MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 2794-2799

Adaptive Digital Policing: The Influence of Blockchain, Ai, And Iot, In Improving Public Security

Chancy Simbeye, Research Scholar, Sharda School of Business Studies, Sharda University, Greater Noida, Uttar Pradesh, India
Dr. Deepa Kumari, Associate Professor, Sharda School of Business Studies, Sharda University, Greater Noida, Uttar Pradesh, India

Abstract
The research examines how Artificial Intelligence (AI), the Internet of Things (IoT), and blockchain technologies affect adaptive digital policing in Malawi Police Service (MPS) particularly with regards to their impact on crime reduction and public safety measures. These technologies have caused revolutionary changes which affect both public safety modernization and law enforcement practices. A research design that combined both qualitative MPS and National Statistics Office (NSO) of Malawi data statistical records evaluated the consequences of police digital technologies. The digital technology implementation produced positive results for crime prevention operations. These technologies encounter multiple barriers to their general implementation throughout all jurisdictions where issues regarding complete integration serve as barriers along with privacy concerns and data security. The research demonstrates that adaptive digital policing lowers crime while increasing public confidence only when organizations resolve adoption obstacles together with security threats using suitable technological solutions.

Keywords: *adaptive digital policing, internet of things, blockchain, artificial intelligence, and public security.*

Introduction

Recent beliefs have been astounded as a result of a rising data security as well as individual and public safety, resulting in the use of technical triangulations to combat public safety offenses (Reza, 2023). Traditional methods of data security have been in use for a long time to aid in safeguarding public safety and improved police reforms; however, in this era of advanced computer technologies, the introduction of Artificial Intelligence (AI), Internet of Things (IoT), and blockchain has led to crime prevention organizations develop and implement modern digital models to prevent crime and public safety. The dearth of adaptive digital policing and public safety is one of the most pressing concerns in criminal investigation, making it hard for all police stations to apply adaptive policing for the various offenses. The Malawi Police Service has implemented numerous digital technologies for criminal databank supervision, including web-based application tabulated in Android database server, fingerprint credential system database server and ICT (Nation, 2018; UNDP Malawi 2025). The smartphone application emerges as a solution to how people report crimes, allowing them to report any crime that occurs in their community. Notwithstanding the advancement of how these systems store the data, Artificial Intelligence (AI), Internet of Things (IoT), and blockchain technologies have yet to be fully implemented throughout all Malawian jurisdictions. In this context, the research seeks to assess 'the role of Artificial Intelligence (AI), the Internet of Things (IoT), and blockchain' technology in improving adaptive digital policing at all police stations in order to reduce crime and increase public safety.

Literature Evaluation.

AI, IoT, and blockchain play important roles in changing police reforms and boosting public security.

Digital policing denotes the use of modern digital technologies such as 'artificial intelligence (AI), the Internet of Things (IoT), and blockchain' to create more efficient and transparent policing processes. This signifies a major shift away from traditional policing approaches and toward more technologically advanced forms that use data to make real-time modifications in response to changing events. Policing does not operate in a vacuum, and it cannot remain static in the increasingly digital environment in which police organizations must work and live. The problems and possibilities that digital disruption presents in police are quickly becoming defining concerns for the service. While it may appear that the rate of technological development is currently too rapid, it will only accelerate more. The MPS has made progress in recent years, notably in terms of mobile technology and migration to cloud services, but more has to be done to satisfy rising digital demand. In the twenty-first century, a significant portion of police efficiency and efficacy is based on the professional use of technology for forensic analysis, fixed speed cameras on roadways, and closed circuit video in crime-prone areas, among other things. Similarly, the purchase and usage of sophisticated crowd control technology has the potential to minimize mortality during public disturbances (MPS). In adaptive digital policing, artificial intelligence analyzes massive volumes of data to predict crimes, plan resource allocation, and improve decision making. For example, AI-based predictive analytics can help police agencies prevent crime by detecting high-risk regions (Lum et al., 2017; Alikhademi et al., 2022). Body cameras, different sensors, and drones are examples of IoT devices that improve situational awareness and enable rapid reaction to situations by collecting pertinent data in real time. These gadgets are extremely useful in giving important situational information during crises and normal patrols (Fraga-Lamas et al, 2016; Kabir & Alam, 2023).

According to Yaga et al. (2019), blockchain technology establishes a new standard in digital record management by enabling unparalleled levels of transparency and security. It does this by producing unchangeable logs of evidentiary information, such as chain-of-custody and transaction records, resulting in a reduction in public trust and accountability degradation, as well as corruption within police procedures (Michael et al, 2018; Sihag et al., 2023; Atlam et al., 2024). The success of these technology integrations also aids in the elimination of operational inefficiencies while addressing long-standing concerns of governance and agency accountability within law enforcement.

The importance of fast adaptable digital policing is becoming increasingly apparent as the rest of the world's technology progress accelerates. Many nations in North America, Europe, and Asia are currently investing in the digital transformation of their police forces in the hopes of improving public safety. Meanwhile, emerging economies such as Malawi are beginning to look to similar technologies as a method to improve resource-constrained service delivery. For this analysis, comparative research will be performed to examine international trends of police reforms as well as the obstacles and opportunities in Malawi.Critics argue that existing law enforcement models are antiquated and rely on reactive, top-down techniques rather than proactive, evidence-based decision making. The algorithms rely on historical data, resulting in a temporal lag in responding to rapidly shifting criminal actions. The lack of openness in law enforcement activities has led to a significant decrease in public trust and confidence (Lum et al., 2017; Alikhademi et al., 2022). These constraints present substantial barriers to tackling modern security concerns, necessitating innovative ways to change police operations.

Modern policing challenges, traditional policing limitations.

The traditional policing model (TPM) has been criticized for its inefficient characteristics that focus mainly on chain of command, which is a top-down approach where command-and-control structures affect those operating on the ground like the patrol team or those that are on a laid-for duty at night can't perfume their roles unless they receive the order from the directives to take action, as a result this endangers According to Lum, et al (2017) study, prone regions that require immediate attention impede operational innovation due to hierarchical order, which also contributes to increasing operational inefficiency. Its strategies fail to complete tasks on time. For example, the TPM emphasizes a top-down approach, also known as a command-control approach of directives, which leads to decreased and delayed information sharing and decision-making operations at the lower levels, contributing to high crime rates in urban areas and lower police work quality (Alikhademi et al, 2022). Reactive policing fails to address the issues at hand, making it more difficult to maneuver effectively as crime systems become more sophisticated and multinational.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 2794-2799

Today, law enforcement agencies are adopting data-driven strategies by leveraging predictive policing analytics that focus on anticipating crime-prone areas, allocating resources, and moving toward evidence-based policing. Despite the limitations and challenges of modern police, the organization is doing everything possible to transition to evidence-based policing. Modern policing continues to employ data-driven strategies, utilizing predictive analytics to allocate resources and forecast crime-prone locations more effectively. The implementation of modern technology such as artificial intelligence (AI) enables police agencies to more accurately analyze large datasets, foresee illicit conduct, and categorize movements (Fraga-Lamas et al., 2016; Lum et al., 2017; Kabir & Alam, 2023). To lessen crime and intensify community protection, data-driven decision-making police is viewed as a viable solution to the drawbacks of volatile policing. Public Trust and Transparency Meeting the needs of the community has been difficult due to a heavy reliance on the command and control approach and the nature of the model, which has hampered operational activities and resulted in poor coordination and accountability to the community they serve.

Michael et al. (2018) reported that instances of extreme lack of openness and disproportionate use of force had undermined public confidence, limiting effective community policing. Because of the implementation of civilian oversight boards and the use of technologies such as IoT, AI, and blockchain, society now wants more police visibility in terms of accountability and transparency in how public knowledge of the police affects their day-to-day operations. What is the current state of police reform? To address international challenges, there has been a significant shift toward the integration of technology in policing practices. As a result of the introduction of modern policing, police reforms have been working to adopt these practices by combining both modern technology and traditional discipline values. According to a study conducted by Fraga-Lamas et al. (2016), there have been improvements in work efficacy as a result of the implementation of modern technology, where data sharing and real-time crime monitoring have led to efficient achievement of both transparency and accountability. For example, jurisdictions in Europe and North America have adopted digital platforms to combat crime. Developing countries are also attempting to incorporate technology in the form of IoT, AI, and blockchain. While their efforts are sometimes limited by resource restrictions and infrastructure issues, countries such as Malawi are beginning to investigate these advances. Law enforcement agencies throughout the world have become more responsive and responsible to how modern policing is being implemented, indicating a concentrated effort (Walker and Archbold, 2018).

Mistakes in Predictive Policing

Despite the numerous hurdles that law enforcement organizations face, predictive policing has demonstrated that community safety has improved. The flaws discovered in algorithms, as well as the ethical implications of AI-driven prediction models, have raised significant concerns about crime forecasting using historical data. Existing preconceptions and discriminatory behaviors might lead to criticism if the underlying data is distorted (Lum et al, 2017; Michael et al, 2018). Furthermore, accountability measures and extensive community participation may be misdirected, increasing dependence on predictive analytics and generating a false feeling of security. The balance between ethical misunderstanding and technical advancement remains a significant challenge in the use of predictive police tactics.

3. Methods and Materials

About the Malawi Police Service

Because of its centralized structure and recent changes, the Malawi Police Service acts as a single and autonomous body of police overseeing all six regions. As a single entity, the Inspector General of Police leads the line of command, followed by the Deputy Inspector General (DIG) Human Resources and Operations. The Malawi Police Service is utilized throughout Malawi to prevent, detect, and investigate crime, apprehend and prosecute offenders, maintain law and order, protect life and property, safeguard fundamental freedoms, and rights of individuals, the enforcement of all laws assigned to the police, and the execution of powers, functions, and duties conferred upon the police by the Constitution of the Republic of Malawi.

Figure depicting Region Police Headquarters and Police Stations.

The Officers In-Charge supervise a total of 48 police stations, which are staffed by designated station Officers. Under each policing region, the following is a comprehensive overview of police stations.

Central West Region Police Headquarters	Central East Region Police Headquarters	South West Region Police Headquarters	South East Region Police Headquarters	Northern Region Police Headquarters	Eastern Region Police Headquarters
1. Lilongwe Police Station	1. Kasungu Police Station	1. Blantyre Police Station	1. Mulanje Police Station	1. Mzuzu Police Station.	1. Machinga Police Station
2. Kanengo Police Station	2. Mponela Police Station2	2. Limbe Police Station	2. Thyolo Police Station.	2. Karonga Police Station	2. Zomba Police Station
3. Lingadzi Police Station	3. Dowa Police Station	3. Soche Police Station	3. Luchenza Police Station	3. Nkhatabay Police Station	3. Balaka Police Station
4. Kawale Police Station	4. Nkhunga Police Station	4. Bangwe Police Station	4. Chikwawa Police Station	4. Rumphi Police Station	4. Mangochi Police Station
5. Lumbadzi Police Station	5. Nkhotakota Police Station	5. Chaleka Police Station	5. Nsanje Police Station	5. Jenda Police Station	5. Makanjira Police Station
6. Kasiya Police Station	6. Salima Police Station	6. Chilomoni Police Station	6. Phalombe Police Station	6. Likoma Police Station	6. Monkeybay Police Station
7. Mchinji Police Station	7. Ntchisi Police Station	7. Mwanza Police Station	7. Chiradzuru Police Station	7. Chitipa Police Station	7. Liwonde Police Station
8. Dedza Police Station		8. Neno Police Station		8. Mzimba Police Station	
9. Ntcheu Police Station		9. Ndirande Police Station		9. Kafukule Police Station	

Figure 1. MPS Regional Headquarters.
Source: MPS, 2024.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 2794-2799

Methods Employed

A Secondary data analysis using reports from Malawi Police Service and National Statistics Office of Malawi was employed to identify AI, IoT and Blockchain use by the public whereby tabulation of figures and charts was generated using MS Excel 2016. On the other hand, a qualitative content analysis and cross referencing sources in the application of AI, IoT and Blockchain to facilitate the data safety and public confidence. The outcomes of the use of technological triangulation by the people may be utilized by law enforcement authorities to formulate and execute the information from the public so that targeted crime prevention initiatives may be utilized. Analyzing and employing technological triangulation tools yields a more complete and dynamic understanding of data safety and crime prevention. This information can also facilitate resource allocation, enhance decision-making, and bolster proactive crime prevention measures. This methodology has been extensively employed in assessing the information between police stations and the civilians (Tobias, & Mwanza, 2024: Ekpo, et al., 2025). This study employed NSO data and that of MPS for data analysis utilizing a methodology. Initially, high-risk crime regions were selected using the results obtained from the figures (www.police.gov.mw/; www.nsomalawi.mw).

Theoretical Review

Adaptive digital policing was used to determine public safety and if police personnel can employ new technology in accordance with the changing environment. The use of adaptive digital policing in police operations will reduce police burden, reduce crime, and boost public trust. To be more specific, the outcomes of adaptive digital policing in police operations can help law enforcement organizations create and effect targeted crime prevention initiatives. As a result of evaluating digital data crime as a system and employing a number of technical tools, inclusive and active perspective of crime hotspots areas and trends may be expanded (Tobias, & Mwanza, 2024). Adaptive digital policing is used to help in allocating resources according to the trends, enlighten decision-making, and assist in curbing crime prevention efforts, so increasing public safety and confidence. This technique has been widely utilized in law enforcement throughout the world to designate the biggest crime hotspot locations and determine the distance that exists between police stations (Kuta et al., 2014; Ganesh et al. 2022). In this project, data was analyzed using Ai, IoT, and Blochchain. First, the investigation examined documents to see if MPS can adapt to new digital technologies in its functions. The use of manual techniques to manage personnel data creates consistency and maintenance issues. Digitalizing the Human Resource Management (HRM) database using specific software or platforms can improve data accuracy, speed procedures, and give a more effective method to evaluate and manage personnel information (www.police.gov.mw/; www.nsomalawi.mw).

Theories of AI, IoT, and Blockchain in Adaptive Digital Policing

As the globe evolves toward contemporary technology, law enforcement agencies are not left behind; they are also aiming for a societally changing atmosphere in the workplace. Technological determinism (TD) holds that technology has a substantial influence on human life. Feenberg (1991) and Paul (2006). addresses TD, with research revealing that the concept of TD is ubiquitous in popular imagination and political debate, as evidenced by the view that the Internet is changing and revolutionizing the public and economy. Criticizers of TD claim that technology is publicly determined and social structures evolve in a developing process, a non-deterministic, and that the effects of its emergent are mostly determined by how it is implemented, which is also socially driven. Policymakers and law enforcement organizations argue that relying too much on technology in illegal activities might increase risks, suggesting a lack of comprehension of technology's philosophy (Manning, 2008; Raharjo et al. 2018). This position is congruent with substantive theory in technology, which regards technology as the basis of a new type of cultural system that reorganizes the entire cosmos as a source of control. Feenberg (1991) says that when we choose to use technology, we make immoral cultural choices, which puts pressure on law enforcement authorities to function in conformity with societal trends. Technology has become more than just relevant; it has also become a source of uncertainty and a way of life, with important implications for adaptive digital policymaking and citizen safety. Technologies coevolve in unexpected and emergent patterns. With the advent of modern technology in present capitalism, the TD issue is continuously resurfacing. The supporters of this theory acknowledge that capitalism is another eye opener of the social structure that accelerates the rate at which technological transformation evolve, however, in order to maintain technology's fundamental role, need to reject the "strong social constructionist" theory, which would enlighten the complete technology's development path in terms of social structures (Paul 2006).

This demonstrates that the adoption of technology is not automatically unbiased in the knowledge development process. The data is organized in an exceptional technique for them since the society is designed distinctively by the mediums of language and technology; they influence the user's psyche and encourage communal transformation. Advocates of technological determinism contend that technological advancement impacts and determines society. The undesirable significances of technological growth are caused by people's inappropriate use of technology, not the technology itself. Toffler (2006) regarded technology as the driving force behind all advances that had a negative impact on every element of social life. He contends that emerging societies have a substantial impact on the human psyche and examines the time in which everything is always changing and criminal acts and law enforcement agencies need to adapt the changing environment.

The difficulties presented by AI, IoT, and Blockchain will amaze the twenty-first century. The features of the digitization technique, such as globalization, decentralization, harmonization, and strengthening, are too powerful to halt in law enforcement institutions. The introduction and adoption of new technologies are the result of social order. Technology and social factors do not exist in distinct worlds or processes. technical change mimics society, whereas society produces technical change. Thus, society is defined by both the technologies that it can create and those that it prefers to use and develop over others. According to this perspective, technology is one of multiple social processes (Feenberg, 1991; Toffler, 2006; and Paul. 2006).

The incorporation of AI, IoT, and Blockchain into MPS has expanded, therefore Digital Confidence Theory highlights the role of technology in affecting public confidence in law enforcement by emphasizing transparency, security, and reliability. In law enforcement, AI promotes justice by reducing human decision-making biases, whereas IoT improves accountability through real-time evidence collection and monitoring. Blockchain boosts trust by ensuring that police records are tamper-proof, lowering the risk of corruption and data manipulation. However, the effectiveness of digital trust in MPS police is heavily reliant on ethical execution and stringent regulatory oversight, which may vary by region. Without specific limits, concerns about monitoring, data exploitation, and algorithmic bias may undermine the trust that these technologies strive to build.

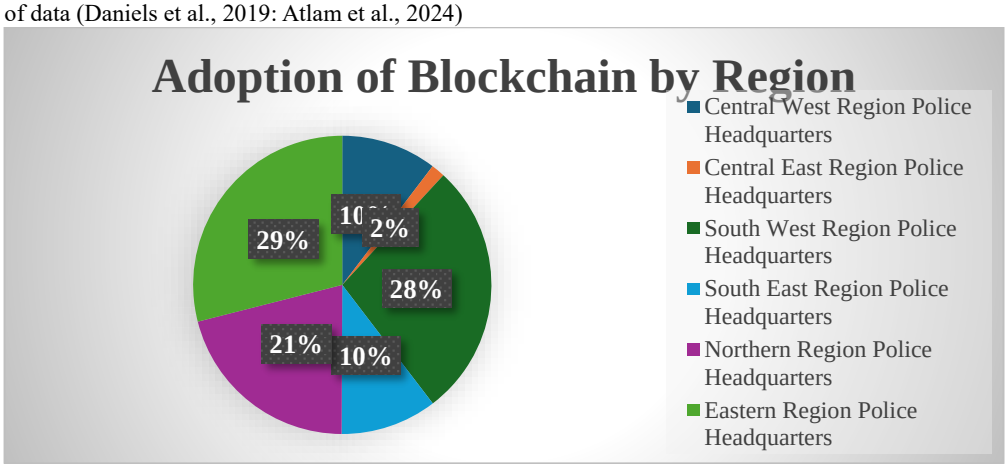
Results

The findings of the study are centered on a systematic update of adaptive digital policing to the Malawi Police across the all six regional police headquarters, involving 48 police stations and concentrating on the implementation of AI, IoT, and Blochchain in MPS, utilizing technological advancement to identify crime hotspots in Malawi and public safety. The study concluded that existing ‘intelligence and criminal record-keeping’ approaches in Malawian state are unable to solve current crime concerns and data security. Manual techniques do not consistently offer accurate, reliable, or comprehensive data, nor do they allow for trend analysis or informed decision-making. It also reduces productivity and causes inefficient worker usage.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 2794-2799

Access and Use of Blockchain by Region

A blockchain is a decentralized database or ledger disseminated among the nodes of a computer network. They are most recognized for their essential function in bitcoin systems, ensuring a secure and decentralized ledger of transactions; nevertheless, their applications extend beyond cryptocurrencies. Blockchains may render data in any sector immutable, signifying that it cannot be modified. This study presents an innovative blockchain-based smart policing system that enhances accountability, openness, and confidence in the storage and protection of data (Daniels et al., 2019: Atlam et al., 2024)



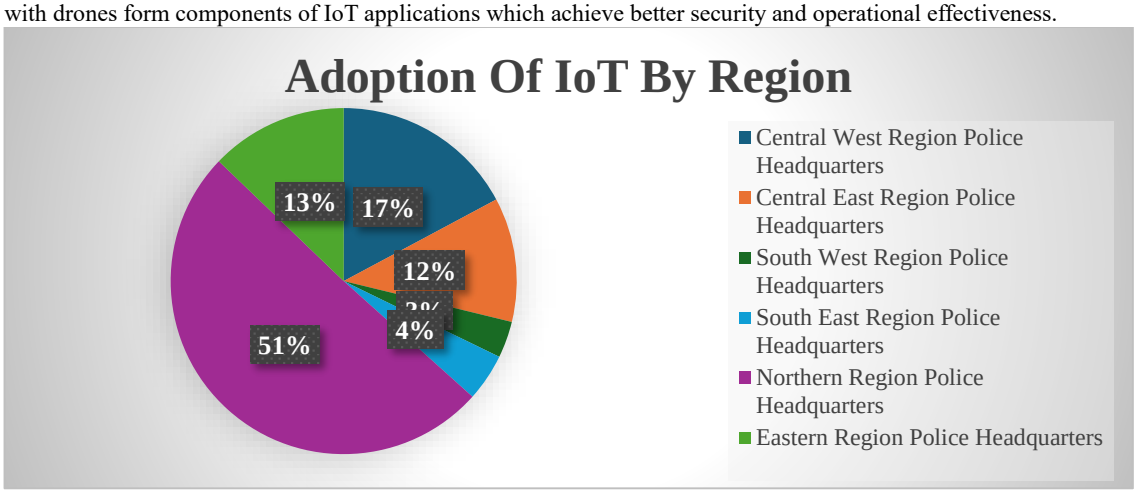
(Figure 2). Source: Author).

The specific proportions of blockchain technology usage by police headquarters in Malawi are shown through this chart. The distribution of blockchain implementation spans six geographical areas called Central West, Central East, South West, South East, Northern, and Eastern. The Eastern Region Police Headquarters has implemented blockchain technology at the highest level of 29%. One-third of the blockchain technology implementation at Malawi Police Service takes place in this region. The South West Region Police Headquarters currently utilizes blockchain technology at a 28% level. These percentages demonstrate that blockchain implementation in this Region to be significant integrated. The Northern Region Police Headquarters accounts for 21%. Indicating a notable operation within the examined areas. The Central West Region Police Headquarters shows 10% adoption among its personnel. This percentage stands substantially lower than those of the top three regions. The adoption rate at the South East Region Police Headquarters matches the Central West region at 10%. According to the figures the Central East Region Police Headquarters shows the lowest implementation levels at 2%. This shows that there is a minimum implementation of blockchain technology adoption conducted by this region.

The depicted graphic demonstrates significant differences in how the policing areas of Malawi utilize blockchain technology. Blockchain adoption levels surpass other regions within the Eastern and South West areas while the Central East lags behind. Analysis shows blockchain adoption in the Northern area surpasses other areas but Central West and South East show less implementation rates.

Access and Use of IoT by Region

IoT in adaptive digital policing defines the procedure of integrating networked strategies and devices along with software to enhance law enforcement competences. These devices which conduct data collection and exchange operations enable smart monitoring systems that perform instant decision-making through real-time analysis. Law enforcement wearable devices and intelligent surveillance systems along with drones form components of IoT applications which achieve better security and operational effectiveness.

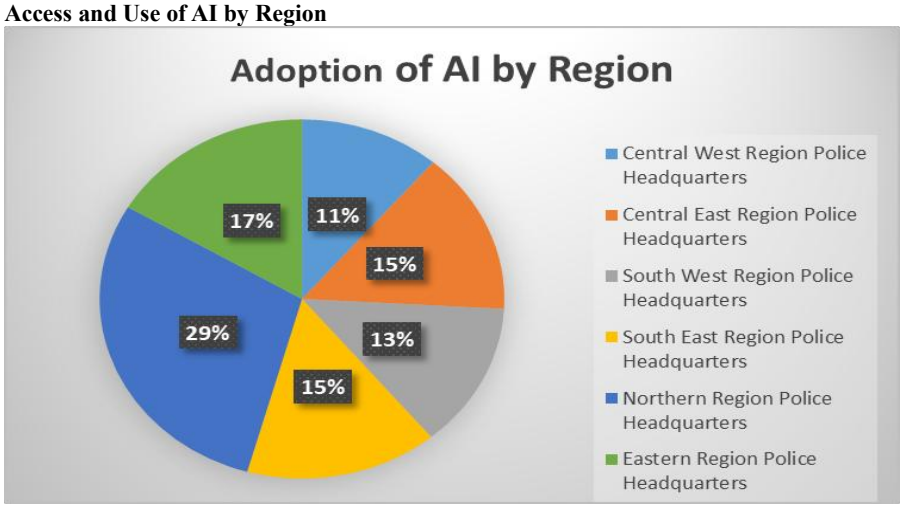


(Figure 2). Source: Author).

The chart shows Internet of Things technology deployment across different police headquarters within Malawi at the country level. The visual presentation shows how Internet of Things (IoT) deployment fragments among the different areas in police headquarters. Internet of Things technology is most prominently used at the Central West Region Police Headquarters where 51% of their system has been implemented. The Central East Region Police Headquarters uses an Internet of Things system amounting to 17% of total implementation. South West Region Police Headquarters recorded an adoption rate of 13%. The South East Region Police Headquarters attains an adoption rate of 12%. The Northern Region Police Headquarters recorded 4%. The Eastern Region Police Headquarters maintain the least adoption rate compared to other locations at 3%. The figure shows that the Central West Region Police Headquarters leads in Internet of Things utilization. The Eastern and Northern police stations remain the lowest level of Internet of Things implementation among these headquarters.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 2794-2799

Access and Use of AI by Region



(Figure 4). Source: Author).

Adoption of AI by Region demonstrates the percentage of AI adoption among people working across different police headquarters areas. A portion of the pie chart represents separate police regions while its size reflects how many authorities from each region adopted artificial intelligence in comparison to other regions.

The Northern Region Police Headquarters demonstrates the highest adoption of technological advancement with 29%. Eastern Region Police Headquarters recorded 17%. The Central East Region Police Headquarters and South East Region Police Headquarters had equal percentage which equates to 15%. The South West Region Police Headquarters recorded13%of the adoption rate of AI. The Central West Region Police headquarters recorded the lowest

The Northern Region Police Headquarters leads all included areas in artificial intelligence adoption levels while the Central West Region Police Headquarters demonstrates the lowest levels of acceptance. The areas fall between full integration of artificial intelligence systems at low and high levels.According to the study's findings of Adaptive Digital adoption by region, the Eastern region police Headquarters reported a high significance in the use of Blockchain and AI, according to figure 2, and 3 which recorded 29% both AI and Blochchain, the Northern region police Headquarters recorded 51% representing the highest level of technological adoption of IoT. In the United States, law enforcement agencies have used AI-powered systems that analyze past data to anticipate and prevent crimes. Law enforcement organizations throughout the world are using current technology, which is producing results. According to Alikhademi et al. (2022), using forecasted digital instruments has been linked to lower crime rates. In the United Kingdom, police agencies have increased transparency and accountability by implementing digital technology like as sensors and body cameras (Lum et al, 2017). The application of AI and IOT in Scandinavian police operations has increased community trust and data management by shortening reaction times and allocating resources (Fraga-Lamas et al, 2016; Kabir & Alam, 2023). According to the chart above, the deployment and usage of AI, IoT, and Blockchain in Malawi is unclear, indicating that the majority of people communicate using mobile phones.

On the other hand, according to the NSO (2019) survey, the Northern Region has the highest proportion of people who have access to Information Communication Technology (ICT), followed by the Central Region and the Southern Region, where the proportion is significantly higher, indicating that people in the North are adapting digitally through the use of modern technology. According to the report, Northerners have greater information and are less likely to commit crimes, but they are more vulnerable to cybercrime through phone calls or internet surfing. People in the north can report cybercrime incidents to safeguard individual data privacy, as opposed to those in the middle and southern parts of Malawi. When questioned, some individuals said they didn't know anything, while others didn't know where to report their crimes. When utilizing a mobile phone or surfing the internet, just a few persons (3.6 percent) NSO (2029) p102 were able to report criminal incidents to the police. This explanation demonstrates that community knowledge is relatively low, highlighting the need to reform and boost community interaction with the police in order to minimize crime and individual data privacy.

The Benefits of Involving the Community

A study conducted by Tobias, & Mwanza, (2024). Says that community engagement is critical for the successful adoption of digital policing. To foster public trust, police departments must give opportunities for citizen monitoring and input. The introduction of new technology may be tailored to the community's expectations and values by organizing community advisory groups and having regular public meetings. Maintaining public trust and decreasing privacy and surveillance concerns necessitates transparent and honest reporting of data collection and utilization, as well as easily accessible methods for criticism (Fraga-Lamas et al., 2016; Kabir & Alam, 2023). Establishing methods for transparency and public oversight is critical for resolving the moral and legal concerns highlighted by digital policing. This can be performed in the following ways. Public Engagement Initiatives that provide opportunities for public input and involve the community in decision-making procedures may assist to reduce the trust gap and ensure that technology implementations are consistent with cultural norms and values.

Building Capacity and Training

Continuous training and capacity building are essential for the success of adaptive digital policing. To properly use contemporary technology, police officers and support workers must have technical abilities as well as digital literacy Tobias, & Mwanza, (2024). Employees should get regular training sessions to learn about ethical norms and legal ramifications, as well as new advances in blockchain, IoT, and AI. Investing in these human resources ensures that the deployment of technology yields actual improvements in public safety and operational performance (Alikhademi et al., 2022).

Interoperability and Data Security

Strong data security and interoperability are critical as law enforcement agencies become more reliant on networked digital technology. Regular security evaluations and the implementation of standardized cybersecurity policies will help to avoid data breaches and unauthorized access. Furthermore, creating a unified, efficient framework for digital policing necessitates the construction of interoperable systems that allow for seamless communication between various technologies (for example, IoT devices and central databases). In addition to protecting private information, these measures promote collaboration and trust among organizations and interested parties (Sihag et al., 2023; Atlam et al., 2024).

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 2794-2799

In conclusion.

Technology has infiltrated both our physical and spiritual lives. Technology is a natural reflection of the human spirit; it is the manifestation of ideas within the human brain. Humans are growing more scattered, while machines are becoming more dominant in human existence, posing issues in a variety of areas, including the creation of unlawful acts under multiple statutes. To solve this issue, normative research methods are used, with a focus on comparative legislation. Laws with an expanding scientific and technical character combine legal components with scientific and technological operations. Lawmakers draft rules that both reflect and reject technological determinism. This appears to be the case when comparing fundamental criminal law legislation based on the Criminal Code to additional laws and regulations that include technological aspects. Technology-based criminal consequences are uncommon under regular criminal law and only emerge when technology is used to do illegal acts such as decency, humiliation, defamation, and crime dimension technology. This argument must be understood, given the politicians' failure to explain.

Furthermore, expanding blockchain forensics will be crucial in tracing unlawful cryptocurrency transactions, while rigorous synthetic biology regulations will help to prevent the use of genetic engineering in criminal activities. To address the risks posed by AI and autonomous systems, global collaboration is essential to develop international legislation governing AI and robotics in law enforcement. The future of the police depends not just on responding to crime, but also on staying ahead via innovation, regulation, and strategic adaptability.

References

1. Alikhademi, E. Drobina, D. Prioleau, B. Richardson, D. Purves, and J.E. Gilbert. (2022). A fairness-focused study of predictive policing. *Artificial Intelligence and Law*, 1–17.
2. Atlam, H. F., Ekuri, N., Azad, M. A., & Lallie, H. S. (2024). Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions. *Electronics*, *13*(17), 3568.
3. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805.
4. Brayne, S. (2021). Predict and Surveil: Data, discretion, and the Future of Policing. Oxford University Press.
5. Chirwa, D.M. (2022). Constitutions Without Constitutionalism, Governments Without Governance: A Critique and Hope for Malawi. *Journal of Southern African Studies*, *48*(6): 1119-1128. https://doi.org/10.1080/03057070.2022.2151774
6. Coulthart, S. & Riccucci, R. (2022). Putting big data to use in government: the case of the US Border Patrol. Public Administration Review, 82(2), pp. 280–289.
7. Daniels, J., Sargolzaei, S.; Sargolzaei, A.; Ahram, T.; Laplante, P. A.; and Amaba, B. (2019). Internet of Things, AI, Blockchain, and Professionalism. *IT Professional, 20*(6), 15–19. DOI: 10.1109/MITP.2018.2875770
8. Dixon, A., & Birks, D. (2021, August). Improving policing with natural language processing. In *Proceedings of the 1st Workshop on NLP for Positive Impact* (pp. 115-124). Association for Computational Linguistics.
9. Ekpo, E., Gbiri, I. A., Daukere, B. E., & Ademola, A. J. (2025). Geospatial assessment of police installation locations in Oyo town, Oyo state, Nigeria.
10. European Commission. (2020). General Data Protection Regulation (GDPR). Retrieved from ec. europa.eu. Retrieved on March 6, 2025 from https://commission.europa.eu/law/law-topic/data-protection_en.
11. Fraga-Lamas, P., Fernández-Caramés, T.M., Suárez-Albela, M., and Castedo, L. & M. González-López (2016). *An evaluation of the Internet of Things for defense and public safety. Sensors, 16*(10), p. 1644.
12. Feenberg, A. (1991). Critical Theory of Technology (Vol. 5). *New York: Oxford University Press*.
13. Manning, P.K. (2008). Vol. 4 covers police technology, including crime mapping, information technology, and rational crime control. NYU Press.
14. Ganesh, N. G., Venkatesh, N. M., and Prasad, D. V. V. (2022). A thorough literature review on forensics in the cloud, IoT, AI, and blockchain. *Illumination of Artificial Intelligence in Cybersecurity and Forensics,* 197–229.
15. ITU World Bank (2024). Challenges and regulatory norms for transformative technologies (AI). The World Bank retrieved on December 3, 2025 https://digitalregulation.org/3004297-2/
16. Kabir, M. S., and Alam, M. N. (2023). A study of IoT, big data, and artificial intelligence applications in law enforcement and the judicial system. *International Research Journal of Engineering and Technology (IRJET), 10(*5), 1777–1789.
17. Lum, C., Koper, C.S., and Willis, J. (2017). Understanding the limitations of technology's influence on police efficacy. *Police Quarterly, 20*(2), 135–163.
18. Malawi Police Service Annual Report (2023), https://www.police.gov.mw/services/police-reports.
19. https://bti-project.org/en/downloads?content=country&country=MWI
20. J. Michael, Cohn, A.L.A.N., and J.R. Butcher (2018). Blockchain technology. *The Journal, 1(7),* pp.1–11.
21. Mondschein, C.F., and Monda, C. (2019). In the context of research, the EU's General Data Protection Regulation (GDPR) is relevant. *Fundamentals of Clinical Data Science,* 1, 55–71.
22. Narayanan A., Bonneau J., Felten E., Miller A., and Goldfeder S. (2016). Bitcoin and cryptocurrency technologies: a detailed overview. *Princeton University Press*.
23. Malawi's National Statistics Office (2019). National Survey on Access and Use of Information and Communications Technologies. National Survey on Access and Use of Information and Communications Technologies by Households and Individuals in Malawi, 2019.
24. Paul S.A. (2006). Technological Determinism. A draft entry for The International Encyclopedia of Organization Studies, edited by Stewart Clegg and James R. Bailey *(Sage).*
25. Raharjo A., Saefudin Y., and Fidiyani R. (2018). The role of technological determinism in the formation of criminal legislation. *In the E3S Web of Conferences* (Vol. 73, p. 2011). EDP Sciences.
26. Tobias, C.J.B. & Mwanza, B. (2024). Spatial and Temporal Analysis: A GIS-based tool for crime monitoring and clustering in Malawi. *ESI Preprints*, 20(8), pages 167-167. DOI: 10.35879/jik.v17i3.413
27. Russell, S. J. and Norvig, P. (2016). Artificial intelligence: A Modern Approach. *Pearson.*
28. Sihag, V., G. Choudhary, P. Choudhary, and N. Dragoni. (2023). *Cyber4drone is a rigorous assessment of cyber security and forensics in next-generation drones. Drones, 7*(7): 430.
29. The Transformational Index (2024). Retrieved March 21, 2025. https://bti-project.org/en/
30. Tobias, C.J.B. & Mwanza, B. (2024). Spatial and Temporal Analysis: A GIS-based tool for crime monitoring and clustering in Malawi. *ESI Preprints*, 20(8), pages 167-167.
31. Toffler, A. (2006). Revolutionary riches. *New Perspectives Quarterly, 23*(3), pp. 7–15.
32. UNODC. (2021). *The Global Study of Homicide*. UN Office on Drugs and Crime.
33. Walker, S. E. & Archbold, C. A. (2018). The new reality of police accountability. *Sage publications.* P, 274
34. Yaga, D.; Mell, P.; Roby, N. & Scarfone, K. (2019). Blockchain technology overview. *Preprint* arXiv:1906.11078.