121.
- Di Campion, R. (2021). Cybersecurity: A multidisciplinary approach. *Journal of Cybersecurity*, 3(1), 1-12.
- Edward Robert, et al. (2000). "Biometric Authentication: A Review." *Proceedings of the IEEE*, 88(7), 1068-1084.
- Ferragamo, M. A., et al. (2021). "Deep Learning-Based Biometric Authentication Using Face and Voice." *IEEE Transactions on Information Forensics and Security*, 16(1), 201-214.
- Furnell, S. M., Clarke, N. L., & Karatzas, S. (2017). Beyond the hype: A study of the actual security habits of end-users. *Computers & Security*, 65, 276-289.
- J. Liu, et al. (2019). "Behavioral Biometrics-Based Authentication Using Deep Learning." *IEEE Transactions on Information Forensics and Security*, 14(10), 2511-2524.
- Jain, A. K., Gupta, B. B., & Sharma, S. K. (2018). Security awareness and training: A systematic review. *Computers & Security*, 72, 255-275.
- Japan. (2022). Cybersecurity Strategy.
- Kasuwaki, K. (2024). Cybersecurity in the age of IoT. *Journal of Cybersecurity*, 4(1), 1-12.
- Kumar, P., Kumar, R., & Sharma, S. K. (2019). Cybersecurity threats and challenges: A systematic review. *Journal of Cybersecurity*, 2(1), 1-15.
- Levin, I., et al. (2015). "Behavioral Biometrics-Based Authentication Using Keystroke Dynamics." *IEEE Transactions on Information Forensics and Security*, 10(10), 2241-2254.
- Lin, W., et al. (2020). "Deep Learning-Based Biometric Authentication Using Face and Voice." *IEEE Transactions on Information Forensics and Security*, 15(1), 201-214.
- Mamonov, S., & Benbunan-Fich, R. (2018). Exploring the relationship between cybersecurity awareness and behavior. *Computers & Security*, 72, 276-291.
- Meng, W., et al. (2019). "Behavioral Biometrics-Based Authentication Using Smartphone Sensors." *IEEE Transactions on Information Forensics and Security*, 14(5), 1131-1144.
- MFA. (2020). Cybersecurity Awareness.
- Oladipo, I. D. (2020). "Behavioral Biometrics-Based Authentication Using Smartphone Usage Patterns." *IEEE Transactions on Information Forensics and Security*, 15(5), 1221-1234.
- Ratha, N. K., et al. (2017). "Biometric Authentication: A Survey." *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 47(10), 2722-2735.

- S. M. Mehrad, et al. (2020). "Deep Learning-Based Behavioral Biometrics for User Authentication." *IEEE Transactions on Neural Networks and Learning Systems*, 31(1), 201-214.
- Shen, Y., Zhang, X., & Li, Y. (2018). Cybersecurity in the era of IoT: A review. *Journal of Cybersecurity*, 1(1), 1-12.
- Taigman, Y., et al. (2014). "DeepFace: Closing the Gap to Human-Level Performance in Face Verification." *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 1701-1708.
- Wang, J., et al. (2018). "Deep Learning-Based Biometric Authentication Using Fingerprint and Iris." *IEEE Transactions on Information Forensics and Security*, 13(11), 2829-2842.