ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may579

The Use of Artificial Intelligence (AI) to Checkmate Security Challenges in Katsina State (A Case Study of Some Selected Local Government Areas)

Maharazu Mamman[1]; Abdussalam Muhammad Mustapha[2]; Amina Lawal[1]

[1]Department of Computer Science, Federal College of Education P.M.B. 2041 Katsina, Katsina State, Nigeria
[2]Department of Mathematics, Federal College of Education P.M.B. 2041 Katsina, Katsina State, Nigeria

Publication Date: 2026/05/25

Abstract: Over the past decade, Katsina State has experienced persistent security challenges, including banditry (kidnapping), cattle rustling, and armed robbery, particularly in seven frontline Local Government Areas (LGAs) out of the thirty-four in the state. These recurrent attacks have led to loss of lives and property, as well as mass migration of residents to relatively safer towns. This study investigates the use of Artificial Intelligence (AI) to checkmate security challenges in selected LGAs of Katsina State. The research adopted a descriptive survey design, using structured questionnaires as the primary instrument for data collection. A total of 90 questionnaires were administered to selected respondents, comprising security personnel, community leaders, and residents across Dan-Musa, Batsari, and Safana Local Government Areas (LGAs). Findings reveal a strong consensus among respondents that AI technologies—such as machine learning, intelligent video surveillance, sensor-based monitoring systems, and data analytics—can significantly enhance intelligence gathering, crime detection, and rapid decision-making. The study highlights that AI integration with Closed-Circuit Television (CCTV) systems can improve monitoring of suspicious activities, support search and rescue operations, assist in forensic investigations, and reduce response time to security threats. Respondents also indicated that automation of routine administrative tasks through AI could enable redeployment of security personnel to high-risk areas. The study concludes that effective deployment of AI-based security systems in Katsina State can strengthen crime prevention strategies and improve overall public safety. It recommends government investment in AI infrastructure, capacity building for security agencies, and policy frameworks to ensure ethical and efficient implementation.

Keywords: *Artificial Intelligence; Security; Public Safety; Community Leaders; Crime Detection*.

How to Cite: Maharazu Mamman; Abdussalam Muhammad Mustapha; Amina Lawal (2026) The Use of Artificial Intelligence (AI) to Checkmate Security Challenges in Katsina State (A Case Study of Some Selected Local Government Areas). *International Journal of Innovative Science and Research Technology*, 11(5), 1434-1448. https://doi.org/10.38124/ijisrt/26may579

I. INTRODUCTION

Artificial intelligence (AI) technology abstracts the idea of creating machine thinking behaving humanly and logically by using sets of computer algorithms. AI is new and prominent due to the latest improvements in the areas of machine learning, deep learning, and big data science. Over the last decade, AI has contributed to transforming many sectors, resulting in the fifth industrial revolution where with AI technology chunks of data can easily be turned into useful information.

With widespread applications of AI in many areas, it can be used in overcoming criminal activities and tracking of criminals. Digital personal assistants, which are characteristics of the present operating system of computers and smartphones solely, depend on AI technology to perform some tasks such as online search, recommendations, voice recognition, image recognition, automated personal banks database warehouse (images, fingerprint, insurance details, and vehicle registration) are maintained using AI tools. This serves as an enormous source of reference data for security personnel.

With the increasing number of kidnappers' attack and cyber-arms emerging significantly over the last 10 years, it is apparent that only AI technology can help safeguard against such crimes [1]. In order to conduct routine searches for people, motorcycles, cars, and forests, AI technology has to be coordinated with military personnel

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may579

which will result in a new defense mechanism. New aggressive methods for instance the dynamic building of protective perimeters, integrated management, and completely automated responses to the environment, would need the deployment of AI methods and knowledge-intensive technologies [2].

Integration of AI into our familiar world needs urgent attention. Presently, in the US and EU Orbital Insight is practicing machine self-training (AI components) for low-resolution photos from satellites [3]. Since the September 11th, 2001 attack, huge amounts of funds have been spent for national security programs. Nigeria is not left out as federal, state, and local governments dedicated billions of Naira in order to curb the security challenges facing the nation.

A suitable quality system can solve all tasks assigned to it, so it is essential to formulate such a task so that the solution obtained from the machine is not questionable in the interest of man; this process is called AI self-learning (Deep learning). The basic idea is that the purpose of the machine must be determined in the extreme outreach of valuable for the people targets, but it does not have to know in advance what they are. Innovative technologies for example quantum computing, may change how AI's technique to receive information about various issues, and allow it to learn by getting feedback, and possibly even imitate human cognitive contact with the globe. There are numerous routine techniques in security processes that AI can handle with ease such as forecasting of a crime, early identification of threats, and accurate forecast in a diverse timeframe. It provide satisfactory and timely backup with detailed multi-factor scenarios that can vividly improve the fight against crime in Katsina state.

➢ *Problem Statement*

Security remains a fundamental responsibility of government and a prerequisite for economic stability and sustainable development. However, Katsina State has experienced escalating insecurity over the past decade, characterized by banditry, kidnapping, cattle rustling, and armed robbery. Despite multiple federal and state interventions—including military operations such as Operation Sharan Daji, amnesty initiatives, negotiated exchanges, and restrictive measures on markets and fuel sales—the crisis has persisted, particularly in frontline Local Government Areas such as Faskari, Sabuwa, Dandume, Jibia, Batsari, Safana, Danmusa, and Kankara. The activities of armed groups operating around the Rugu Forest and along transnational routes have led to widespread displacement, destruction of property, and loss of lives. The continued rise in attacks, even in the presence of heavy military deployment, highlights the limitations of conventional security strategies.

Given the complexity and organized nature of banditry operations, there is an urgent need for innovative and intelligence-driven approaches to security management. In the digital age, Artificial Intelligence (AI) offers advanced capabilities in data collection, processing, analysis, and real-time decision-making. Planned criminal activities often leave digital footprints that can be detected through machine learning, predictive analytics, and intelligent surveillance systems. Therefore, integrating AI into the security architecture of Katsina State is justified as a strategic response to complement existing efforts, enhance intelligence gathering, improve rapid response mechanisms, and provide a more proactive and technology-driven solution to curbing insecurity in the state.

➢ *Objectives*

- To examine the level of awareness of security personnel on the use of Artificial Intelligence in combating insecurity in Katsina State.
- To assess the perception and readiness of traditional rulers and community stakeholders toward adopting AI-based security solutions.
- To explore the potential application of machine learning techniques in predicting and preventing planned criminal attacks in selected Local Government Areas.

➢ *Research Questions*

The following research questions are to be answered in this study:

- How is Artificial Intelligence (AI) currently being applied to address security challenges in selected Local Government Areas of Katsina State?
- What specific security threats in the selected LGAs can be effectively detected, monitored, or prevented through the use of AI technologies?
- What factors influence the effectiveness and adoption of AI-based security solutions in addressing security challenges within the selected LGAs of Katsina State?

II. LITERATURE REVIEW

Security challenges such as kidnapping, banditry, terrorism, and communal conflicts have significantly affected Northern Nigeria, particularly Katsina State. The increasing complexity and sophistication of these security threats have exposed limitations in conventional security strategies, including manual surveillance, reactive policing, and intelligence gaps. Scholars argue that modern security challenges require technologically driven solutions capable of predictive analysis, rapid data processing, and real-time response. Artificial Intelligence (AI), defined as computer systems capable of performing tasks that normally require human intelligence such as learning, reasoning, and decision-making, has emerged as a transformative tool in addressing contemporary security concerns [4].

Globally, AI has been integrated into various security architectures, including predictive analytics, automated surveillance, anomaly detection, and cyber threat intelligence. Research by [5] emphasizes that machine learning algorithms are highly effective in identifying patterns within large datasets, enabling early detection of security breaches and suspicious activities. Similarly, [6]

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may579

demonstrate how AI-powered computer vision systems can detect abnormal behaviors in real time, thereby enhancing surveillance efficiency in high-risk environments. These technological advancements suggest that AI systems can significantly improve monitoring capabilities in volatile regions.

Predictive policing, a major application of AI in security management, relies on historical crime data to forecast potential hotspots and allocate resources effectively. [7] argue that predictive models enhance operational efficiency by guiding law enforcement agencies toward data-driven decision-making. However, [8] caution that algorithmic bias may reinforce existing inequalities if datasets are not carefully managed. Despite these concerns, predictive analytics remains a promising tool for proactive security management, especially in regions experiencing recurring patterns of banditry and kidnapping such as some Local Government Areas in Katsina State.

AI-driven facial recognition and biometric surveillance systems have also gained prominence in modern security operations. [9] note that facial recognition technologies can assist law enforcement agencies in identifying suspects and tracking criminal networks. In areas with insurgent activities, such systems can support intelligence gathering and enhance rapid response mechanisms. For Katsina State, where mobility of armed groups across communities presents challenges, AI-enabled surveillance infrastructure could strengthen border monitoring and internal community security frameworks.

In addition to physical security applications, AI plays a critical role in cyber security. As security operations become digitized, vulnerabilities in communication systems, databases, and government infrastructure increase. [5] highlight that AI systems can detect anomalies in network traffic, identify malicious patterns, and respond autonomously to cyber threats. This capability is essential for protecting sensitive security information and ensuring coordinated response strategies in high-risk environments.

Within the African context, AI adoption in security remains in its developmental stage but shows considerable potential. [10] discuss the relevance of AI-assisted systems in enhancing border security and monitoring transnational criminal activities in West Africa. Their findings indicate that integrating AI technologies with traditional security structures can improve surveillance efficiency and intelligence coordination. However, infrastructural deficits, limited technical expertise, and funding constraints remain major barriers to effective implementation.

The Nigerian security landscape presents unique socio-economic drivers of insecurity, including unemployment, poverty, and weak institutional capacity. [11] argue that sustainable security solutions must combine technological innovation with socio-economic interventions. AI systems, when integrated into community policing frameworks, could enable early-warning mechanisms, data-driven patrol deployment, and real-time incident reporting. For selected Local Government Areas in Katsina State, such localized AI deployment may enhance responsiveness and reduce reaction time during security incidents.

Despite its advantages, the deployment of AI in security operations raises ethical and governance concerns. [12] emphasizes the importance of regulatory frameworks to prevent misuse, ensure accountability, and protect citizens' privacy rights. In low-resource settings, [13] further identify infrastructural limitations, poor data quality, and inadequate training as key obstacles to AI adoption. These challenges suggest that while AI presents promising opportunities to checkmate security threats in Katsina State, careful planning, legal oversight, and institutional capacity-building are essential.

In the eighties, a similar wave transformed the world with personal computer technologies, where computational power became very cheap and affordable. In the same way, AI makes prediction cheap and affordable and will lead to immediately automating routine and reproducible works through machines [14]. [15] proposed an approach to artificial intelligence as a tool for combating insecurity in Nigeria. Nigerian government and Katsina state in general can fully adopt and implement a similar approach proposed by [16] to control rising insecurity. [17] proposed a machine-learning based Internet of Things (IoT) smart home system to detect and reduce urban insecurity in Uganda, this research can extended to both rural and urban areas in Katsina state, Nigeria.

Overall, the reviewed literature indicates that Artificial Intelligence has strong potential to transform security management through predictive analytics, surveillance automation, and intelligent threat detection. Although empirical studies focusing specifically on Katsina State remain limited, global and regional evidence supports the feasibility of AI-driven security interventions. This study therefore contributes to existing knowledge by examining how AI technologies can be strategically deployed within selected Local Government Areas of Katsina State to enhance security operations and mitigate emerging threats.

III. METHODOLOGY

A quantitative approach was followed. [18] stresses that quantitative research focuses on gathering numerical data and generalizing it across groups of people or explaining a particular phenomenon. It emphasizes objective measurements and the statistical, mathematical, or numerical analysis of data collected through polls, questionnaires, and surveys or by manipulating pre-existing statistical data using computational techniques. According to [19], a descriptive survey design describes a condition or phenomenon as it exists naturally without manipulations.

- *Sample Size*

The sampling technique is a procedure applied to choose among the accessible population, a representative of the same population upon which generalization could be made. In simple terms, it is a method of using a small

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may579

portion of the population for investigation, and in the end, generalization is made on the whole population. For the purpose of this research a sampling frame of 90 respondents from Dan-Musa, Batsari and Safana LGAs will be used, 30 respondents from each local government area.

➢ *Instrument for Data Collection*

The techniques employed for data collection is basically the questionnaire, as a primary source of data. It provides an opportunity for respondents to give a frank, anonymous answer. It makes it easier to collect data from respondents and relatively easier to analyze the collected data [20] (Bolarinwa, 2015).

The questionnaire is a structured type because the research considered it to be more appropriate for the study [18] Igwenagu (2016) opined that "Questionnaire is an observational technique which comprises series of items presented to a respondent in a written form, in which the individual is expected to respond, the respondents are given a list of written items which he responds by ticking the one he considers appropriate".

➢ *Validity of the Research Instrument*

According to [20] validity refers to "the degree to which the instrument measures what it is supposed to be measuring". In order to make the questionnaire reliable and valid, it will given out to one of the staff of Umaru Musa Yaradua University Katsina for validation.

- *Data Analysis*

Data collected from the respondents are analyze and interpreted using a frequency table.

➢ *Simulation Environment*

The simulation scenario consists of one hexagonal cell with 500m radius. The total bandwidth is 5MHz with 25 resource block per slot of 12 subcarriers spacing.

➢ *Computer Resources*

The proposed machine algorithm will implemented using a system-level simulator [22] (Ikuno et al., 2010) developed in MATLAB (MATLAB R2014a). The Windows 7 64-bit operating system runs on an Intel core i5 machine with a 3.2 GHz core processor and 8GB of Random Access Memory (RAM). The simulation results generated are transferred to an Excel file and are depicted using the Gnutplot graphics utility version 5.1.

➢ *Simulation Setups*

The simulation experiments are conducted to evaluate the performance of the proposed schemes, using the same simulation platform [21] (Ikuno et al., 2010) implemented using object- oriented MATLAB.

➢ *Pseudocode*

The pseudocode for the proposed algorithm is presented as follows:

```
BEGIN AI_Bandit_Detection_Matching_System

SET ThresholdHigh = 0.80
SET ThresholdMedium = 0.60

FOR each Suspect in SuspectDatabase DO

// STEP 1: Compute Facial Similarity
FaceScore ← CosineSimilarity(IncomingFaceVector, Suspect.FaceVector)

// STEP 2: Compute Movement Pattern Similarity
MovementScor←MovementSimilarity(IncomingMovement Vector, Suspect.MovementVector)

// STEP 3: Compute Location Matching Score
IF IncomingLocation == Suspect.LastKnownLocation THEN
LocationScore ← 1.0
ELSE
LocationScore ← 0.5
ENDIF

// STEP 4: Compute Final Weighted Score
FinalScore ← (0.60 × FaceScore)
+ (0.25 × MovementScore)
+ (0.15 × LocationScore)

// STEP 5: Classify Risk Level
IF FinalScore ≥ ThresholdHigh THEN
RiskLevel ← "HIGH RISK"
AlertStatus ← "TRIGGER ALERT"

ELSE IF FinalScore ≥ ThresholdMedium THEN
RiskLevel ← "MEDIUM RISK"
AlertStatus ← "FLAG FOR MONITORING"

ELSE
RiskLevel ← "LOW RISK"
AlertStatus ← "NO ALERT"
ENDIF

// STEP 6: Store Result
SaveResult(Suspect.ID, FinalScore, RiskLevel)

ENDFOR

END AI_Bandit_Detection_Matching_System
```

➢ *Workflow for the Proposed Work*

Figure 1 illustrated the diagram for the workflow for the proposed work. Figure 2 represent the drone with install CCTV monitoring at the Dajin Rugu forest. Figure 3 show the matching area of the suspected bandits and criminal area.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may579

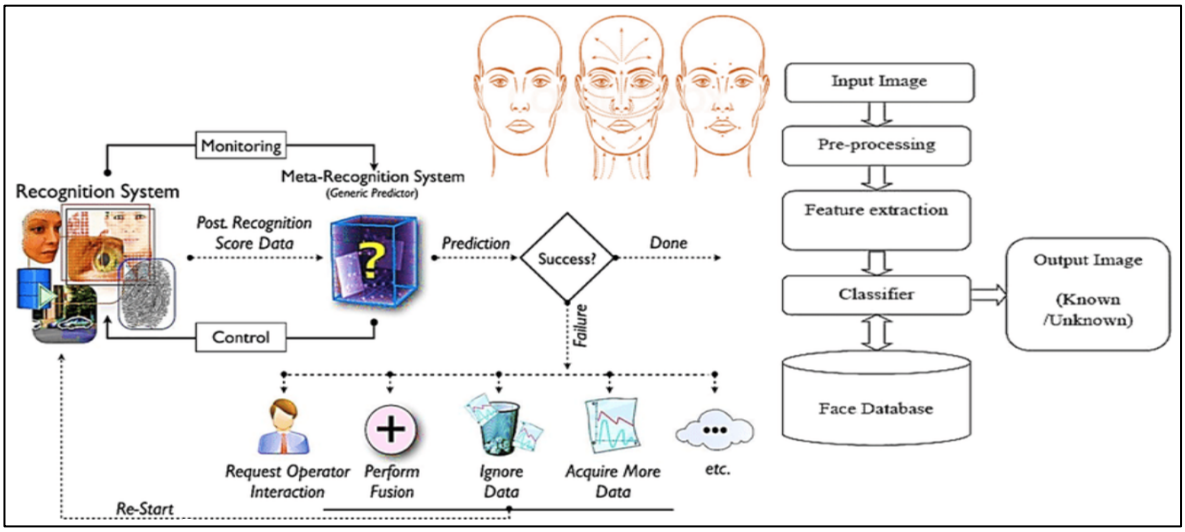

Fig 1 Workflow Diagram

Fig 2 Drone at Dajin Rugu Forest

Fig 3 Suspected Bandits and Criminals Areas

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may579

IV. RESULTS AND DISCUSSIONS

The discussion of this results obtained in this research is of twofold. The first segment is the implementation of the pseudocode in section 3.7 and analysis of the results obtained from questionnaire at the Appendix 1

A. AI Bandit Detection System Results Interpretation

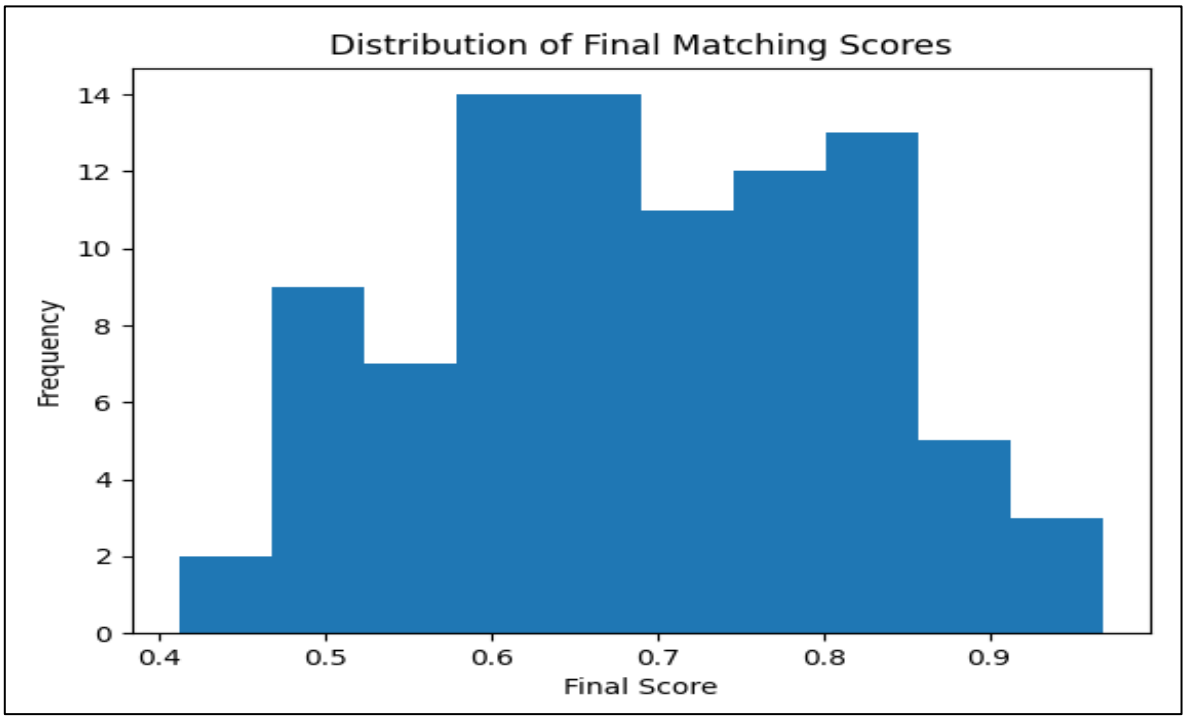

Fig 4 Distribution of Final Matching Scores

Figure 4 shows that most of the final matching scores fall between 0.6 and 0.85, indicating that many suspects are within the medium to high similarity range. This suggests that the system effectively identifies potential matches using combined inputs.

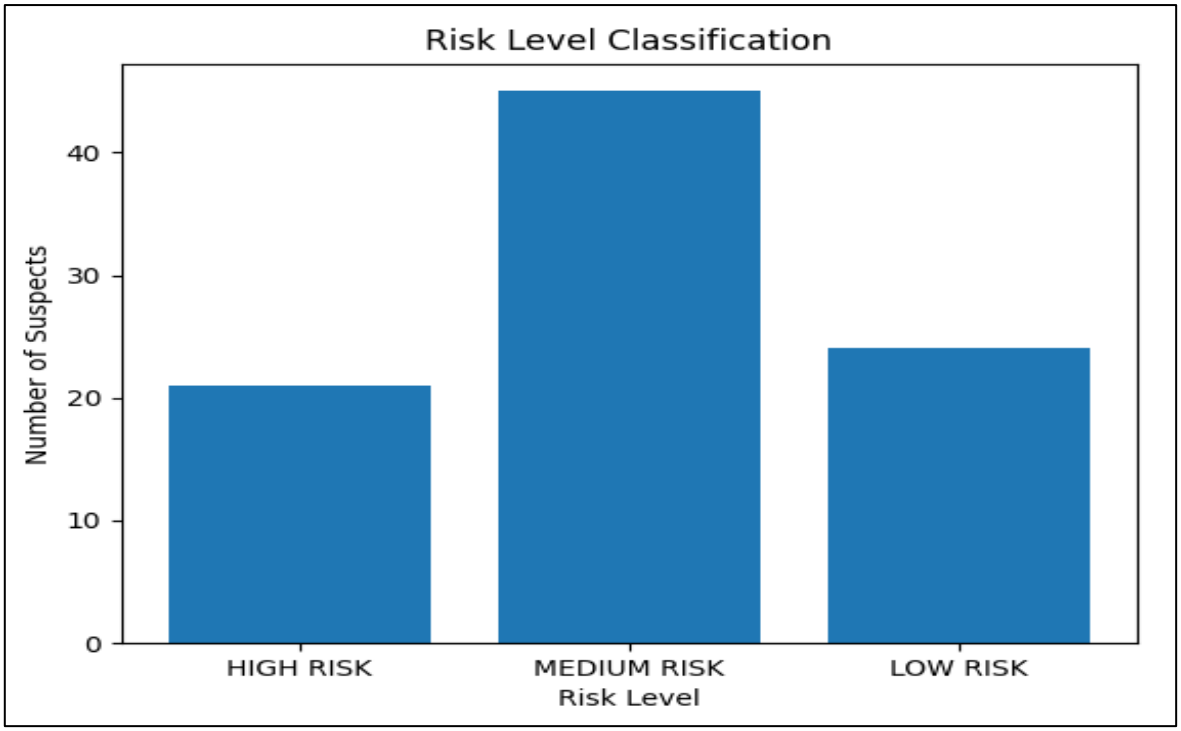

Fig 5 Risk Level Classification

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may579

Figure 5 indicates that the majority of suspects fall under the Medium Risk category, followed by High Risk, while fewer are classified as Low Risk. This shows that the system is sensitive in identifying individuals requiring monitoring.

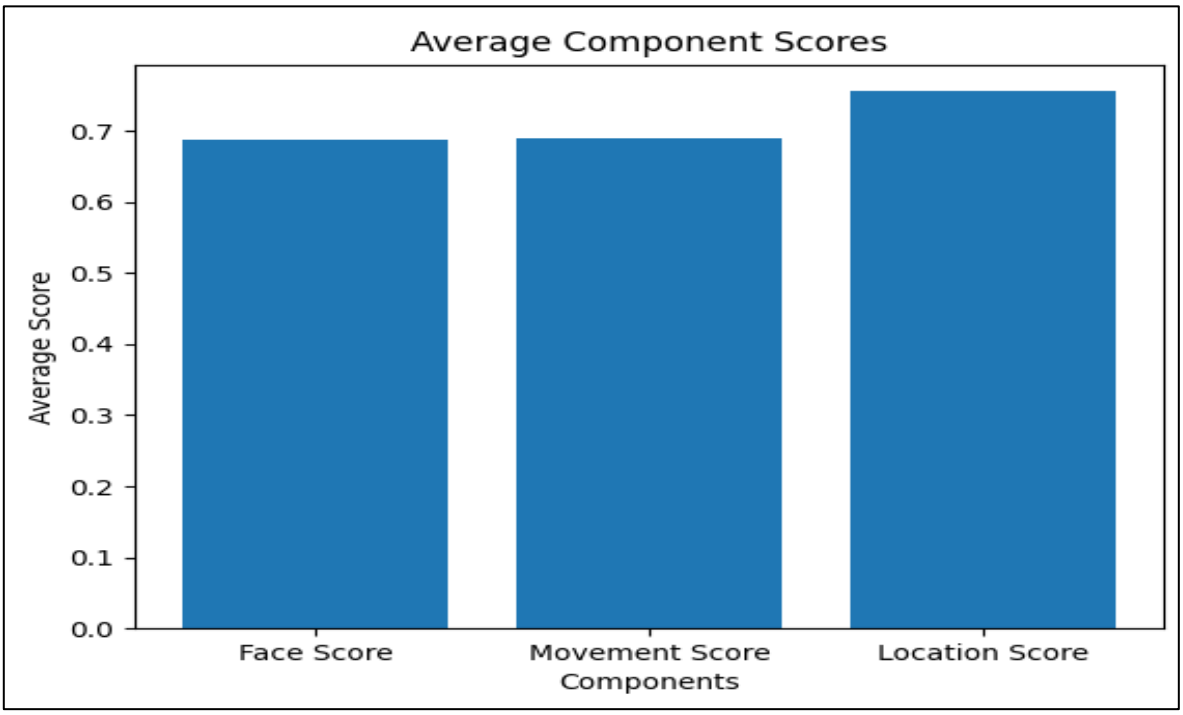

Fig 6 Average Component Scores

Figure 6 reveals that facial recognition has the highest average score contribution, followed by movement pattern, while location has the least contribution. This confirms that facial recognition is the most influential factor in the more.

B. Data Analysis and Presentation from the Questionnaire Results

➢ *Section A: Demographic Information*

Table 1 Gender Distribution

Gender	Frequency	Percentage (%)
Male	55	61.10
Female	35	38.90
Total	90	100

From the Table 1 it shows that majority of the respondents are male (55) representing 61.10% which indicates that they have dominated the sample as a result of their high involvement in educational sector, security sector as well as traditional rulers. The Female respondents are 35 represent 38.90% indicating low participation in education, security, and traditional rulers.

Table 2 Age Distribution

Age Group	Frequency	Percentage (%)
18–25	20	22.20
26–35	30	33.30
36–45	25	27.80
46+	15	16.70
Total	90	100

Table 2 indicated that majority of the respondents are within 26–35 years presenting 33.30%. This show that the youth are the leaders in areas such education, security and traditional rulers.

Table 3 Educational Qualification

Qualification	Frequency	Percentage (%)
Secondary School	15	16.70
NCE/ND	25	27.80

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may579

HND/BSc	35	38.90
Postgraduate	15	16.70
Total	90	100

Table 3 show that 35 of the respondents are HND/BSc holders representing 38.90%, 25 of the respondents hold NCE/ND certificates representing 27.80%, while the secondary school and postgraduate both have 15 respondents each representing 16.70 respectively.

Table 4 Occupation

Occupation	Frequency	Percentage (%)
Security Personnel	20	22.20
Civil Servant	18	20.00
Traditional Leader	10	11.10
Business Person	15	16.70
Student	20	22.20
Others	7	7.80
Total	90	100

Table 4 illustrated that majority of the respondents are security personnel and students 20 each representing 22.20% respectively. 18 civil servants representing 20.00%, we have 15 business person in the study representing 16.70%, 10 traditional rulers representing 11.10% while other are 7 representing 7.80%.

Table 5 Distribution of Respondents by Local Government Area (LGA)

LGA	Frequency	Percentage (%)
Dan Musa	30	33.30
Batsari	30	33.30
Safana	30	33.30
Total	90	100%

Table 5 shows that the respondents are evenly distributed across the three Local Government Areas, with Dan Musa, Batsari, and Safana each having 30 respondents representing 33.30% respectively. This indicates equal representation of the study areas, ensuring balanced responses across the selected LGAs.

Table 6 Years of Experience in Security-related Matters

Years of Experience	Frequency	Percentage (%)
1–5 years	25	27.80
6–10 years	20	22.20
11 years and above	15	16.70
Not Applicable	30	33.30
Total	90	100

Table 6 indicates that the highest number of respondents 30 (33.30%) reported not applicable in terms of security-related experience, while 25 respondents representing 27.80% have 1–5 years of experience. Additionally, 20 respondents (22.20%) have 6–10 years, and 15 respondents (16.70%) have 11 years and above. This shows that although many respondents lack direct experience, a considerable number possess relevant security knowledge.

- *Section B: Responses to Research Questions*

Table 7 Artificial Intelligence (AI) Technologies are Currently Being Applied in Some Selected LGAs of Katsina State to Support Security Operations.

Response	Frequency	Percentage (%)
Strongly Agreed	25	27.80
Agreed	30	33.30
Disagreed	10	11.10
Strongly Disagreed	5	5.60
Undecided	20	22.20
Total	90	100

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may579

Table 7 shows that the majority of respondents agreed (30 representing 33.30%) and strongly agreed (25 representing 27.80%) that AI technologies are currently being applied in selected LGAs. This indicates a general awareness and acceptance of AI usage in supporting security operations.

Table 8 AI Tools Such as Machine Learning, Intelligent Video Surveillance, and Data Analytics Improve Intelligence Gathering in Addressing Insecurity within the Selected LGAs.

Response	Frequency	Percentage (%)
Strongly Agreed	30	33.30
Agreed	35	38.90
Disagreed	8	8.90
Strongly Disagreed	5	5.60
Undecided	12	13.30
Total	90	100

Table 8 indicates that most respondents agreed (35 representing 38.90%) and strongly agreed (30 representing 33.30%) that AI tools improve intelligence gathering. This suggests that AI technologies are perceived as effective in enhancing security intelligence in the study areas.

Table 9 AI-Based Surveillance Systems (e.g., Smart Cameras and Drones) can Effectively Detect Crimes Such as Banditry, Kidnapping, and Cattle Rustling in the Selected LGAs.

Response	**Frequency**	**Percentage (%)**
Strongly Agreed	28	31.10
Agreed	32	35.60
Disagreed	10	11.10
Strongly Disagreed	6	6.70
Undecided	14	15.60
Total	90	100

Table 9 shows that the majority of respondents agreed (32 representing 35.60%) and strongly agreed (28 representing 31.10%) that AI-based surveillance systems can effectively detect crimes. This implies strong confidence in AI systems for crime detection within the selected LGAs.

Table 10 Sensor-Based Monitoring Systems and Predictive Analytics can Help Prevent Security Threats before they Occur.

Response	**Frequency**	**Percentage (%)**
Strongly Agreed	27	30.00
Agreed	33	36.70
Disagreed	9	10.00
Strongly Disagreed	6	6.70
Undecided	15	16.70
Total	90	100

Table 10 indicates that most respondents agreed (33 representing 36.70%) and strongly agreed (27 representing 30.00%) that sensor-based monitoring and predictive analytics can prevent security threats. This reflects a positive perception of AI in proactive security management.

Table 11 The Integration of AI into Security Operations Enhances Rapid Decision-Making and Response Time Among Security Agencies

Response	**Frequency**	**Percentage (%)**
Strongly Agreed	29	32.20
Agreed	34	37.80
Disagreed	8	8.90
Strongly Disagreed	5	5.60
Undecided	14	15.60
Total	90	100

Table 11 shows that the majority of respondents agreed (34 representing 37.80%) and strongly agreed (29 representing 32.20%) that AI integration enhances rapid decision-making and response time. This highlights the importance of AI in improving operational efficiency among security agencies.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may579

Table 12 Inadequate Infrastructure (Such as Internet Connectivity, Electricity Supply, and Technical Equipment) Affects the Effectiveness of AI-Driven Security Solutions in the Selected LGAs.

Response	Frequency	Percentage (%)
Strongly Agreed	35	38.90
Agreed	30	33.30
Disagreed	8	8.90
Strongly Disagreed	5	5.60
Undecided	12	13.30
Total	90	100

Table 12 indicates that most respondents strongly agreed (35 representing 38.90%) and agreed (30 representing 33.30%) that inadequate infrastructure affects the effectiveness of AI-driven security solutions. This suggests that infrastructural challenges remain a major barrier to AI implementation.

Table 13 Lack of Technical Expertise and Training Among Security Personnel Limits the Successful Adoption of AI Technologies in Katsina State.

Response	Frequency	Percentage (%)
Strongly Agreed	32	35.60
Agreed	33	36.70
Disagreed	10	11.10
Strongly Disagreed	5	5.60
Undecided	10	11.10
Total	90	100

Table 13 shows that the majority of respondents agreed (33 representing 36.70%) and strongly agreed (32 representing 35.60%) that lack of technical expertise limits AI adoption. This implies that skill gaps among personnel hinder effective utilization of AI technologies.

Table 14 Community Acceptance and Cooperation Play a Significant Role in the Successful Implementation of AI-Based Security Systems.

Response	Frequency	Percentage (%)
Strongly Agreed	28	31.10
Agreed	36	40.00
Disagreed	8	8.90
Strongly Disagreed	4	4.40
Undecided	14	15.60
Total	90	100

Table 14 indicates that most respondents agreed (36 representing 40.00%) and strongly agreed (28 representing 31.10%) that community acceptance plays a significant role in AI implementation. This highlights the importance of public cooperation in security initiatives.

Table 15 Government Support, Funding, and Policy Framework are Essential for the Effective Deployment of AI in Combating Insecurity in the Selected LGAs**.**

Response	Frequency	Percentage (%)
Strongly Agreed	40	44.40
Agreed	30	33.30
Disagreed	5	5.60
Strongly Disagreed	3	3.30
Undecided	12	13.30
Total	90	100

Table 15 shows that the majority of respondents strongly agreed (40 representing 44.40%) and agreed (30 representing 33.30%) that government support and funding are essential for AI deployment. This emphasizes the critical role of government in ensuring successful implementation.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may579

Table 16 I am willing to Support and Adopt AI-Driven Security Solutions as a Sustainable Strategy for Addressing Security Challenges in the Selected LGAs of Katsina State.

Response	Frequency	Percentage (%)
Strongly Agreed	33	36.70
Agreed	32	35.60
Disagreed	8	8.90
Strongly Disagreed	5	5.60
Undecided	12	13.30
Total	90	100

Table 16 indicates that most respondents strongly agreed (33 representing 36.70%) and agreed (32 representing 35.60%) that they are willing to support and adopt AI-driven security solutions. This suggests a high level of acceptance and readiness among respondents.

RECOMMENDATIONS

- The government should invest in AI-driven security technologies such as intelligent surveillance, drones, and data analytics systems. This will enhance real-time monitoring and improve response to security threats.
- Security personnel should receive regular training on the use of AI tools and technologies. This will ensure effective operation and maximize the benefits of AI in security management.
- AI technologies should be integrated with current security frameworks like CCTV and communication systems. This will improve coordination, intelligence sharing, and decision-making.
- Clear policies and regulations should guide the use of AI in security operations. This will ensure data privacy, accountability, and prevent misuse of technology.
- Communities should be educated and involved in AI-based security initiatives. This will build trust, encourage cooperation, and enhance the effectiveness of security measures.

ACKNOWLEDGEMENT

This Research is sponsored by Tertiary Education Trust Fund Nigeria (TETFUND) through Institution Based Research (IBR) grant of Federal College of Education Katsina, Kastina State, Nigeria at the Department of Computer Science.

➢ *Conflict of Interest*

The authors declared their in no conflict of interest.

REFERENCES

[1]. Syed, M. H., & Javed, W. (2023). Study of Artificial Intelligence in Cyber Security and the emerging threat of AI-driven cyber attacks and challenges. *Journal of Aeronautical Materials*, 43(1), 1557–1570.

[2]. Bai, J., Wu, Y., Wang, G., Yang, S. X., & Qiu, W. (2006). A novel intrusion detection model based on multilayer self-organizing maps and principal components analysis. *Lecture Notes in Computer Science*, 3973, 255–260. https://doi.org/10.1007/11760191_37

[3]. Radulov, N. (2019). Artificial intelligence and security: Security 4.0. *International Scientific Journal "Security & Future"*, 3(1), 3–5.

[4]. Russell, S., & Norvig, P. (2020). *Artificial intelligence: A modern approach* (4th ed.). Pearson.

[5]. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176.

[6]. Zhang, Y., Chen, L., & Wang, S. (2019). Real-time abnormal behavior detection using computer vision. *International Journal of Computer Vision & Security*, 7(2), 112–130.

[7]. Wang, X., & Brown, E. (2020). Predictive policing and resource allocation: An empirical study. *Policing: An International Journal*, 43(5), 865–880.

[8]. Lum, K., & Isaac, W. (2016). To predict and serve? Significance and challenges of predictive policing algorithms. *Annual Review of Law and Social Science*, 12, 355–371.

[9]. Garvie, C., Bedoya, A. M., & Frankle, J. (2016). *The perpetual line-up: Unregulated police face recognition in America*. Georgetown Law Center on Privacy & Technology.

[10]. Okoye, P., & Adeyemi, T. (2021). Artificial intelligence and border security in West Africa. *African Journal of Security Research*, 8(1), 73–89.

[11]. Iro, U., & Ogbonna, I. (2020). Socio-economic drivers of insecurity in Northern Nigeria. *Journal of Development Studies*, 12(3), 147–167.

[12]. Cummings, M. (2021). Artificial intelligence and the future of security policy. *Security Dialogue*, 52(4), 310–329.

[13]. Adetunji, O., & Olusanya, E. (2022). Challenges of AI adoption in low-resource settings: A focus on African security sectors. *Journal of Technology in Developing Regions*, 11(2), 234–250.

[14]. Ergen, M. (2019). What is artificial intelligence? Technical consideration and future perception. *Anatolian Journal of Cardiology*, 22(2), 5–7.

[15]. Okwor, U. D. (2022). Artificial intelligence as a tool for combating insecurity in Nigeria. Retrieved from https://engineersforum.com.ng/wp-content/uploads/2021/06/artificial-intelligence-as-a-tool-For-combating-insecurity-in-nigeria.pdf

[16]. Salisu, M. A., & Samuel, I. R. (2024). Harnessing artificial intelligence to address rising insecurity, ineffective governance, and economic downturns.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may579

International Journal of African Sustainable Development Research, 6(2), 55–66.

[17]. Miiro, E., & Kato, I. (2024). A machine-learning-based IoT smart home system to detect and reduce urban insecurity in Uganda: A case study of Kampala Metropolitan Area. In *2024 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)* (pp. 1–6). IEEE.

[18]. Igwenagu, C. (2016). *Fundamentals of research methodology and data collection*. Lambert Academic Publishing.

[19]. Nworgu, B. G. (2016). *Educational research: Basic issues and methodology* (Revised and enlarged ed.). University Trust Publishers.

[20]. Bolarinwa, O. A. (2015). Principles and methods of validity and reliability testing of questionnaires used in social and health science research. *Nigerian Postgraduate Medical Journal*, 22(4), 195–201.

[21]. Ikuno, J. C., Wrulich, M., & Rupp, M. (2010). System-level simulation of LTE networks. In *2010 IEEE 71st Vehicular Technology Conference (VTC Spring)* (pp. 1–5). IEEE.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may579

APPENDIX 1

Department of Computer Science Federal College of Education Katsina Kastina State Nigeria

Dear Respondent

I am researcher from the above department and institution conducting a research with the title "The use of Artificial Intelligence (AI) to checkmate security challenges in Katsina State. (A Case Study of some selected Local Government Areas). I would be glad if you provide me with the information needed in the questionnaire, I promise to treat all information given by you as confidential and would be used only for this research work. Thanks.

A. Section A

➢ *Section A: Demographic Information*
Please tick (✓) the appropriate option.

- Gender:

☐ Male
☐ Female

- Age Group:

☐ 18–25 years
☐ 26–35 years
☐ 36–45 years
☐ 46 years and above

- Educational Qualification:

☐ Secondary School
☐ NCE/ND
☐ HND/Bachelor's Degree
☐ Postgraduate Degree

- Occupation:

☐ Security Personnel
☐ Civil Servant
☐ Traditional Leader
☐ Business Person
☐ Student
☐ Others (Specify) _____

- Local Government Area (LGA):

☐ _____

- Years of Experience in Security-related Matters (if applicable):

☐ 1–5 years
☐ 6–10 years
☐ 11 years and above
☐ Not Applicable

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may579

B. Section B

- Artificial Intelligence (AI) technologies are currently being applied in some selected LGAs of Katsina State to support security operations.

a) Agreed
b) Disagreed
c) Strongly Agreed
d) Strongly Disagreed
e) Undecided

- AI tools such as machine learning, intelligent video surveillance, and data analytics improve intelligence gathering in addressing insecurity within the selected LGAs.

a) Agreed
b) Disagreed
c) Strongly Agreed
d) Strongly Disagreed
e) Undecided

- AI-based surveillance systems (e.g., smart cameras and drones) can effectively detect crimes such as banditry, kidnapping, and cattle rustling in the selected LGAs.

a) Agreed
b) Disagreed
c) Strongly Agreed
d) Strongly Disagreed
e) Undecided

- Sensor-based monitoring systems and predictive analytics can help prevent security threats before they occur.

a) Agreed
b) Disagreed
c) Strongly Agreed
d) Strongly Disagreed
e) Undecided

- The integration of AI into security operations enhances rapid decision-making and response time among security agencies.

a) Agreed
b) Disagreed
c) Strongly Agreed
d) Strongly Disagreed
e) Undecided

- Inadequate infrastructure (such as internet connectivity, electricity supply, and technical equipment) affects the effectiveness of AI-driven security solutions in the selected LGAs.

a) Agreed
b) Disagreed
c) Strongly Agreed
d) Strongly Disagreed
e) Undecided

- Lack of technical expertise and training among security personnel limits the successful adoption of AI technologies in Katsina State.

a) Agreed
b) Disagreed
c) Strongly Agreed

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may579

d) Strongly Disagreed
e) Undecided

- Community acceptance and cooperation play a significant role in the successful implementation of AI-based security systems.

a) Agreed
b) Disagreed
c) Strongly Agreed
d) Strongly Disagreed
e) Undecided

- Government support, funding, and policy framework are essential for the effective deployment of AI in combating insecurity in the selected LGAs.

a) Agreed
b) Disagreed
c) Strongly Agreed
d) Strongly Disagreed
e) Undecided

- I am willing to support and adopt AI-driven security solutions as a sustainable strategy for addressing security challenges in the selected LGAs of Katsina State.

a) Agreed
b) Disagreed
c) Strongly Agreed
d) Strongly Disagreed
e) Undecided