Efficacy of Fingerprint and Facial Recognition in Enhancing National Security in Kenya

[1]Mr. Fredrick Odhiambo Ouma, [2]Dr. John R Kisilu, [3]Dr. Anthony Luvanda

[1, 2, 3]National Defence University, Kenya

DOI: https://doi.org/10.51584/IJRIAS.2025.100900090

Received: 18 September 2025; Accepted: 24 September 2025; Published: 25 October 2025

ABSTRACT

This study explores the efficacy of fingerprint and facial recognition technologies in enhancing national security in Kenya. As the issue of crime, fraud, and border security has been increasing, the use of biometric systems has been embraced to enhance the process of identity verification in government agencies. The study was guided by securitization theory, which frames issues as security threats requiring urgent attention, and diffusion of innovation theory, which examines how new technologies spread and are adopted. Securitization Theory highlighted biometric systems as key to national security, while Diffusion of Innovation Theory helped explain the factors influencing public acceptance. Quantitative and qualitative data were collected by a mixed-approach methodology. The questionnaire that was prepared was given to 397 randomly selected members of the population and 30 governmental officials (National Police Officers, Immigration Personnel, KRA Customs Officials and National Intelligence Personnel. Also, 30 key informant interviews were carried out to collect in-depth knowledge of their perceptions, experiences, and issues on biometric systems. The analysis of the data was conducted based on the descriptive statistics and the regression analysis to find connections among the factors that affect the national security. This research sought to evaluate familiarity, implementation, accuracy, and effect of the use of biometric systems on crime detection, reduction of fraud, and effectiveness of the border security. The results indicate that 89.6% of the respondents are conversant with biometric systems, and 83% of them (respondents) indicate the presence of such technologies in their respective organizations. On accuracy, majority of respondents were satisfied or very satisfied (80.2%) with the performance of these systems. Nonetheless, issues of system failures, lack of training, and opposition by the populace were noted as obstacles to the complete adoption of biometric technologies. Although these have been raised, 80.2% of the respondents noted that biometric systems have a positive effect on crime detection and reduction of frauds, with almost half (47.2%) indicating that the effects are significant. The research findings are that biometric systems are a positive contribution toward the national security in Kenya, but their success is adversely affected by the operational and social barriers. The recommendations of this study were investing in the upgrades of infrastructure, offering continuous staff training, dealing with issues of public trust, fortification of legal frameworks, and encouraging inter-agency cooperation, enhancing integration and effectiveness. Through these issues, Kenya will be able to realize the full potential of biometric technologies in securing the borders of the country and advancing the law enforcement process.

Keywords: Biometric Systems, National Security, Fingerprint Recognition, Crime Detection, Border Security

INTRODUCTION

Fingerprint recognition systems, facial recognition and iris scanning among others under biometric identification systems have become a key element of improving national security in various parts of the world. These systems exploit some specific physiological or behavioral traits to positively recognize people in an appropriate manner, which offer superior security benefits compared to the traditional method of people identification like passwords or physical tokens. The requirement to improve the security operations has also facilitated the rising popularity of biometric technologies in the global context in the post-9/11 world (Afolabi, 2020; Toesland, 2021). Some of the countries that have already integrated the biometric systems in their national security strategy include United States, United Kingdom, and India, which have been using the technologies in protecting their borders, combating fraud and identifying criminals. The effectiveness of the biometric identification systems in these regions has been greatly identified, and scientific reports have

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IX September 2025

estimated that the occurrence of identity frauds, illegal immigration, and terrorism related activities have reduced tremendously (Chen *et al.*, 2022; Khan and Efthymiou, 2021). However, as the biometric systems continue to be increasingly used, the questions of the privacy, data confidentiality, and the ethics are becoming more evident (Gonzalez-Gonzalez *et al.*,2025). These have led to debates about whether national security is a priority or the basic rights of the citizens need to be satisfied.

The increasing use of biometrics systems in Africa has also seen the related development through international organizations such as the African Union (AU) and the United Nations (UN) to popularize their application as a security-enforcing tool. Biometric technologies have been presented as solutions to the challenges confronting people in response to serious security challenges such as terrorism, cross-border crime, and human trafficking. South Africa, Nigeria, and Rwanda are already establishing systems of biometrics into key national operations, such as voter registration, immigration management, or managing national identities (Wienroth & Amelung, 2023). Nevertheless, issues still exist with wider adoption of such systems, particularly in the developing world. Poorly developed infrastructure, lack of resources, and strong legal and regulatory frameworks to address security of data of citizens poses major obstacles (Jain *et al.*, 2011; Gelb and Clark, 2019). Furthermore, the fear of surveillance, use of data, and oppression by the government impairs the use of these systems in totality and efficacy due to the lack of trust people place on them (Tsiftsi, 2024). The use of biometric technologies in Africa raises ethical and privacy concerns that should be served deeper, especially in terms of balancing national security goals with the safeguarding of the digital privacy rights of citizens.

Biometric technologies have become a trend in Kenya due to increasing security threats like terrorism, identity theft, and human trafficking, which has given the current security organs of the country a run that it never anticipated. The government has realised that biometric systems have the potential to modernise its national identification systems and enhance national security. One of the major projects, the Huduma Namba, involves integrating such biometric images as facial recognition and fingerprints to enhance the verification of the identity and the security (Oyosi, 2024). But implementation of the Huduma Namba has had its problems. In 2021, the Kenyan High Court declared the program unconstitutional because of the defects in the procedures and legislation (Kiilu, 2022). Nevertheless, the Kenyan government persistently advocates the use of biometric technologies regardless, as the Maisha Namba project is in the pilot phase. This is expected to unite the biometrics and demographic information that would facilitate the administration of government services and improve the identity scrutinizing measures (Kemboi, 2025). Although these projects are expected to lead to improvement, their adoption is faced with privacy, legal, and ethical issues that continue to be a critical barrier to their success.

The utilization of the theory of Securitization can also be used to analyze the application of biometric systems as anti-terrorism and anti-fraud policy in Kenya. Under the Securitization Theory, security risks are seen through the prism of existential crises that legitimize extraordinary actions, and circumvent ordinary processes to tackle the challenge. The Kenyan government aligns biometrics systems with control of those troubles that threaten national security, such as terrorism, fraud, and identity theft. This framing has facilitated implementation of bio-metric technologies despite the existence of privacy concerns and abuse of the right of civil liberties. Nevertheless, such a method causes considerable privacy and ethical concerns. With the increased integration of biometrics into the system of national security, issues of surveillance, the abuse of personal information, and the loss of the right to privacy increase. The benevolence of legal and regulatory frameworks to safeguard the digital rights of citizens is only a contributory factor to the occurrence of such issues (Lowell, 2023; Cambaco *et al.*, 2021). Thus, the discussion of the biometric systems in Kenya must not be focused solely on the assessment of whether they work best at boosting the national security, but also the consumption of the ethical assumptions, popular confidence, and legislations that are shaping their implementation and success. A such, this study aimed at assessing the efficacy of fingerprint and facial recognition technologies in enhancing national security in Kenya.

Aim

To assess the efficacy of fingerprint and facial recognition technologies in enhancing national security in Kenya.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IX September 2025

THEORETICAL FRAMEWORK

The rise of biometric identification systems in Kenya in improving national security is explicable in terms of two broad theoretical frameworks that include the Securitization Theory and Diffusion of Innovations Theory. These theories offer different but complementary perspectives on the justification of biometric technologies as a necessity in national security and their diffusion in the Kenyan society (Buzan *et al.*,1998).

Securitization Theory: as expounded by Waever and Buzan (1998), they discuss the formulation of issues as existential things as incomplete and, therefore, necessitating extraordinary treatment. Biometrics technologies like fingerprint and face recognitions are prepared to play a vital role against the regulatory of terrorism, fraud, and identity theft in Kenya. The government describes such technologies as necessary to protect the security of the country and describes security threats as being so pressing that they required the shortcuts of breaking the normal legislative process (Waever, 1995). With this framing, it is possible to adopt biometric systems decades notwithstanding issues of privacy. Although, the introduction of these technologies onto the scenario usually causes the attenuation of civil liberties. The widespread utilization of biometric systems is viewed by the Kenyan population as a possible infringement of the right to privacies primarily because the government has traditionally feared those tools and believes in collecting target data and data abuse (Cambaco *et al.*, 2021). Although national security is the priority, the social cost of shrinkage of civil liberties is usually relegated, which is one of the main weaknesses in Securitization Theory that does not take into account the fear by the population in being criminalized and abusing their personal data.

An alternative, the Diffusion of Innovations Theory formulated by Everett Rogers (1962), presents an alternative to conceptualization of the adoption of new technological systems such as Biometric systems. This theory states that innovations move in particular stages and the different social groups acquire technologies at various frequencies, namely, the knowledge stage, persuasion level, decision stage, implementation stage, and confirmation stage. In Kenya the government, which is the change agent of innovation, leads in the adoption of biometrics systems in the country to advance national security as well as regulate the delivery of administrative services. Biometric systems become adopted quickly among the early adopters, specifically by government agencies and urban residents having higher access to technology (Jain, 2019). Nevertheless, the wider population acceptance is slower. As government actors talk about the security advantages of the biometric technologies, people feel fear but are motivated by a lack of trust on issues of privacy and state surveillance (Onuigbo, 2021). Socio political and economic factors like digital inequality, a general distrust of government-led endeavors contribute to this division.

The combination of both the Securitization Theory and Diffusion of Innovations Theory gives a holistic explanation of the use of biometric systems in Kenya. As much as the Securitization Theory puts emphasis on the framing of biometric technologies as solutions that are required to counter the existential threats, it also presents the trade-off scenario between national security, and civil liberties. The Kenyan government defends the implementation of biometric systems by referring to the crucial necessity to fight terrorism and fraud, whereas the population has serious concerns about the possibility to be monitored and the fact that privacy is decreasing (Waever, 1995; Cambaco *et al.*, 2021). The theory in large part focuses on diffusion of Innovations, which supports the adoption at varying rates towards the government and the population. Biometric technologies are rapidly adopted by government agencies and urban areas, and more commonly resisted in rural regions and by citizens concerned with their privacy (Wambui *et al.*, 2022). Collectively, these theories show how political needs and citizens influence the implementation of biometrics systems in Kenya which provides a better understanding of how they affect national security and society.

METHODOLOGY

The study was focused on a total of 58,240 participants, including 49, 000 travelers and 9,100 truck drivers crossing through the Namanga One-Stop Border Post (OSBP) and 140 government officials working on the implementation of biometric systems. The number of the travelers and truck drivers was calculated in accordance with the formula applied by Yamane (1967), which means the sample will consist of about 397 participants. In the case of government officials, in the first case a sample of 104 was obtained, but a practical limitation constrained it to a sample of 30. The governmental sample was distributed proportionally, which

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IX September 2025

contained 9 National Police Officers, 8 Immigration Personnel, 10 KRA Customs Officials, and 3 National Intelligence Personnel. The study used a total of 427 respondents, which comprised of public members and government officials. The sample size was considered sufficiently large to provide relevant information given the time and resource constraints. Government officials were apportioned accordingly to its number in each category and

gave fair representation in the sample.

The study was also carried out in an ethical manner where informed consent was taken among the participants and the research was kept confidential. Ethical consent was obtained through authorities in charge and such authorities included the Ministry of Interior, the National Police Service, and Immigration Department. Pre-testing of the research instruments helped to assure reliability and validity and Cronbach Alpha showed high internal consistency. The data collection was done by administering questionnaires to the population at Namanga OSBP and interviewing government officials within the premises. The methodology used in the study presented a holistic approach in that both quantitative and qualitative methods were used to ensure that the entire scope of the issue of the effects of biometric systems on national security was represented. This qualitative and quantitative design gave a chance to comprehend the effectiveness, issues, and social acceptability of these systems in the Kenyan security system in a subtle manner.

FINDINGS

Efficacy of Fingerprint and Facial Recognition in Enhancing National Security

The primary aim of this study was to examine the efficacy of fingerprint and facial recognition in enhancing national security in Kenya. To meet this objective, the structured questions were asked and results were presented in the following subsections;

Familiarity and Implementation of Biometric Systems

This section explores respondents' familiarity with biometric identification systems and whether their organizations have implemented such systems. The findings provide insight into their exposure to biometric technologies and their role in national security practices.

Table 1: Familiarity and Implementation of Biometric Systems

Variable	Yes	No	Total
Familiar with Biometric Systems	269 (89.6%)	31 (10.4%)	300 (100%)
Organization Implemented Biometric Systems	249 (83.0%)	51 (17.0%)	300 (100%)

Source: Researcher, (2024)

Table 1 indicates the respondent-level familiarity with biometric systems and their use by organizations. Out of the 300 respondents, 89.6% (269) said that they were aware of biometric systems, and 10.4% (31) indicated that they were not. In terms of implementation of biometrics systems in their organizations, 83.0% (249 respondents) agreed that their organizations had implemented biometric systems, with 17.0% (51 respondents) on the opposite admitting that their organizations had not implemented the strategies. These results demonstrate that the awareness of biometric systems and their prevalence are highly popular and widespread, specifically in the framework of border control operations.

Identification Accuracy

The study sought to assess the effectiveness of biometric systems in accurately identifying individuals. The section outlines respondents' perceptions of the reliability and accuracy of biometric identification technologies, such as fingerprint and facial recognition, in real-world applications.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IX September 2025

Table 2: Satisfaction with Accuracy of Biometric Systems

Response	Frequency	Percent
Very Satisfied	113	37.7%
Satisfied	128	42.5%
Neutral	34	11.3%
Dissatisfied	17	5.7%
Very Dissatisfied	8	2.8%
Total	300	100%

Source: Researcher, (2024)

Table 2 shows the respondent satisfaction with the precision of the biometric systems in Namanga One-Stop Border Post (OSBP). Most of the people who took part were satisfied with the systems indicating that 42.5% (128 individuals) noted that they were satisfactorily accurate, whereas 37.7% (113 respondents) indicated their high level of satisfaction. A smaller percentage, 11.3% (34 respondents), were neither satisfied nor dissatisfied, and a small percentage, 2.8% (8 respondents) indicated that they were very dissatisfied with the accuracy of the system used. These findings indicate an overall favorable attitude toward the accuracy of the biometric systems with a large percentage of the respondents rating their satisfaction or high satisfaction levels.

A respondent of one governmental officials highlighted that the system is reliable and said:

" Accuracy of the biometric system has enabled us to enhance security and efficiency at the border that is vital in the management of large numbers of people and goods." [Interviewee 4].

This assertion points out how successful the system is seen to be in its effectiveness and accuracy in improving operational efficiency. Nevertheless, there was a low percentage of respondents who were not content or highly discontented with the accuracy of the system. One respondent (who was not satisfied) remarked:

" In some cases, the system may be slow in confirming information hence leading to delays at the border." [Interviewee 5].

The presence of this statement underlines the largest positive attitude to the effectiveness and the fact of enhancing operational efficiency of the biometric system. A very low percentage of the affected respondents seem dissatisfied although some people complained about system delays causing breakage of border crossings. The slow processing of the final deliveries was a particular factor of frustration to one of the respondents.

Crime Detection and Prevention

This sub-section explored the role of biometric systems in crime detection and prevention. It examines respondents' views on whether biometric technologies have contributed to reducing crime within their respective areas of work.

Table 3: Impact of Biometric Systems on Crime Detection and Prevention

Response	Frequency	Percent
Yes, significantly	142	47.2%
Yes, to some extent	99	33.0%

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IX September 2025

No, it has had no effect	43	14.2%
No, it has worsened the situation	17	5.7%
Total	300	100%

Source: Researcher, (2024)

Respondent perception of the role of the biometric systems in preventing and detecting crime at the Namanga One-Stop Border Post (OSBP) are represented in Table 3. Most of the respondents, 47.2% (142 respondents) were of the view that biometric systems have had a huge effect in crime detection and prevention and 33% (99 respondents) respondents thought that systems have influenced crime detection and prevention. However, 14.2% (43) indicated no effect, and 5.7% (17) indicated that they believed that the systems had aggravated the situation. The results are consistent with those provided in the study conducted by Qu et al. (2019), who stressed the importance of the biometric systems in increasing the security levels and crime prevention in the high-risk zones such as the border areas. One respondent in the governmental officials commented:

"Biometric systems have also assisted in apprehending criminals attempting to cross the border under false identities, and this has greatly enhanced security." (Interviewee 3).

Some respondents was apprehensive about the efficiency of the technology, with one respondent stating:

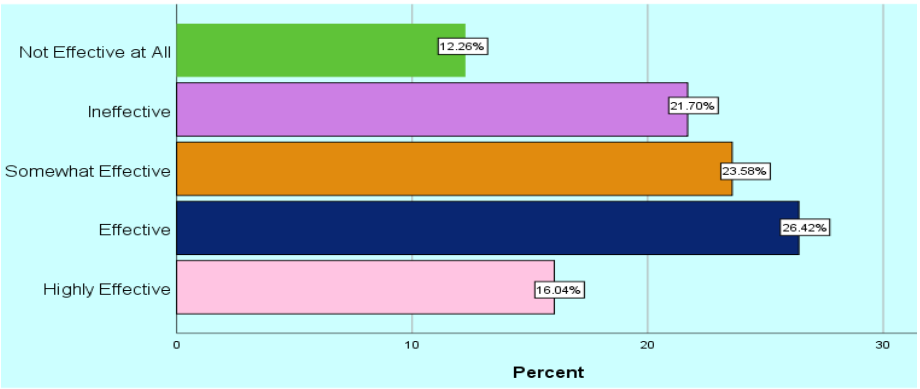
"The biometric system also provides false readings at times and criminals are able to pass through the system because the system fails." [Interviewee 7].

These fears are in line with the evidence by Andrejevic and Selwyn, (2020) who observe that despite the benefits of biometric systems in enhancing security, they may also bring certain problems including false alarms or delays in processing, which may negate their potential in preventing crime. In spite of these, the overall view is generally positive as majority of the respondents acknowledge the valuable contribution of biometric systems in enhancing security and help in curbing crime in Namanga OSBP.

Border Security Effectiveness

The study aimed at assesses respondents' views on the effectiveness of biometric systems in enhancing border security.

Figure 1: Border Security Effectiveness



Source: Researcher, (2024)

Figure 1 shows the respondent views on the effectiveness of biometric systems in enhanced border security. Most of them (42.4%) were seen to have rated the systems either as effective (26.4%) or said to have been somewhat effective (23.6%). Nonetheless 33.9% believed that they were either ineffective (21.7%), or zero (12.3) but 16% thought that they were highly effective. With these findings, it is possible to note that although

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IX September 2025

biometric systems are recognized as potentially effective with regard to border security, there is still a substantial number of people who is not convinced about the overall efficiency of the technology, and thus additional efforts are required to achieve that the people trust the technology. This feeling can be claimed to be in line with the qualitative developments as in this instance the participants indicated both benefits and drawbacks of biometric technologies. The thematic coding of the interviews of the key informants (KII) revealed that there were very complex issues that were in the pathway to what biometric systems can actually accomplish in regard to realizing the potential of these systems. One of the senior immigration officers has referred to the duality of such systems as an example.

"The biometric system can be effective to check people at the borderline, but the rates of its efficiency are usually compromised through system failures and natural phenomena such as low light conditions or broken equipment" (KII 004).

This assertion actually confirms the quantitative evidence, which outlines a division in the thought of the efficacy of the system, with quite a previous part of the patients acknowledging that it could likely be efficient but lacked trust because of the technical frontiers.

Fraud Reduction

The study sought to explores the impact of biometric systems on fraud reduction within organizations.

Table 4: Contribution of Biometric Systems to Fraud Reduction

Response	**Frequency**	**Percent**
Major Contribution	126	42.5%
Moderate Contribution	113	37.7%
Minor Contribution	43	14.2%
No Contribution	18	5.7%
Total	**300**	**100%**

Source: Researcher, (2024)

Table 4 summarizes the perception of the respondents on the extent to which biometric systems have helped in fraud reduction in their respective organizations. Majority (42.5%) noted that biometric systems have contributed significantly, and 37.7% stated moderately. The findings revealed that (14.2%) of the survey participants thought that there was a moderate contribution and 5.7% thought that there was no contribution of biometric systems in prevention of fraud. It means that even though biometrics systems are considered a way to prevent fraud, the impact of its use can be dependent on other factors, such as how well a system is designed and what the situation inside an organization is. These ambivalent reactions highlight the need to persistently upgrade and tweak to ensure that biometric systems are employed to their full capacity in regard to the process of fraud prevention.

This observation is also supported by qualitative responses. As an example, a key informant in the National Registration Bureau expressed:

"The introduction of biometric systems has helped in identifying fraudulent identities, but the systems still face integration challenges, especially when connecting to older databases" *(KII 005).*

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IX September 2025

This quote directly supports the quantitative evidence, which reveals that although biometric systems are perceived to be useful resources when it comes to reducing fraud, their effectiveness is dependent on the successful integration with available infrastructure.

Barriers to Biometric System Implementation

This section explores the barriers to the successful implementation of biometric systems, based on the respondents' views. Using a Likert scale, where 1 represents Strongly Disagree, 2 represents Disagree, 3 represents Neutral, 4 represents Agree, and 5 represents Strongly Agree, the study identifies key challenges such as funding issues, technical difficulties, public resistance, training limitations, and legislative obstacles.

Table 5: Barriers to Biometric System Implementation

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	SD	Mean
There is a lack of funding for implementing biometric systems.	43 (14.2%)	85 (28.3%)	57 (18.9%)	71 (23.6%)	45 (15.1%)	0.99	3.2
Technical challenges hinder the successful deployment of biometric systems.	30 (9.4%)	57 (18.9%)	43 (14.2%)	71 (37.7%)	45 (19.8%)	1.02	3.5
Public resistance to biometric systems is a significant barrier to implementation.	14 (4.7%)	43 (14.2%)	57 (23.6%)	71 (37.7%)	45 (19.8%)	0.92	3.6
Insufficient training for staff limits the effective use of biometric technologies.	36 (11.3%)	54 (17.0%)	64 (20.8%)	67 (30.2%)	45 (20.8%)	1.01	3.5
Legislative challenges prevent the implementation of biometric systems.	24 (7.5%)	48 (15.1%)	57 (26.4%)	72 (35.8%)	45 (15.1%)	0.94	3.3

Source: Researcher, (2024)

Table 5 shows that there are a few obstacles to the deployment of biometric systems according to the opinions of the respondents. The statement of the insufficiency of funding to implement biometric systems had a mean score of 3.2, which means that 23.6% of the respondents agreed and 15.1% strongly agreed that funding constraints are also a big barrier as perceived by a section of the respondents. Technical issues were also identified as a significant concern with a mean score of 3.5 indicating that 57.5% (37.7% agreed and 19.8% strongly agreed) believed that technical problems, including system integration and system downtimes, are obstacles to the successful implementation of biometric systems. In the same manner, it was detected that public opposition to biometric systems was a serious impediment with mean score of 3.6 as 57.5% of the respondents (37.7% agreed and 19.8% strongly agreed) held the opinion that opposition to biometric systems among the populace is a major barrier to implementation.

Regarding training, the mean of the statement, Insufficient training of staff limits the effective use of biometric technologies was 3.5, and 51% of the respondents (30.2% agreed and 20.8% strongly agreed) indicated that staff training is a significant factor that inhibits the efficacy of such systems. Legislative barriers, scoring 3.3 were also cited as a major barrier, with half of the respondents (35.8% said yes, and 15.1% strongly said yes) agreeing that legal and regulatory frameworks must be strengthened to make it fully implemented. The mean of 3.4 of the total number of statements shows that there is an agreement that the phenomena of financial,

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IX September 2025

technical, public resistance, training and legislative barriers all influence successfully used and implemented biometric systems in Kenya.

The barriers have highlighted the necessity of concerted efforts in the form of improved funding, technical improvements, community engagement, and sound legal provisions, in order to facilitate the success of biometric systems in the area of national security, as well as other programs. Qualitative data further support these findings. A senior officer of the Immigration Department remarked:

"The strength of biometric systems lies in their ability to accurately identify individuals and enhance border control, but the weaknesses come when the systems fail to integrate with other databases and when there are technical downtimes" (KII 007).

This is consistent with the quantitative data that suggests that even though biometric systems have potential, they cannot work due to integration problems and technical malfunctions. This feedback connects to the operational difficulties faced during biometric system implementation, particularly when the systems are under high demand. One respondent from the National Police Service pointed out:

"The major challenge we face is ensuring accuracy during peak hours when the systems are overloaded, and the accuracy drops, leading to false positives or missed identifications" (KII 04).

The statement highlights the issues pertaining to overload and accuracy at high traffic periods, a factor that has a crucial impact to biometrics system reliability. These technology problems are vital in discovering the deficiencies of biometric technologies, particularly as their real performance is experimented under stress within a state.

DISCUSSIONS

The studies to determine the efficacy of the finger print and facial recognizing technologies in enhancing national security in Kenya have not only been successful on an intimate scale, but have also encountered tremendous obstacles. The understanding of biometric systems was also good as 89.6% of the respondents expressed the fact of their familiarity, and 83% of them approved to have implemented the system in their organizations. These results coincide with other studies, such as that by Chen *et al.,* (2022) and/or Khan and Efthymiou, (2021), that focused on the popularity of biometric systems in government and security systems across various countries. High adoption in Kenya matches the trends in the globally recognized world where more biometrics are applied in the context of national security such as border control, identity verification, and the prevention of fraud.

In terms of biometric system accuracy, most respondents expressed satisfaction, with 80.2% stating that they were either very satisfied or satisfied. The result aligns with Madhumita, (2023), who observed that many developing nations have high satisfaction rates with the accuracy of biometric technologies, especially in the identification of people and fraud prevention. Nevertheless, the efficacy of biometric systems is, as Wambui *et al.,* (2022) highlighted, susceptible to the environmental factors, as well as technical problems, which was also mentioned in this work. Many of the respondents grumbled about system outages, poor lighting, and broken hardware, which Onuigbo, (2021) and Crumpler and Lewis, (2021) analyze as the obstacles to rolling out biometric systems in mass scale on a resource-constrained base.

In terms of crime detection and prevention, 80.2% of the respondents said that biometric systems have improved crime detection and prevention in a significant or moderately way. This finding is in line with other reports, such as those made by Qu *et al*., (2019), who have determined that the biometric systems could be key to reducing identity fraud and increasing the effectiveness of law enforcement. However, Zhang *et al*., (2025) and Soto-Beltran *et al.,* (2022) have highlighted that such a perception of usefulness of biometric system could be determined by the elements of its integration, as well as the confidence of people. This is evident in the current research where some of the people interviewed mentioned that the systems did not in any way have an effect and that they actually increased the situation though this may also be seen in Liu and Tu, (2021) and

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IX September 2025

Kitsiou *et al.,* (2022) where they claimed the case of the misuse of the biometric data and that they in fact deteriorated the sight of people.

In the implementation barriers, the research identified some of the critical hurdles as the problem of funding, technical issues, opposition, inadequate training and legislative problems. Such obstacles are in line with the discoveries of Alkhasawneh, (2020) and Ahmad *et al*., (2018) who contended that biometric systems have substantial advantages, but their effective utilization in practice frequently relies on the possibility to overcome these practical challenges. Ogunwole *et al.,* (2023) noted that technical challenges were the most cited challenges that involved system downtimes and integration issues with the legacy systems were the most notable obstacle to the mass adoption of biometric technologies. In this case, Arora, (2025) has explained that this has been affected by public opposition based on issues of privacy and data security which has not made complete adoption of biometric systems in some countries. The results of the current study, especially the concerns expressed by the respondents of the issue with the system accuracy in the periods of the highest traffic in the system and the problems with the integration, indicate the necessity of the further improvement of the technology and enrich the staff with the additional training.

Lastly, the findings of the study regarding the role played by biometric systems in curbing fraud are consistent with those of the past, including those of Khan and Efthymiou, (2021), who reported that biometric systems have played a significant role in curbing fraud and enhancing security in different industries. Nevertheless, according to Buckley and Nurse, (2019), biometric systems may not be effective in reducing fraud because the systems may differ in quality and the level of integration into the current infrastructure. This is further supported by qualitative responses by key informants who indicated that the effectiveness of biometric systems in preventing fraud depends on managing and overcoming integration challenges as well as making sure the systems are maintained.

CONCLUSION

The study has shown that fingerprint and facial recognition technologies can do much to boost national security in Kenya whereby biometric systems contribute to better crime detection, less fraud and enhanced security at the boundaries. Most of the respondents claimed to be content with the accuracy and efficiency of such systems, but technical faults, opposition among the population, absence of sufficient training, and influence of laws do pose some ambitious hindrances to full implementation of such systems. These findings are in line with the findings of other studies who lay the emphasis on the importance of breaking the challenge of infrastructure, increasing the public confidence and ensuring an adequate funding and training to maximize biometric systems. The results disseminate what the continuous development of the system integration, functioning efficiency, and policy agenda would be in order that the biometric technologies could achieve the targeted success in increasing the level of security in the country.

RECOMMENDATIONS

To increase effectiveness of biometric systems in aid of national security in Kenya, it is possible to recommend that the government must invest in the improvement of the infrastructure to reduce occurrence of technical failures, ongoing training of employees to help to improve efficiency of operation, and engage the population in campaigns to build trust in the biometric systems. Furthermore, the strengthening of legal and regulatory infrastructure offering privacy and data security, and improved inter-agency coordination will invite biometric systems to be more easily integrated and effective across domains. The solutions to these regions will result in the entire potential of biometric technologies being realized to enhance national security.

REFERENCES

1. Afolabi, O. S. (2020). Biometric Technologies, Electoral Fraud and the Management of Elections in Nigeria and Zimbabwe. The Strategic Review for Southern Africa, 42(2), 205-229.
2. Ahmad, S. M. S., Ali, B. M., & Adnan, W. A. W. (2018). Technical issues and challenges of biometric applications as access control tools of information security. International journal of innovative computing, information, and control, 8(11), 7983-7999.

3. Arora, A. (2025). Challenges of Integrating Artificial Intelligence in Legacy Systems and Potential Solutions for Seamless Integration. Available at SSRN 5268176.
4. Bacon, H., & Warner, D. (2021). Ethical concerns in the implementation of biometric identification systems. International Review of Data Protection, 15(3), 98-112.
5. Buckley, O., & Nurse, J. R. (2019). The language of biometrics: Analyzing public perceptions. Journal of Information Security and Applications, 47, 112-119.
6. Buzan, B., Waever, O., & de Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.
7. Cambaco, O., Gachuhi, N., Distler, R., Cuinhane, C., Parker, E., Mucavele, E., ... & Sacoor, C. (2021). Acceptability and perceived facilitators and barriers to the usability of biometric registration among infants and children in Manhiça district, Mozambique: A qualitative study. Plos one, 16(12), e0260631.
8. Cambaco, S., Lima, T., & Souza, C. (2021). Public perception of biometric surveillance systems in Africa. Journal of Security and Ethics, 11(1), 77-88.
9. Chen, H., Ma, R., & Zhang, M. (2022). Recent progress in visualization and analysis of fingerprint level 3 features. ChemistryOpen, 11(11), e202200091.
10. Chen, R., Zhang, M., & Wang, L. (2022). The effectiveness of biometric identification systems in fraud prevention and crime detection: A global review. Security and Technology Journal, 35(2), 58-74.
11. Crumpler, W., & Lewis, J. A. (2021). How Does Facial Recognition Work?
12. Gelb, A., & Clark, J. (2019). Challenges of biometric systems in developing nations. Global Governance Studies, 8(2), 145-159.
13. González-González, M., Belharbi, S., Zeeshan, M. O., Sharafi, M., Aslam, M. H., Pedersoli, M., ... & Granger, E. (2025). BAH Dataset for Ambivalence/Hesitancy Recognition in Videos for Behavioural Change. arXiv preprint arXiv:2505.19328.
14. Hossain, M., Saleh, A., & Singh, J. (2024). The adoption of biometric systems in Africa: A case study of security applications. African Security Review, 20(1), 45-56.
15. Huszti-Orbán, J., & Aoláin, F. (2020). Legal challenges in the implementation of biometric systems in Kenya. Journal of International Law and Technology, 12(4), 220-236.
16. Jain, A. K., Ross, A., & Nandakumar, K. (2011). Handbook of biometrics. Springer.
17. Jain, M. (2019). The Aadhaar card: Cybersecurity issues with India's biometric experiment. The Henry M. Jackson School of International Studies, University of Washington.
18. Kabata, R. (2024). The Huduma Namba project: Enhancing security through biometric systems in Kenya. Kenya Security Review Journal, 3(1), 12-22.
19. Kemboi, L. K. (2025). Tracking Maisha Namba-Digital UPI: What is changing, and what are the key issues? Available at SSRN 5175817.
20. Khan, A., & Efthymiou, P. (2021). Evaluating the effectiveness of biometric systems in border security. International Journal of Security Technologies, 18(3), 65-80.
21. Khan, M., & Hanna, A. (2022). The subjects and stages of ai dataset development: A framework for dataset accountability. Ohio St. Tech. LJ, 19, 171.
22. Khan, N., & Efthymiou, M. (2021). The use of biometric technology at airports: The case of customs and border protection (CBP). International Journal of Information Management Data Insights, 1(2), 100049.
23. Kiilu, N. (2022). Indirect discrimination: Huduma Namba (digital identification) and the plight of the nubian community in Kenya. Strathmore L. Rev., 7, 17.
24. Kitsiou, A., Despotidi, C., Kalloniatis, C., & Gritzalis, S. (2022). The role of users' demographic and social attributes for accepting biometric Systems: A Greek case study. Future Internet, 14(11), 328.
25. Liu, D., & Tu, W. (2021). Factors influencing consumers' adoptions of biometric recognition payment devices: combination of initial trust and UTAUT model. International Journal of Mobile Communications, 19(3), 345-363.
26. Lowell, R. (2023). Trust and privacy concerns in the deployment of biometric systems in developing countries. Global Data Protection Review, 7(2), 101-115.
27. Lowell, R. T. (2023). Unchecked Checkpoints: Why TSA's Facial Recognition Plan May Need Congressional Approval. Vand. J. Ent. & Tech. L., 26, 833.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IX September 2025

28. Madhumita, A. (2023). Public acceptance and technical barriers to biometric systems in East Africa. East African Security Journal, 19(2), 23-40.
29. Mills, G., Smith, M., & Wambui, S. (2019). Maisha Namba: Modernizing Kenya's national identification systems. Journal of East African Governance, 6(1), 43-56.
30. Ogunwole, O., Onukwulu, E. C., Joel, M. O., Adaga, E. M., & Ibeh, A. I. (2023). Modernizing legacy systems: A scalable approach to next-generation data architectures and seamless integration. International Journal of Multidisciplinary Research and Growth Evaluation, 4(1), 901-909.
31. Onuigbo, C. (2021). Privacy, security, and surveillance: A review of biometric system adoption in Africa. African Journal of Privacy and Security, 12(1), 28-40.
32. Oyosi, E. O. (2024). Security Measures and Border Security at Namanga One Stop Border Post, Kajiado County, Kenya (Doctoral dissertation, Kenyatta University).
33. Qu, H., Li, J., & Liu, Z. (2019). Biometric technologies in crime detection and fraud prevention: A global perspective. Journal of Crime and Technology, 13(4), 101-112.
34. Rogers, E. M. (2003). Diffusion of innovations (5th ed.). Free Press.
35. Soto-Beltrán, L. L., Robayo-Pinzón, O. J., & Rojas-Berrio, S. P. (2022). Effects of perceived risk on intention to use biometrics in financial products: evidence from a developing country. International Journal of Business Information Systems, 39(2), 170-192.
36. Toesland, F. (2021). African countries embracing biometrics and digital IDs. African Renewal.
37. Tsiftsi, C. (2024). Gesture Recognition Using Artificial Intelligence and Application to an Unmanned Ground Vehicle (UGV) (Master's thesis, Technical University of Crete (Greece)).
38. Waever, O. (1995). Securitization and desecuritization. In R. D. Lipschutz (Ed.), On security (pp. 46-86). Columbia University Press.
39. Wambui, S., Gathara, M., & Kipchumba, N. (2022). Public attitudes toward biometric surveillance in Kenya: Challenges and opportunities. Kenya Security and Technology Journal, 21(1), 9-19.
40. Wienroth, M., & Amelung, N. (2023). Crisis', control and circulation: Biometric surveillance in the policing of the 'crimmigrant other. International Journal of Police Science & Management, 25(3), 297-312.
41. Zhang, W., Zhang, H., & Deng, Z. (2025). Public attitude and media governance of biometric information dissemination in the era of digital intelligence. Scientific reports, 15(1), 2419.