C O A S

Center for Open Access in Science

Open Journal for
Information Technology

2024 ● Volume 7 ● Number 1

https://doi.org/10.32591/coas.ojit.0701

ISSN (Online) 2620-0627

OPEN JOURNAL FOR INFORMATION TECHNOLOGY (OJIT)
ISSN (Online) 2620-0627
www.centerprode.com/ojit.html * ojit@centerprode.com

Publisher:

Center for Open Access in Science (COAS), Belgrade, SERBIA
www.centerprode.com * office@centerprode.com

Open Journal for Information Technology, 2024, *7*(1), 1-54.
ISSN (Online) 2620-0627

CONTENTS

Center for Open Access in Science ▪ https://www.centerprode.com/ojit.html
Open Journal for Information Technology, 2024, *7*(1), 1-10.
ISSN (Online) 2620-0627 ▪ https://doi.org/10.32591/coas.ojit.0701.01001k

Decision Making on Introducing of Blockchain Technology in Croatian Public Administration

Alen Kišić

VERN' University, Zagreb, CROATIA

Neven Vrček

University of Zagreb, Varaždin, CROATIA
Faculty of Organization and Informatics

Received: 20 March 2024 ▪ Revised: 28 April 2024 ▪ Accepted: 10 May 2024

Abstract

Blockchain technology has many features enabling great potential to transform every aspect of life. In this paper, we consider application of Blockchain in public administration sector. We utilize the Value Measuring Methodology (VMM) for the purpose of the profitability assessment of introducing Blockchain into the public administration. This process is conducted by multi criteria decision making with a group of experts. Results of cost-effectiveness analysis and AHP analysis, which are part of VNM, indicated direct user value as the largest benefit, followed by operational value for the State. Potential risks are identified along with the costs summarizing an analysis.

Keywords: Blockchain technology, public administration, value measuring methodology, effective public administration.

1. Introduction

"The most efficient way to produce anything is to bring together under one management as many as possible of the activities needed to turn out the product" (Drucker, 2003). Peter Drucker's quote describes exactly the idea behind the implementation of Blockchain technology in the Public Administration sector. Why? Public Administration is a complex system. It is centralized in terms of the responsibility for managing and providing of public services, yet fragmented in terms of the organizational structure and the ability to share information. Blockchain technology has the potential to simplify the confidential information management, to provide an easier access to information to government agencies, as well as to protect the security of such information. Government agencies have much to gain by experimenting with such technology and developing it through pilot projects. Blockchain can help agencies turn paper records into electronic ones and manage them through a safe infrastructure, as well as enable them to turn some of such records into the "smart" ones. IT departments within government agencies should create rules and algorithms that will allow for an automatic information sharing in Blockchain with third parties once the specific prerequisites are met. In the long run, this technology could enable individuals and organizations to take direct control over the information the Government keeps on them. Blockchain is a distributed ledger (Vacca et al., 2020). This means

Correspondence: Alen Kišić, VERN' University, Zagreb, CROATIA.

that data is not stored in a central database as in traditional data system architecture, but is maintained over a distributed network. Blockchain confirms new transactions based on a set of pre-defined rules. Blockchain stores a transparent and immutable record of all the transactions made. Some Blockchain features make this technology an attractive solution to specific issues the public service agencies are facing. Those features are given in an addition. First one is increased efficiency. Blockchain provides both the process and organization efficiency. Transactions for processing (be it a financial or information-related transactions are less error-prone and are simpler. For the public sector, Blockchain represents a specific opportunity to provide conventional services (Alketbi, Nasir & Talib, 2018), which were previously in paper format only, in the electronic form (Estonia, for instance, provided health care records in Blockchain). Second, data integration. The chain immutability through Blockchain protects it from being changed or removed. It provides a transparent structure and a visible transaction trace, which prevents unauthorized record tracing and provides a more secure network. Third one is reduced risk. It provides an opportunity to reduce and eliminate corruption. For instance, in the area of social assistance distribution, tax process management and land registry management. Some of the most advanced applications of Blockchain in the public sector are e-services in Estonia (Sullivan & Burger, 2017) and the Dubai initiative (Bishr, 2019) aimed at providing all the public services to its citizens through Blockchain.

This research paper provides the analysis of the existing examples of the implementation of Blockchain technology in the Public Administration of different countries all over the world, based on what it presents a proposal of the implementation of Blockchain to the Croatian Public Administration. The central part of the paper describes and implements the Value Measuring Methodology (VMM) for the purpose of the profitability assessment of introducing Blockchain into the Public Administration. Expert judgements play an important role in decision making, especially in expensive and innovative IT projects implementations. Building predictions and performing expert examinations in are among the tasks requiring experts' involvement in decision-making processes. We have taken expert knowledge into account to conduct expertise and obtain valuable insight into perception of Blockchain implementation potential in public sector.

The paper is organized as follows. In the second chapter, the Value Measuring Methodology implementation is described step-by-step. The third chapter provides ideas for the introduction of the Blockchain technology into the Croatian Public Administration with fourth chapter, assessing their cost-effectiveness. The conclusion provides the VMM framework for the cost-effectiveness assessment and the value assessment results carried by applying the AHP method.

2. Methodology

The Value Measuring Methodology (VMM) defines four steps which need to be performed for the purpose of the assessment of cost-effectiveness. The four methodology steps are the following (Mataracioglu, 2015):

(1) Developing a Decision Framework;

(2) Defining the Alternatives;

(3) Analysing the Alternatives;

(4) Documentation and Communication.

The methodology inputs are the requirements. The first step output is the decision-making framework. The second step output are the alternatives with estimated values, costs and risks. Here, we have used experts' viewpoints to build reliable model. Main premise was, if a person is considered to be an expert in the given domain, his estimates are credible and close to the real values. The third step output is the comparison of values, costs and risks. The end result is the guideline supporting the decision-making on the implementation.

There are four tasks to be completed in the first step (VMM, 2018), which are the following:

(i) Identify and define value structure;

(ii) Identify and define risk structure;

(iii) Identify and define cost structure;

(iv) Begin documentation.

As a result of the completion of the aforementioned tasks, we get a value structure with priorities, the list of risk factors and the cost structure. The value structure consists of the five following factors: direct customer value, basic/operational value for the State, strategic/political value, financial value for the State and social/public value. Those factors are described as follows (VMM, 2019): (i) Direct Customer Value: Benefits directly realized by the customer or a group of customers. The customers can be government employees, government agencies, citizens, etc; (ii) Basic/Operational Value for the State: Improvements of the current government operations and processes; (iii) Strategic/Political Value: Benefits which bring the organization closer to achieving its strategic goals; (iv) Financial Value for the State Financial benefits (cost reduction); (v) Social/Public Value.

Benefits which are not directly related to the Customer but to the society as a whole.

Value structure describes the benefits through two different layers. The first layer consists of the five aforementioned factors that must be analyzed in order to identify the opportunities for the creation of value for the society, government and individuals. The second layer includes the measures defining such values within a quantitative framework.

Following step-by-step algorithm is performed:

(i) Numerous of alternatives defined and five experts involved in evaluating those alternatives;

(ii) Individual pair comparisons performed by experts are modelled;

(iii) Individual pair comparisons are aggregated using a geometric mean method with individual expert competence considerations;

(iv) Alternative weights are calculated as eigenvalues of aggregate pair comparison matrices built with expert competence consideration;

(v) Results are discussed.

As part of risk identification, risk factors must be identified, as well as the risk occurrence probability and the risk impact. The list of costs records the expenses associated with the defined values. This methodology assesses the return on investment through a sort of a compromise between the value (benefits), costs and risks (VMM guide, 2018). Therefore, the assessment based on this model includes a multidimensional analysis of value, such as the direct customer value, social/public value, financial value for the State, operational/basic value for the State and strategic/political value. The aforementioned values are measured through a set of elements. Accordingly, it becomes possible to make a decision for each element. This method is not just about achieving the benefits or reducing costs; both aspects are included in an objective way. Such a VMM model allows for a comparison of different values. Moreover, it provides qualitative data to decision and policy makers who support the assessment of potential benefits of using specific services.

3. Assessing the cost-effectiveness of introducing Blockchain into the Croatian Public Administration

Blockchain is a technology providing the Internet values: it is a new, distributed ledger which can help us transform the business world and change the old order of people's jobs for the better. When considering the potential application of the Blockchain technology in the Public Administration, the three essential Blockchain values provide the potential solutions. Those values are the following: record keeping, value transfer and smart contracts. Wherever there is a need for one of the three values, the Blockchain technology must be considered as a potential solution.

3.1 *Identity management*

Digital identity is a trigger allowing for the integration of the remaining Blockchain elements. Whether it is about cryptocurrency or a car, each property must be electronically stored in order for it to be included into a Blockchain transaction. In doing so, the owner or the person who is carrying out the transaction needs a digital identity so as to be involved in the transaction. The importance of this challenge has been recognized by the participants in the public sector worldwide, where one-fifth of the population lives with no officially recognized identity.

Potential challenges are: (i) lack of standards necessary to establish a digital identity, and (ii) different types of verification procedure hinder the economic engagement and may obstruct the provision of public sector services.

Potential values are: (i) a safe identity could provide efficient transactions within a wide range of different types of assets, and (ii) individual and explicit control over the purpose into which the elements of identity are divided.

3.2 *Land registration*

A reliable property records can be created by ensuring a unique and non-corrupted record on Blockchain and evaluating the record status changes among the owners. The purchase of houses and/or land and their transfer through a safe system would serve as a basis for investment and economic growth. Potential challenge lies in licenses and registration procedures which are based on paper and are fragmented. It makes them expensive, inefficient and vulnerable to unauthorized handling. Potential values are: (i) a decentralized and standardized land registration system could reduce the number of the required intermediaries, increase the degree of confidence in the identity of parties involved in the transaction, increase the efficiency of the procedure and reduce the time and costs of process implementation; and (ii) the recording of proprietary rights through Blockchain would significantly reduce the costs.

3.3 *Voting*

The voting activity is a common topic when it comes to the application of Blockchain. Potential challenges with this one are: (i) cyber-attacks could compromise the election results, and (ii) delayed results or inefficiencies associated with remote voting. Potential values: (i) Reduced costs through voting enabled by Blockchain, (ii) Increased voting safety, (iii) Higher voter turnout, and (iv) Increased transparency.

Accordingly, this paper suggests applying Blockchain in the public sector for the following purposes.

3.4 *Blockchain types*

Blockchain are divided into two main categories: public and private. Public Blockchain allows participants to read it and use it to carry out transactions, and to participate in the process of creating the consensus (Guegan, 2017). There is no central register, nor a trusted third party. Public Blockchain works with a coin or token. Blockchain is private (or mixed) if the consensus process can only be achieved by a limited number of participants. The private Blockchain doesn't have to use mechanisms based on cryptography (Guegan, 2017). Private and mixed Blockchain are faster and consume less energy because there is lower number of transaction checkpoints. The public are completely democratic and open, but slower and more energy demanding.

In the context of selection of Blockchain for public administration, only a private type of Blockchain is suitable for public administration because all rights to conduct transactions on the network and information belong to the state. Users, citizens or organizations, have access to the system with a key.

3.5 *Purposes of Blockchain implementation*

There are numerous purposes of Blockchain implementation: identification, registers, payments assuming responsibility, and automation.

The days when identity checks had up to a few dozen steps are over. With digitized birth certificates and ID documents Blockchain provides a single personal identifier. It is a completely new and reliable member identification method which includes both the identification of citizens and government agencies, providing all sorts of services from electronic voting to confidential legal dispute settlement.

Blockchain provides the digitalization of land registry, vehicle registration and medical records registration, and more. Once recorded, the documents become digital evidence, available, for example, for a reliable utilization in legal battles. This reduces the printing and tracking costs, with smart contracts that can automate the specific activities. For instance, by introducing the electronic driver's license, the owner can receive a notice of the expiry or can simply renew the license through the automatic debit payment from the owner's bank account.

There is a great potential for the use of Blockchain and cryptocurrencies by the existing financial institutions. Blockchain technology has a huge potential for fraud elimination and for eliminating the possibility of tax evasion owing to the transparent and reliable built-in protocols. Social security benefits, supports, tax returns and cross-border payments can be automated and accessible to the public.

Blockchain enables one to assume responsibility in all the sectors. Financial development and cash flow can be permanently recorded and tracked; the results of votes can be updated online in real time. Public services can be easily accessible to the citizens, owing to a new degree of transparency.

The performing of processes related to application submission, payments made and received, issuing visas and license transfer can be simplified compared to previous years. Blockchain is particularly useful in the development of the market the existing infrastructure of which could not accept the radical change otherwise.

In this context, Blockchain could represent the key step in the implementation of applications of public interest:

- The implementation of a digital identity online for the purpose of e-services;
- Creating the online voting (e-voting) platform;

- Improving public registers and notarial services;
- Improving the land registry system;
- Increasing transparency and assuming responsibility in the financing of political campaigns and political parties;
- Creating new intellectual property licensing, copyright collection and management systems, less dependent on intermediaries;
- Preparation of certificates of origin for physical products, such as wood, preventing marketing from illegal areas;
- Creating a complete IoT platform (Internet of Things);
- Creating a new certificate layer in Agriculture, encouraging green and environmentally friendly practices.

4. Research results

For the afore-mentioned application examples, the cost-effectiveness analysis is performed by group of experts through the VMM methodology steps, which is given below. Blockchain values in the Public Administration System were identified as follows:

Direct (for users)

- Simple approach to services (license renewal, bill payment services): in terms of the effort invested into locating and obtaining services;
- Faster services: in terms of the time required for service delivery and/or reducing of waiting time, faster execution of transactions;
- Better services: in terms of the quality and added value of service characteristics (such as service delivery process transparency);
- Increasing users' satisfaction with the services;
- Increased transaction safety.

Basic/operational for the State

- Increasing the volume of service provision: in terms of the number of administrative transactions and the number of service users;
- Improved, shared infrastructure;
- Increased employee productivity: redistribution of a large number of hours of economic productivity in the reduced document processing time;
- Elimination of redundant procedures;
- Increased public sector efficiency: providing paperless transactions.

Strategic (political)

- Building international relations: strengthening international business relations, selling services worldwide;
- Strengthening the economy – through additional revenue generated by the companies providing products and services (such as bank accounts, postal services, etc.) – leads to the increasing of the Croatian GDP;
- Improving the State's image: with no investment in marketing;

- Creating new business opportunities in the private sector;
- Increasing the level of trust from the citizens;
- Financial for the State;
- Reduced service provision costs (such as reduced costs of holding elections);
- Reduced internal operating costs due to the reduced:

  (a) costs associated with paper production and distribution,

  (b) human resources performing manual tasks, such as paperwork handling,

  (c) form sending and processing, all as a result of the electronic provision of services.

Social (public)

- Reduced CO2 emissions: due to reduced traveling;
- Increased participation of citizens in political processes: higher voter turnout;
- Increased confidence in the Government's ability to authenticate users: leading to an increase in the citizens' safety;
- Reduced number of identity theft frauds.

The analysis of the values of Blockchain leads to the conclusion that the implementation would bring more administrative transactions and clients due to an increased visibility and availability of services. At the same time, it would enable the citizens and business partners to establish new companies using technology. The State would make multiple financial savings through the reduction of costs in terms of distribution, as well as human resources. The last but not the least, there is a number of non-quantifiable benefits, such as the feeling that the State contributes to strengthening business and international relations through this initiative.

4.1 *Value analysis*

Analytic Hierarchy Process (AHP) methodology has been previously used in strategic decision making (e.g. Oreški, 2012) and decision making in government (e.g. Đurek, Kadoić & Oreški, 2021). The application of AHP is given below. It is used for the purpose of determining the weights of specific values and groups of values. Previous research papers suggest (Glass, 1999; Procaccino et al., 2002) that experts' opinions have deep divergence between managers/users/members of the development team regarding importance and risks of involved factors, as well of different levels of management. Whereas managers/users focus their attention on budget and business objectives, the members of the development team mainly pay attention to technical aspects. Thus, in this work, different views were taken into account. Five experts were included consisting of: deputy mayor of a county, deputy mayor of a city, deputy mayor of municipality, user/vice dean of IT faculty, Member of Parliament.

The goal is to obtain the experts' perceptions of different decision-making levels about the importance of values in order to establish a rank among them. It is a valuable effort, since different levels of management have significantly different perceptions on such projects' success.

Table 1 in appendix shows the weights for each category. As all experts' opinions were considered to be of the same importance, geometric mean was used as the aggregation method for the calculation of the average weights. It is important to note that consistency ratio associated to the comparison matrices are far below the maximum value, 0.1, suggested by previous research papers (Zahedi, 1986). According to the obtained results, the direct user value has the largest weight, which is followed by the basic, operational value for the State. Strategic and financial values are of the same weight, while the social values have the lowest pondered value. As shown in Table, more simple approach to services was the most critical factor in the Direct value for category of users. Improved, shared infrastructure was the most critical factor in Basic/operational for State value category.

Creating new business opportunities in the private sector and Increasing the level of trust from the citizens were the most critical factors in the Strategic (political) category. Increased participation of citizens in political processes: higher voter turnout is most important Social benefit.

Reduced service provision costs shown to be more critical than Reduced internal operating costs in Financial for the State category.

4.2 *Risk and cost analysis*

It is difficult to identify the risks and manage them when the final results of such an implementation as well as its implications are still difficult to grasp. However, there are several groups of potential risks which must be pointed out.

Political risks are associated with the Government's consistency which is necessary for maintaining the funding stability and legislative priorities which change frequently with the changing of the coalitions in power. The main political challenge is, therefore, is to maintaining the importance of the project for the coalitions in power, thus enabling the project's sustainability, maintaining the project's independence at the same time in order for the project to attract the support of the people with broad political interest. The other potential risk regards communication and public relations. The idea of using the technological platform to build a global user database is more typical of the business world than of the public administration sector. The third group of risks are technological risks. User safety is the main prerequisite for a successful implementation of such technology in the public administration sector. Further technological risks regarding cyber-attack threats. Today, the protection of digital services and databases supporting them is crucial to national security. Experts have rated those risks probabilities and their possible impacts on project implementation. Results are presented in table 2 in appendix. Experts consider Lack of standards for establishing a digital identity mostly as risk of low or medium probability to occur. Most of the experts see impact of this risk on project as medium. No expert considers this risk as high impact on project. Political risk is recognized as risk of low level by majority of experts. However, there is no consensus among experts regarding impact of Political risks on project implementation, where opinions vary from low to high. According to experts, Communication with citizens seems to be risk of low probability and low impact of Blockchain implementation in public administration, whereas Cost overruns are risk of medium probability. Experts gave software failure risks more place for consideration then hardware failure risks.

Recent research studies (e.g. Sresakoolchai & Kaewunruen, 2020) emphasize importance of proper risk allocation to assure that projects can be run smoothly.

The final task as part of the first step is the cost assessment. In this paper, specific costs are not listed due to prices variation, but groups of costs are identified which will be incurred by such implementation.

System planning and development (Hardware costs*,* Software costs*,* Development costs*,* Analysis costs*,* Travelling costs).

System implementation (Purchasing costs*,* Personnel costs*,* Training costs).

System maintenance (Hardware costs, Software costs, Technical support costs).

This is where we can identify the three basic types of costs, which are the following: the system planning and development, system implementation and system maintenance costs.

5. Conclusion

The literature review has shown a great potential of the implementation of the Blockchain technology in the Public Administration sector. The examples of the good practices of developed countries investing ever more in Blockchain is encouraging and provides an incentive for the implementation of the same system in Croatia. The VMM methodology was used to analyze the values, risks and costs that such an implementation would bring based on experts' opinions.

The main strengths of this paper are two-folds: (i) as far as we know, this research represents first scientific approach to analyze Blockchain in Croatian public administration, (ii) it provides a method for ranking critical success factors of Blockchain implementation in Croatian public administration and it also allows a consistency measure of results.

Here, we have proposed an application of the analytic hierarchy process to rank different critical success factors related to Blockchain implementation. This approach performs better than results based just on qualitative analysis. It is important to note, by using this approach, the level of importance of each factor is compared to the others.

Acknowledgements

This research did not receive any specific grant from funding agencies in the public commercial, or not-for-profit sectors.

The authors declare no competing interests.

References

Alketbi, A., Nasir, Q., & Talib, M. A. (2018). Blockchain for government services – Use cases, security benefits and challenges. In *15th Learning and Technology Conference* (L&T) (pp. 112-119). IEEE.

Bishr, A. B. (2019). Dubai: A city powered by blockchain. *Innovations: Technology, Governance, Globalization*, *12*(3-4), 4-8.

Drucker, P. F. (2003). *A functioning society*. New Brunswick, NJ: Transaction.

Đurek, V., Kadoić, N., & Oreški, D. (2021). Effective decision making in local government using the hybrid approach based on multi-criteria decision-making methods and machine learning. In *16th International Symposium on Operational Research* (SOR 2021) (pp. 565-570).

Glass, R. L. (1999). Evolving a new theory of project success. *Communications of the ACM*, *42*(11), 17-19.

Guegan, D. (2017). Public blockchain versus private blockchain, halshs-01524440.

Hyvärinen, H., Risius, M., & Friis, G. (2017). A blockchain-based approach towards overcoming financial fraud in public sector services. *Business & Information Systems Engineering*, *59*(6), 441-456.

Jalakas, P. (2018). Blockchain from public administration perspective: Case of Estonia. Tallinn.

Jayasinghe, D., Cobourne, S., Markantonakis, K., Akram, R. N., & Mayes, K. (2017). Philanthropy on the Blockchain. In *IFIP International Conference on Information Security Theory and Practice* (pp. 25-38). Springer, Cham.

Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. *IEEE Software*, *35*(4), 95-99.

Mataracioglu, T. (2015). On the technical description of value measuring methodology. *International Journal of Managing Value and Supply Chains* (IJMVSC) Vol. 6, No. 2, June 2015.

Ojo, A., & Adebayo, S. (2017). Blockchain as a next generation government information infrastructure: A review of initiatives in D5 Countries. In *Government 3.0 – Next Generation Government Technology Infrastructure and Services* (pp. 283-298). Springer, Cham.

Oreški, D. (2012). Strategy development by using SWOT-AHP. *Tem Journal*, *1*(4), 283-291.

Pawlak, M., Poniszewska-Marańda, A., & Kryvinska, N. (2018). Towards the intelligent agents for blockchain e-voting system. *Procedia Computer Science*, *141*, 239-246.

Procaccino, J. D., Verner, J. M., Overmyer, S. P., & Darter, M. E. (2002). Case study: Factors for early prediction of software development success. *Information and software technology*, *44*(1), 53-62.

Sresakoolchai, J., & Kaewunruen, S. (2020). Comparative studies into public private partnership and traditional investment approaches on The High-Speed Rail Project Linking 3 Airports in Thailand. *Transportation Research Interdisciplinary Perspectives*, 5, 100116.

Sullivan, C., & Burger, E. (2017). E-residency and blockchain. *Computer Law & Security Review*, *33*(4), 470-481.

Vacca, A., Di Sorbo, A., Visaggio, C. A., & Canfora, G. (2020). A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges. *Journal of Systems and Software*, 110891.

VNM (2019). An Overview of Value Measuring Methodology (VMM). Available at http://www.cioindex.com/article/articleid/98962/anoverview-of-value-measuring-methodology-vmm, retrieved 12.09.2019.

VNM guide (2019). Value Measuring Methodology Guide. Available at http://www.cioindex.com/article/articleid/791/value-measuringmethodology-guide, retrieved 12.09.2019.

Zahedi, F. (1986). The analytic hierarchy process – A survey of the method and its applications. *Interfaces*, *16*(4), 96-108.

Center for Open Access in Science ▪ https://www.centerprode.com/ojit.html
Open Journal for Information Technology, 2024, *7*(1), 11-22.
ISSN (Online) 2620-0627 ▪ https://doi.org/10.32591/coas.ojit.0701.02011m

Data Protection in Healthcare Information Systems Using Cryptographic Algorithm with Base64 512 bits

Agnes K. Muthaura & John Kandiri

Kenyatta University, School of Applied Sciences, Nairobi, KENYA

Received: 4 April 2024 ▪ Revised: 3 July 2024 ▪ Accepted: 9 August 2024

Abstract

Recent advancement in technology in Healthcare Information Systems has led to a rise in cyber-attacks and data leakages at the data level. Existing data-level protection techniques that are developed to ensure data-level protection in Healthcare Information Systems lack integration of key security models such as Mandatory Access Controls, Role Based Access Controls and database security approaches in the design and development of data protection methods. In this study, science research methodology was used to design and develop a cryptographic algorithm with Base64 512 bits to enhance data protection at the data level. The algorithm was tested in a healthcare information system through experiments and simulations. The performance of the algorithm was tested to evaluate encryption and decryption process, strength on brute force attack and plain text vulnerability. The results of the observations showed that the developed algorithm with Base64, AES with fixed length of 512 bits, achieved optimal performance.

Keywords: mandatory access controls, role based access controls, discretionary access controls, label based access controls, advanced encryption standard, electronic medical records.

1. Introduction

Healthcare Information System is a system that is used in a healthcare facility to capture and store patient's data (Scott-Clark, 2023). In most cases these systems are classified as distributed systems because they are connected to several other systems and networks for proper management of patient data (Scott-Clark, 2023). To avoid information leakage, patient data which is very confidential must be protected at the application level and at the data level as leakage of this information leads to serious medical legal issues. As the number of medical records stored electronically increase, enhancement of how this data is secured must be considered (Scott-Clark, 2023). Delay in the retrieval of patient records at the right time can cause death and also lower the level of health care services offered by the healthcare facility (Babatunde et al., n.d.). Criminal assaults in social insurance have exponentially increased since 2010 and are now the leading cause of medical data breaches (Babatunde et al., n.d.). Almost all healthcare organizations have encountered no less than one data breach, costing million dollars on average per organization (Babatunde et al., n.d.). The level of security and data protection in Healthcare Information Systems varies from one healthcare facility to the other. Healthcare Information Systems are generally integrated with Electronic Medical Records. The health information system stores bio data of the patient which include name, sex, gender, religion, marital status, date of birth and many more and Electronic Medical Record system stores the clinical data for the patient such as

Correspondence: Agnes K. Muthaura, Kenyatta University School of Applied Sciences, Nairobi, KENYA.

vital signs, allergies, diagnosis, investigations, medications, assessment, recommendations and patient medical history (Scott-Clark, 2023). The patient data stored as clinical data is the most sensitive data that must be encrypted using an enhanced cryptographic algorithm and secured with a private key (Devin Partida, 2022). The existing data protection models and database security methods and techniques focus more on protection of data on subjects (users) access to the system and less focus on objects(data) protection at data level. The implementation of data protection at the database level is generally configured as a default setting such as Mandatory Access Controls (Bell La Padulla models, Biba Models, Clark & Wilson models) (Diamantopoulou et al., 2017a). Electronic Medical Records in Healthcare Information Systems must be protected using enhanced cryptographic algorithm at the data level. The main objective of this study was to develop an enhanced cryptographic algorithm with Base 64 512 bits to protect data at the data level.

2. Background

Data protection in Healthcare Information Systems at the data level is very critical and sensitive and it offers privacy and confidentiality of patient data and information. Patients' data must be protected from access control level, the front end and at the database level, the backend. There has been an increase on the use of technology in healthcare sector and thus increased use of Healthcare Information Systems. This has also led to an increase in cybercrimes in Healthcare Information Systems (Diamantopoulou et al., 2017a) and this calls for improved data protection algorithms in healthcare data using enhanced Cryptographic Algorithms. Data protection in Healthcare Information Systems focus more on the access control level (application level) and less focus at the data level (Database level) thus allowing a very huge risk of data exposure for patient data at the database level or the backend. An attacker can easily hack the log in details and access the system through frontend by simply decrypting the passwords and if the patient data is not encrypted at the backend using enhanced cryptographic algorithms the information will be accessible by an unauthorized user. There is existence of cryptographic algorithms used in Healthcare Information Systems at the access level and database level but there is need for enhancement using enhanced cryptographic algorithm proposed in this research. It is estimated that thousands and millions of personal data and information of patients is leaked especially on their credit cards and bank details (George & Bhila, 2019). Healthcare facilities and public health sector invests quality time in the data lifecycle (George & Bhila, 2019)

The General Data Protection Regulation goal is protection of sensitive or confidential data and unforeseen risk of data loss or theft, encryption makes sure that all confidential or sensitive information is protected by an agreeable security level at the destination and at the source (Diamantopoulou et al., 2017b).

3. Literature review

This is the detailed literature review of enhanced cryptographic algorithm Base64 512 bits, database approaches and securities, healthcare information system vulnerabilities and the various security models. Cryptography is the study of mathematical calculations and techniques, cryptography function transfers plain text into cipher text (encryption) and transfers cipher text into plain text (decryption). Some refer cryptography to "secret writing" (Ahmed et al., 2018). The plain text is encrypted to cipher text and decrypted into plain text using a security key or security keys, enhancing data protection in Healthcare Information systems is a mandatory requirement and a sensitive activity that requires protection of both subject (users) and objects (data) (Harman et al., 2012). The patient data and information must be secured from application access control level to database access control level. This guarantees security of sensitive data and information from end to end and improves on patients care and user experience.

3.1 *Hill ciphers*

This is one of the oldest cryptographic algorithms that was developed by Leiser Hill in 1929 and uses mathematical manipulations such as linear Algebra. To enhance the algorithm, matrix manipulation is used and uses Mod 26. This means the alphabets A to Z are substituted with numbers or integers 1 to 26 to encrypt and decrypt data. Unfortunately, this algorithm has high known plain text vulnerability. Studies show that Hill Cipher has been modified using mathematical manipulations to strengthen the algorithm from known plain text vulnerability attack and brutal force attack. The modified Hill Cipher has a higher avalanche effect as compared to the original Hill Cipher. Despite this modification the algorithm is vulnerable to known plain text, uses a private key and its performance is slow on decryption of the encrypted data.

3.2 *Security models*

There are several security models that enhance data protection at the application access level such as OTP (One Time Password) and database access control level such as Mandatory Access Control models. These are the access control methods for Database security that focus only on confidentiality and integrity (Paragas, 2020). The other models that enhance data security include Bell La Padulla Models and Biba Models. Traditional data protection techniques such as masking, Image fusion, digital water marking and encryption are an expansion of Discretionary Access Control. DAS restricts access to objects(data) based on the identity of the subject (user). Role Based Access Control, aims at strengthening the security of data but only from the subject (user) access control level. RBAC restricts network access based on the roles of individual users within an enterprise. Thus, the traditional data protection models and access controls lack enhanced cryptographic algorithms to protect sensitive data in healthcare information systems at the object (data) level and that are very complex without compromise especially in this era of high increase in cybercrimes (Lucca et al., 2020). Data protection in healthcare information system can be enhanced by use of enhanced cryptographic algorithm that validates the subject (user) on access at the application level to the (Object) database level by encryption and decryption of the patient data.

3.3 *Database security in Healthcare Information Systems*

Database security is incorporated in every database and has several layers and with the security types such as access control, auditing, authenticating and encryption. Database security approaches in Healthcare Information Systems classified as authentication-based security, trust-based security approaches, access control (DAC, MAC and RBAC Models) based approaches and Cryptographic based approaches (a technique for securing database) (Rjaibi & Bird, 2004). lacks an enhanced data level protection algorithm to guard the data against the emerging advanced cyber-attacks techniques.

From review of the literature, the research identified a gap in the existing types of cryptographic algorithms in healthcare information systems at the data level. The most default security configuration used as cryptographic algorithms to offer data level protection are inadequate and thus the patient data is vulnerable to cyber-attack. MD5 algorithm is used for user authentication and a TDE (Transparent Data Encryption) algorithm that encrypts sensitive data stored in tables and table spaces. This data is transparently decrypted for authorized users and applications to access the data. Transparent Data Encryption algorithm is adequate for data stored in a media and the decryption security key stored in a separate module from the database (KeyStore), if the hacker happens to hack the password or gain access to KeyStore the patient data would be compromised. A lot of effort has been noticed in identifying the existing cryptographic algorithms in healthcare information systems, a Modified Hill Cipher cryptographic algorithm was identified as the most adequate for enhancing data privacy and protection for sensitive data. This research project informed that the challenge of securing data access at the database level by cryptographic algorithms can be solved by enhancing the existing cryptographic algorithms. "Modified Hill Cipher cryptographic algorithm where cipher text could not be easily predicted and that it has substantial strength and ability to withstand data breach on information ("Health Data in the Information Age," 1994). Modified Hill Cipher cryptographic algorithm had a higher avalanche effect compared to the original Hill Cipher. This means that the Modified Hill Cipher cryptographic method passes the minimum average avalanche effect (Paragas et al., 2019) The average entropy index obtained by the Modified Hill Cipher cryptographic method was higher than the entropy index obtained by original Hill Cipher, which means that the cipher text is unpredictable in Modified Hill Cipher cryptographic method, compared to the original hill cipher, which has a lower entropy index (Paragas, 2020). This modification of original hill cipher to a modified hill cipher demonstrated a significant improvement in strengthening the security of the cipher. This reduces the capability of a known plain text attack by ensuring security at the data level in healthcare information systems.

This study examined that enhancing cryptographic algorithms at the database level improves on the data privacy in healthcare information systems. The proposition of implementing this project study will be a great achievement in providing a solution to data protection and privacy of sensitive data at the database level in healthcare information systems.

3.4 *Evaluation criteria of acceptable cryptographic algorithm*

Adequate data level encryption algorithm must have at least the following features which include, utilization of RBAC, strength on brute force, known plain text vulnerability, use of private key and ease of data decryption and database performance. An evaluation criterion was used to test the adequacy of each security feature for each specified cryptographic algorithm at the data level. This determined how the cryptographic algorithm Base64 512 bits was designed and developed for adequate data level protection.

4. Materials and methods

This chapter describes detailed research design methods and methodology in a systematic way on how cryptographic algorithm Base64 512 bits was designed, developed, tested and deployed for data protection in healthcare information systems. The methodology that was used to develop the cryptographic algorithm Base64 512 bits was the design science research methodology. This research methodology was best suited for this research because it combined both mathematical and computational methods that assisted in developing the algorithm. This contributed to measuring the quality of developing the artefact. It is based on guidelines that are branched from several science disciplines and this made the integration of security models and database security approaches simple during the implementation phase. It adopts proof methods of verification as opposed to existing empirical methods and this enabled extensive testing of the artefact and thus accurate results.

4.1 *The design science approach in research methodology*

This research work adopted the design science approach as the research methodology because primarily it involved studying of existing security frameworks such as MAC Models (Biba, Bell La Padulla, Clark Wilson) and the existing database security methods such as various cryptographic algorithms (Symmetric and asymmetric) and access controls such as RBAC and DAC. The research studied how security algorithms have been implemented in healthcare facilities and in theories on literature review. The study analyzed the existing security algorithms, their features and characteristics in data protection for enhanced security at the data level. The results of the analysis of the existing security algorithms determined how the artefact was developed. The developed model was evaluated and tested in a healthcare Information system to check its viability. The developed model was implemented iteratively until the users considered the algorithm fit for use.

4.2 *Cryptographic algorithm Base64 512 bits development*

This section describes how the model was developed from requirement gathering and analysis to design, testing and analysis of test results. The artefact was designed and developed from the analysis of the security features and characteristics of the existing cryptographic algorithms obtained from literature review.

4.3 *Requirements analysis and data classification*

Requirements for artefact development were obtained from literature review. The requirements for system development were obtained from the analysis of the results from evaluation criteria of the main characteristics and features of an acceptable cryptographic algorithm. The cryptographic algorithm that was found to achieve the minimum requirements was identified and the features that did not meet the criteria were improved to develop a cryptographic algorithm Base64 512 bits at the data level. Modified Hill Cipher was identified and the following features were enhanced RBAC, use of private key and ease of data decryption and database performance.

The features and characteristics of existing cryptographic algorithms that were incorporated for artefact development were as obtained from the literature: Strength on brute force attack, known plain text vulnerability, use of private Key, Ease of data decryption and Database performance, Role Based Access Controls. The evaluation and analysis of the features and characteristics of the existing cryptographic algorithms that were obtained as the input requirements for the artefact development were classified accordingly.

4.4 *Design phase*

The requirements gathered during requirement gathering phase were incorporated to design a model that was used for development of the cryptographic algorithm Base64 512.The design of the artifact was based on design modelling tools such as the use case diagrams, sequence diagrams and a class diagram for the database structure. This phase involved description of a component diagram from the use case diagram and the algorithm data flow diagram was used to display the implementation of the prototype.

4.5 *Development phase*

Development of the artefact was done using Python programming language and involved integration of the following data level security measures as identified from literature review: Role Based Control Access, brute force attack, known plain text vulnerability, private key, ease of decryption and database performance. Each of the security measure was implemented at different levels and stages as illustrated in Figure 3.3. To ensure authentication of users, roles and password profiles access to the database, a Role Based Access Control security measure was implemented. This security measure involved restriction of users and applications from accessing the database thus a user could only access the database according to the roles and permissions assigned to them and according to the verification of their passwords. MAC security models: Biba and La Padulla security measures were added to RBAC to control the extent to which read and write actions could be executed by a user or an application. To enhance the strength on brute force attack MD5 hashing function encryption algorithm was used to mask passwords permanently and a password policy. The password policy was to ensure that all the parameters set by a user to access the system would comply with the policy. Thus, any attempt by an unauthorized user to guess the password would be impossible. Advanced Encryption Standard, Base64 Algorithm, 512 key length bits was used for encryption and decryption of data stored at the database and this was to improve known plain text vulnerability. Combination of AES and Base64 algorithm with an additional of 512 bits at the data level made it very difficult for any malicious attacker whatsoever to guess the plain text that was encrypted to cipher text. Delay in data retrieval can lead to death and Medical legal penalties thus ease of data decryption and database performance as a security measure, database optimization was automatically configured for each row, column, table and views. This ensured that the speed of data decryption was fast to allow for ease of access to data at the data level when necessary.

5. Results and analysis

This chapter contains a detailed discussion of the results of the research findings and detailed explanation of how each of the specific objective of the study was achieved.

5.1 *Existing data encryption algorithms in healthcare information systems*

The first objective of this study was to investigate the existing data encryption algorithms in Healthcare Information Systems and their security characteristics for data protection at the data level. An evaluation criterion was used to test the adequacy of each security feature for each specified cryptographic algorithm at the data level. This determined how the cryptographic algorithm Base64 512 bits was designed and developed for adequate data level protection. The evaluation criteria of an acceptable cryptographic algorithm in healthcare information systems were conducted from the literature review and modified hill cipher cryptographic algorithm was identified to have minimum acceptable characteristics for data protection- at the data level. The cryptographic algorithm characteristics for data protection at the data level identified in modified hill cipher were enhanced to develop cryptographic algorithm with Base64 512 bits. The comparison of characteristics for data protection at the data level between modified hill cipher and the developed cryptographic algorithm with Base64 512 bits was conducted by simulation and experiments in a healthcare Information system. Most security characteristics for data protection at the data level of modified hill cipher resulted to perform better than the other algorithms and thus it was considered for comparison with the developed cryptographic algorithm with Base64 512 bits. The results showed that modified hill cipher cryptographic algorithm lacked utilization of RBAC matrix while the developed cryptographic algorithm with Base64 512 bits had RBAC implemented. Modified hill cipher algorithm was weak on brute force attack and high known plain text vulnerability while cryptographic algorithm with Base64 512 bits was strong on brute force attack and low known plain text vulnerability. Modified hill cipher was slow in encryption and decryption of data for storage and retrieval from the database while the developed algorithm performed at optimum database speed. Both modified hill cipher and the developed algorithm had private key implemented for secure of data access to the database.

5.2 *Data protection techniques Analysis in Healthcare Information Systems at the data level*

The second objective was to evaluate data protection techniques in Healthcare Information Systems at the data level for integration in the design of the cryptographic algorithm with Base64 512 bits. The following are the major data protection techniques as they were obtained from literature review: Authentication Based security, Trust based security, cryptographic based models. Analysis for the identified data protection techniques was conducted to prove that they were the major data protection techniques. Authentication based security was analyzed for authentication of users and applications into the database. Authentication method was instantiated to different applications and different users for validation. Users and applications were authenticated into the system using their specific user IDs, application IDs and passwords. The results showed that adequate implementation of authentication methods improved security at the database level as compared to modified hill cipher that had no authentication methods. The analysis of Trust based security technique was obtained from vigorous testing of trust-based security methods into the system. This was done by testing to ensure that the users and applications performed the functions that they were designed to perform. When a user or application was subjected to unmatched function it would fail. The results showed that the developed cryptographic with Base64 512 bits enforced trust-based security. From the analysis of the results, it was observed that incorporating trust-based methods in a healthcare information system enhances security at the data level. Access control-based security analysis was conducted by designing roles, permissions, users and access controls to the database. Different users and applications were assigned different roles to perform specific actions in the system. Database actions (CRUD) create, read, update and delete were performed to ascertain that specific users with specific roles could only access and perform specific actions. The developed cryptographic algorithm was found to only allow specific users and applications to access and perform specific actions at the database level. The results of the analysis indicated that a secure system is as good as the roles and permissions assigned to users and application to access specific actions at the data level. The analysis of cryptographic security-based models was conducted by testing of encryption and decryption of data of different sizes and the performance of the database. The developed cryptographic algorithm with Base64 512 bits showed that the encryption and decryption of data during storage and retrieval process did not affect database performance as re-indexing of tables, columns, rows and views was configured for automatic database optimization. The results of the analysis indicated that encryption of data at the data level is very critical as health information system stores very confidential data and that speed of database performance is very critical for retrieval and storage of data. During cryptographic based security model's analysis, known plain text vulnerability was tested to find out the impact and effect of a small change in cipher text. This showed that the plain text could not easily be guessed from cipher text. Cryptographic algorithm Base64 512 bits system was designed to incorporate the major database security models in healthcare information systems.

5.3 *Design and development of cryptographic algorithm with Base64 512 bits*

The main and third objective of this study was to design a cryptographic algorithm with Base64 512 bits for improved data protection in healthcare information systems. The following are the steps and stages of development of the cryptographic algorithm with Base64 512 bits that were followed to achieve the results of this objective:

1) Model development;
2) functional and non-functional requirements;
3) System design and modelling;
4) experiments and simulations.

5.4 *Performance evaluation of cryptographic algorithm with Base64 512 bits*

The fourth objective of this study was to evaluate the performance of the developed cryptographic algorithm with Base64 512 bits in protecting data in healthcare systems. This was compared with modified Hill cipher for evaluation and validation. The results of the comparison were the empirical evidence which showed that the developed algorithm performed better in terms of data encryption and decryption. The developed cryptographic algorithm with Base64 512 obtained optimal database performance as compared to modified hill cipher. To test the performance of the developed algorithm, various test scenarios were tested by a Senior Database Administrator, Senior Security Officer and Systems Administrator. The analysis of the various scenarios on performance of the cryptographic algorithm with Base64 512 bits were as follows:

5.4.1 *Encryption and decryption process*

The senior security officer tested the viability of the algorithm to validate that the algorithm meets the characteristics of cryptographic algorithm. This process involved input of data into the system, various types of data using CRUD (create, read, update, delete functionality) and verifying the raw data in the database to be encrypted as the operations were being carried out. The encryption and decryption process implemented on the developed cryptographic algorithm with Base64 512 bits was found to meet encryption and decryption criteria as compared to Modified Hill cipher which was observed to implement a very weak encryption and decryption technique that follows a known sequence of A to Z substituted into integers 0-26.

5.4.2 *Turnaround time for encryption and decryption*

In this scenario the system administrator tested the amount of time taken to encrypt and decrypt data during storage and retrieval processes. This was to measure the time delays for encryption and decryption- of data. A timer was set to calculate how much time it would take to encrypt data before it is stored in the database. The timer was set again to calculate the amount of time it would take to decrypt the data when retrieving the data for use. Different data sizes were obtained and tested for several scenarios. Small size of data was encrypted and decrypted and the speed of the database identified. A medium size of data was obtained, encrypted, decrypted and the speed of the database obtained. A larger data size was encrypted and decrypted and subsequently the speed of the database obtained. The amount of time-taken for retrieval and storage of data at the database was obtained at every scenario. The overall observation was that Cryptographic Algorithm with Base64 512 bits performed at optimal speed for both storage and retrieval process and for all data sizes as compared to modified Hill Cipher that was observed to slow database performance as the size of the data increased.

5.4.3 *Strength on brute force attack*

The senior security officer in this scenario tested the strength of the Algorithm for brute force attack. Several attempts to gain access to the system through systematic guessing of password at login could not penetrate the database. This was because a robust password policy was implemented on the developed cryptographic algorithm with Base64 512 bits. To test the length of the password, the security officer would test different lengths of characters up to a minimum of eight characters. If the length was less than eight characters the test would fail and if the characters were more than eight characters the test would pass. To test the use of alphanumeric characters in a password the security officer would enter a mixture of numbers, digits and special characters. If any of the parameter was excluded into the password the test would fail otherwise if all the parameters were entered the test would pass. To test for password lock after a certain number of wrong attempts, the wrong password was entered the first time and the second time, this would give a warning that the account would be blocked if another wrong attempt was done. When the wrong password was entered the third time the account was blocked and access denied. To test restriction on use of names as a password, the system would check if the password contained a name similar to the username and if any similarity in the name was found the password would fail. The system timeout was also tested to ensure that if the user's screen was idle for a set time, the system would automatically lock the screen. The security officer tested this by logging into the system and allowing the time set to lapse for session time out to occur. The results obtained from these tests indicated strengthened brute force attack at the data level as compared to Modified hill cipher which was observed to be weak on brute force attack as the password policy was not implemented.

5.4.4 *Known plain text vulnerability*

This scenario was conducted by a senior security officer to test the level of vulnerability for known plain text. A very small change in plain text resulted into a very huge change on the cipher text. Any alteration in plain text would send a notification immediately to DBAs and System Security officers for immediate action. Audit logs were also created to keep a record of the change using encrypted plain text and altering it as is, to see the change when the data is decrypted. Examining the Master logs for the record of changes. The developed algorithm had a very low vulnerability on known plain text as compared to modified Hill cipher which was observed to have a higher known plain text vulnerability. A small change on plain text did not result to any significant change on the cipher text.

5.4.5 *Use of private key*

Database Administrators conducted this test scenario to test the importance of the private Key in the Algorithm and secure storage of the private Key. The DBAs confirmed that the private Key was stored securely and accessible to authorized users only. This private Key on the developed algorithm was stored in a different environment rather than the same environment where the system was running for private access only. The modified Hill cipher was observed to obtain a private key but it was stored on the same environment where the system was running.

5.4.6 *Role Based Access Control (RBAC)*

This scenario was to test the security of access level to the system. The test was conducted users with different roles and permissions to test access and modification of data in the system. The Database Administrators created users with specific roles and permissions to access specific objects and actions at the Database. The user nurse could only access the data that they had access to, and this was for all other users such as doctors, Health Information Officers and Finance officers. It was observed that the implementation of RBAC in the developed algorithm ensured secure access to the database for both users and applications. Only users and applications with the specific roles and permissions could access data at the database as compared to modified Hill cipher that did not have any access level implemented at all. The overall performance of the developed cryptographic algorithm with Base64, AES of fixed length key of 512 bits was found to be acceptable in all the scenarios that were tested.

6. Discussion and conclusion

This chapter contains three main sections namely, discussion which entails discussion on the key points of the results and the summary of the research findings, conclusion based on the objectives of the research, and the recommendation section which provides the recommendation based on the findings of the research.

6.1 *Key points of the results and the summary of the research findings of the experiments and simulations*

This section describes the key points of the results and the summary of the research findings of the experiments and simulations in a healthcare information system per objective of the study. Research findings indicated that the developed cryptographic algorithm had a very low risk of known plain text vulnerability, very strong on brute force attack, better on user management with restricted access to the database, fast database performance and a very secure private key. This was attained because of an additional security layer of Base64 and of AES with a fixed key length of 512 bits. Authentication of users and application to the database was implemented as Role Based Access Control and Mandatory Access Control to control user actions and application access at different levels of database access. This enhanced data protection at the data level. Comparing developed cryptographic algorithm Base64 512 bits with the existing algorithms such as modified hill cipher showed that the additional security layer introduced in the developed algorithm of Base64, AES algorithm and fixed length key of 512 bits reduced known plain text vulnerability, improved strength on brute force attack, enhanced ease of data decryption and performance of the database, improved role-based access control for user management and this made the developed cryptographic algorithm with Base64 512 bits different from other existing cryptographic algorithms.

6.2 *Conclusion*

This sub section provides a final summary of the research findings with the corresponding research objectives. From the research findings, all the objectives of the study were fully achieved as summarized herein. The following is the summary of the research findings with the corresponding specific objectives of this study.

The main objective of this study was to design an enhanced cryptographic algorithm with Base64 512 bits for improved data protection in healthcare information systems. A cryptographic algorithm with Base64 512 bits model was designed, a prototype was developed and tested through experiments and simulations in a healthcare information system. Additional security layer of encryption using Base64 algorithm and use of AES with a fixed key length of 512 bits improved significantly the security of the sensitive data in a healthcare information system. The second objective of the study was to investigate the existing data encryption algorithms in Healthcare Information Systems and their security characteristics for data protection at the data level. From research findings Symmetrical and Asymmetrical Data encryption algorithms were examined and the following major security characteristics were evaluated and incorporated in the design of cryptographic algorithm with Base 64 512 bits: The third objective of this study was to evaluate data protection techniques in Healthcare Information Systems at the data level for integration in the design of the cryptographic algorithm with Base64 512 bits. During the design phase of the cryptographic algorithm with Base64 512 bits the following data protection techniques in healthcare information system were examined and incorporated in the cryptographic algorithm model. Authentication based security techniques that ensured authentication of users and applications into the database, Trust based security techniques that improved on the management of system trust issues, Access control-based security (DAC, MAC, RBAC) that enhanced access control levels for users and applications into the database and Cryptographic based security Models that facilitated in strengthening the encryption and decryption of data. The fourth objective of the study was to evaluate the performance of the cryptographic algorithm with Base64 512 bits in protecting data in healthcare systems. When the algorithm was fully developed, it was tested to evaluate the performance. The evaluation was conducted in both experiments and simulations. Some scenarios were evaluated via experiments such as, role-based access controls, strength on brute attack and database performance which involved encryption and decryption to determine the speed of data retrieval and data saving. Known plain text vulnerabilities and use of private key was simulated in a simulator.

6.3 *Recommendation*

This section gives the take home message of what to DO or NOT to DO based on the findings foregoing and the conclusions. From the research findings it shows that patient data is very sensitive and critical and may even cause death if it is delayed. Patient data is very expensive, valuable and a greater target by cyber criminals. Therefore, there is need for continuous improvement and new innovations on data protection techniques and cryptographic algorithms at the data level in healthcare information systems at the same rate or above the rate at which the cyber criminals are inventing new ways of attack daily. As cryptographic algorithms are developed to enhance data protection at the data level by additional of the number of bits in the algorithm, the performance of the database may slow down and therefore causing delays. The developed cryptographic algorithm with Base64 512 bits would improve data protection of any sensitive and critical data at the data level and especially hospitals, government institutions that store personal sensitive information of its citizens, Military and examination bodies of any country. For future Research Work, since this study was based on literature review further research could be conducted in real life systems to compare the effectiveness of the major security characteristics. For optimal testing and better results on the performance of the algorithm all the preferred major security characteristics can be conducted both on experiment and simulation and can be preferably performed by qualified Database Administrators and Systems Security Administrators.

Acknowledgements

This research did not receive any specific grant from funding agencies in the public commercial, or not-for-profit sectors.

The authors declare no competing interests.

References

Ahmed, A., Abdulsalam, Y. S., & Olaniyi, O. M. (2018). Enhanced tiny encryption algorithm for secure electronic health authentication system. *International Journal of Information Privacy, Security and Integrity*, *3*(3), 230. https://doi.org/10.1504/ijipsi.2018.10013222

Babatunde, A. O., Taiwo, A. J., & Dada, E. G. (n.d.). *Information security in health care centre using cryptography and steganography*.

Diamantopoulou, V., Angelopoulos, K., Flake, J., Praitano, A., Ruiz, J. F., Jürjens, J., Pavlidis, M., Bonutto, D., Sanz, A. C., Mouratidis, H., Robles, J. G., & Tozzi, A. E. (2017a). Privacy data management and awareness for public administrations: A case study from the healthcare domain. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10518 LNCS*, 192-209. https://doi.org/10.1007/978-3-319-67280-9_11

Diamantopoulou, V., Angelopoulos, K., Flake, J., Praitano, A., Ruiz, J. F., Jürjens, J., Pavlidis, M., Bonutto, D., Sanz, A. C., Mouratidis, H., Robles, J. G., & Tozzi, A. E. (2017b). Privacy data management and awareness for public administrations: A case study from the healthcare domain. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10518 LNCS*, 192-209. https://doi.org/10.1007/978-3-319-67280-9_11

George, J., & Bhila, T. (2019). Security, confidentiality and privacy in health of healthcare data. *International Journal of Trend in Scientific Research and Development*, *3*(4), 373-377. https://doi.org/10.31142/ijtsrd23780

Harman, L. B., Flite, C. A., & Bond, K. (2012). State of the art and science electronic health records: Privacy, confidentiality, and security. *American Medical Association Journal of Ethics* (Vol. 14). www.virtualmentor.org712.

Health Data in the Information Age (1994). In *Health Data in the Information Age*. National Academies Press. https://doi.org/10.17226/2312

Lucca, A. V., Silva, L. A., Luchtenberg, R., Garcez, L., Mao, X., Ovejero, R. G., Pires, I. M., Barbosa, J. L. V., & Leithardt, V. R. Q. (2020). A case study on the development of a data privacy management solution based on patient information. *Sensors (Switzerland)*, *20*(21), 1-24. https://doi.org/10.3390/s20216030

Paragas, J. R. (2020, October 3). An enhanced cryptographic algorithm in securing healthcare medical records. *Proceeding – 2020 3rd International Conference on Vocational Education and Electrical Engineering: Strengthening the Framework of Society 5.0 through Innovations in Education, Electrical, Engineering and Informatics Engineering, ICVEE 2020*. https://doi.org/10.1109/ICVEE50212.2020.9243228

Paragas, J. R., Sison, A. M., & Medina, R. P. (2019). Hill Cipher modification: A simplified approach. *2019 IEEE 11th International Conference on Communication Software and Networks, ICCSN 2019* (pp. 821-825). https://doi.org/10.1109/ICCSN.2019.8905360

Rjaibi, W., & Bird, P. (2004). *A multi-purpose implementation of mandatory access control in relational database management systems*. In *Very Large Data Bases*. https://doi.org/10.1016/B978-012088469-8.50088-7

Center for Open Access in Science ▪ https://www.centerprode.com/ojit.html
Open Journal for Information Technology, 2024, *7*(1), 23-42.
ISSN (Online) 2620-0627 ▪ https://doi.org/10.32591/coas.ojit.0701.03023n

Crime Prediction and Mapping Using Machine Learning Algorithms

Lucas Ngoge, Kennedy Ogada & Dennis Kaburu

Jomo Kenyatta University of Agriculture and Technology, Nairobi, KENYA
School of Computing and Information Technology

Received: 4 April 2024 ▪ Revised: 3 July 2024 ▪ Accepted: 11 August 2024

Abstract

One of the major roles of government is to curb crime. Despite the measures the government has taken to counteract criminal activity, the security situation in many urban centers has gotten worse. The goal of this study was to create and assess a machine learning model with the core function of forecasting crime categories and utilizing contextual features found in the datasets to visualize the locations in which they occur. This was achieved by combining time, space, and contextual information with machine learning to improve crime prediction and mapping. The datasets were collected from various sources were subjected to a number of machine learning algorithms to evaluate how well they performed. The random forest algorithm emerged as the best algorithm with a classification accuracy of 97% or 0.973301 using the confusion matrix. The longitude and latitude features were used to tag the specific locations of crime occurrences on a map.

Keywords: machine learning algorithms, classification, prediction, mapping, data visualization.

1. Introduction

Like most urban settings in the world, Kenya battles with all forms of crime. There has been an upsurge in different types of crime as reported in many parts of urban centers, despite the strategies and efforts the government put in place to combat them as presented in (NPS, 2022). This situation is aggravated by the weak social control that operates through formal and informal institutions for reporting crimes that took place. Due to the aforementioned problems, it was necessary to review models that, from technology, have contributed to the improvement of the crime prevention strategies that guarantee public safety. The growth of research methodologies aimed at extracting data from records to better understand criminal patterns and ultimately prevent future occurrences has been brought about by the increase in the recording of crime data, but it may be challenging to resolve any case involving crime if there are no data available beforehand. Therefore, creating a machine-learning model that can classify data is necessary as stated by (Veena et al, 2022*)* are able to forecast classes using the features that are present in it. The increased use of these approaches in crime analysis has enabled significant advances in crime prediction and mapping. According to (Sarker, 2021) machine learning enables computers to automatically learn from experience without being explicitly designed. These learning algorithms are broadly categorized into two major types, namely supervised and unsupervised. In supervised learning, datasets are used to train, test, and produce the intended outcomes for the models, but

Correspondence: Lucas Ngoge, Jomo Kenyatta University of Agriculture and Technology, School of Computing and Information Technology, Nairobi, KENYA.

in unsupervised learning, the models classify or cluster an inconsistent, unstructured dataset. In a dataset by Kanimozhi et al. (2021) multiclass target variables were classified using supervised learning methods such as Decision Trees, Random Forests, Naive Bayes, K-Nearest Neighbors, and Support Vector Machines. Additionally, with these techniques, the crime predictors such as 'Incident_Number', 'Incident', 'Crime_Decsription', 'Crime_code', 'Crimetype', 'Arrest',' Age', 'Gender', 'Date', 'Year', 'Month', 'Location', 'Location_code', 'Lat' and 'Long' were used to correctly classify and predict a target variable.

A machine learning technique called classification divides data into labels or classes to help with accurate analysis and forecasting. In order to help forecast results based on a given input (Pratibha et al, 2020), it is utilized to develop patterns that accurately characterize the significant data classes within the data set. Classification algorithms look for connections between attributes that could help forecast the outcome. The algorithms are used to analyze input and produce a prediction as illustrated in Llaha (2020). Classification models are expected to input an unseen dataset and correctly predict category labels, as shown in Figure 1 below:

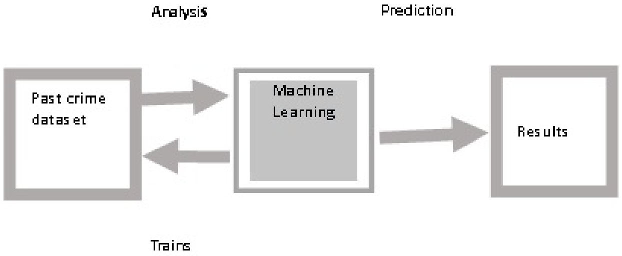


Figure 1. Classification process

Crime prediction is a process where a model uses different algorithms to solve classification problems based on historical data. Using machine learning, these models can predict the likelihood of a crime provided that the required dataset is available as explained in Mahmud et al. (2021). The crime data used to develop the model was collected from various sources including law enforcement organizations within Nairobi County and various websites sources. It consisted of fifteen (15) predictors (columns) and two thousand and fifty-nine (2059) rows/instances. This data was preprocessed into a suitable form to improve the classification of various types of crime. Various machine learning algorithms were applied to it to determine their performance and effectiveness in predicting different types of crime. Law enforcement agencies are faced with large volumes of data generated every day about a crime that require machine learning and visualization tools to analyze and depict their occurrence locations. By preprocessing this data into a suitable form, law enforcement agencies can use machine learning models with the best performance to get correct predictions of crime categories and their occurrence locations as explained in Llaha (2020). However, as demonstrated in (Sarker, 2021), the success and efficiency of a machine-learning solution depend on the accuracy and performance of the learning algorithm Thus, it is through this background, that a machine learning model was developed that centered on predicting crime categories and visualizing their occurrence locations using contextual features present in the datasets. The main objective of this research was to find an effective model for crime prediction by comparing the accuracies of the various classification algorithms to select one with the best performance on the test dataset. From the research findings, the random forest algorithm was selected as the best algorithm with a classification accuracy of 97% or 0.973301. The visualization of crime was done and presented using interactive plots such as bar graphs, line graphs, pie charts, and maps.

This paper addresses the need to combine time, space, and contextual information with machine learning to improve crime prediction and mapping. This model intends to identify the types of crime that are likely to take place in a location at a particular time. This information can be used to distinguish the types of preventive measures to be used for each type of crime. This paper is structured as follows, Section 1 is the introduction; Section 2 reviews the literature on related work in machine learning algorithms used in crime prediction; Section 3 describes the methodology and the dataset; Section 4 presents the results and discussions on the application of machine learning algorithms; and Section 5 presents the overall conclusions.

2. Related works

Numerous studies have been conducted to address crime reduction and several predictive algorithms have been suggested. These studies have used machine learning models to see how well they predict different types of crime and show where they occur. Machine learning models are predictive models that analyze recent and past data to make accurate predictions about what will happen in the future as explained by Theng and Theng (2020). According to Mohamed et al. (2022) machine learning is the scientific study of the techniques that computer systems employ to carry out a certain task effectively without utilizing several explicit instructions. They are classified into two broad categories namely supervised and unsupervised machine learning in Figure 2 below:

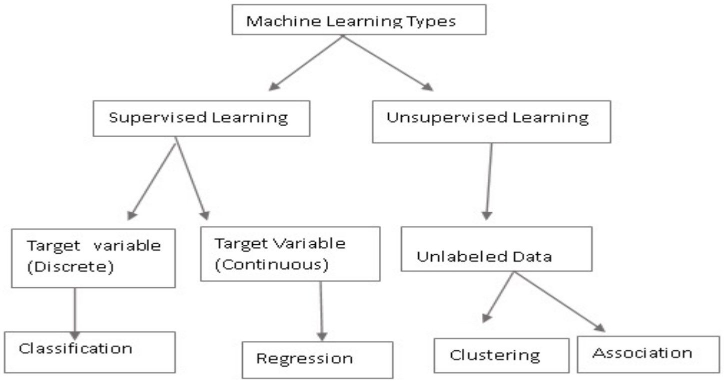


Figure 2. Types of machine learning algorithms

In unsupervised learning, the machine learning algorithms divide an inconsistent, unstructured dataset into classes or clusters while in supervised learning, the machine learning models use datasets to train, test, and get the desired results on them. To find links between attributes that could help predict the outcome, they employ classification algorithms. Regression and classification are the two sorts of tasks that supervised learning is capable of handling. While classification uses the value of a categorical target or categorical class variable to predict similar information, regression uses new, unseen input data to predict a numeric value. According to Mohamed et al. (2022) it is a beneficial strategy for any kind of statistical data. Although classification is a well-known machine learning technique, it has problems with duplicates and missing data. According to (Yoganand et al. (2020) missing values in the dataset can be problematic during both the training and classification phases. Despite the great range of supervised learning methods that are accessible, classification is the most widely used technique in predictive modeling.

According to Sen and Engelbrecht (2021), the most used classification algorithms are Decision Trees/Rules, Random Forest, K-Nearest Neighbors, Gradient-Boosted Machines, Naive Bayes, and Support Vector Machines amongst others. Several studies on crime prediction have demonstrated that it is easy to identify the location of criminal activity using classification techniques as suggested in the work of Pratibha et al. (2020). The authors presented research on the opportunities and challenges of machine learning in predicting future crime categories and visualizing their occurrence locations. They conducted an experiment using various machine learning methods such as K-Nearest Neighbors, Decision Trees, Extratress, Artificial Neural Networks, Support Vector Machine, and particular inputs to predict crimes. They used crime datasets collected from many sources to train and test models. They then evaluated the effectiveness of these models in predicting violent crimes occurring in a particular region and the results showed that the decision trees outperformed other algorithms with a classification accuracy of (88%). In their conclusions, the decision tree, K-Nearest Neighbors, and Extratress classifiers worked best with optimal training even though any model that works best is dependent on the dataset that is used.

In Llaha (2020), the author experimented with machine learning methods and evaluated their performances in analyzing datasets collected about past crimes. Experiments showed that utilizing tiny datasets, the Decision Tree performed better with a classification accuracy of (76%). He added that the decision tree seems more practical compared to other algorithms since it directly explains the principles because doing so makes them easier to understand. When deciding what proper activities to take to undertake criminal interventions, the application of machine learning in crime analysis is crucial.

In Wasim et al. (2020), the authors put forth a methodology designed to estimate the likelihood of crime occurring in a city by examining the data that is already available and visualizing the results on a Google map for easier understanding. By utilizing a clustering algorithm called K-means, which divides similar objects into clusters, the model was able to forecast the majority of locations where the offence will take place based on the findings of the data. However, the model’s reliance on K-means prevented it from handling noisy data and outliers, making it unsuitable for finding clusters with non-convex forms. In Tahir et al. (2021), the authors developed a predictive model using the Naive Bayes algorithm and a dataset of criminal offenses to analyze and predict crimes in India and the experiment results showed that the naive bayes algorithm performed better at predicting distinct types of crimes and their occurrences at different times and places, but they were not suitable for large datasets. In other studies, the random forest algorithm has demonstrated a better performance in mapping geographic data compared to other conventional methods. For example, the study by Nguyen et al. (2018) used random forest (RF) to map the Land use/Land cover (LULC) of Dak Lak province. The authors used data obtained from the Landsat 8 Operational Land Imager (OLI) to generate maps depicting Land use/Land cover.

From the findings of the related research, we can conclude that the prediction accuracy of machine learning algorithms depends upon the quality of data used and the type of attributes selected for prediction. It was also noted that a common issue in machine learning is learning to appropriately classify datasets. Machine learning algorithms are used to extract and predict specific properties from a dataset to aid in crime mitigation, as demonstrated by Saraiva et al. (2022). The recent popularity of criminology of place combined with machine learning has enabled the policing paradigms to shift from reaction to prevention.

3. Methodology

The machine learning workflow illustrated in Figure 5 was used as a methodology to develop the model. Machine learning techniques can be applied to data to extract information that can help in making better decisions regarding crime patterns and their occurrence locations. This research aimed at developing and testing machine learning models that predict types of crime and their occurrence locations. Nine (9) experiments were done according to the machine learning workflow illustrated below. Nine (9) datasets of different instances of 200, 400, 600, 900, 1000,1200, 1800, 2000, and 2059 were used to conduct the experiments where each of the five (5) machine learning models was applied to each dataset and their performance accuracy was computed and recorded. Python Jupiter Notebook Integrated Development Environment (IDE) was used to develop and run the models. The algorithms built were Decision Tree (DT), Random Forest (RF), Naive Bayes (NB), KNeighbors (KNN), and Support Vector Machines (SVM).

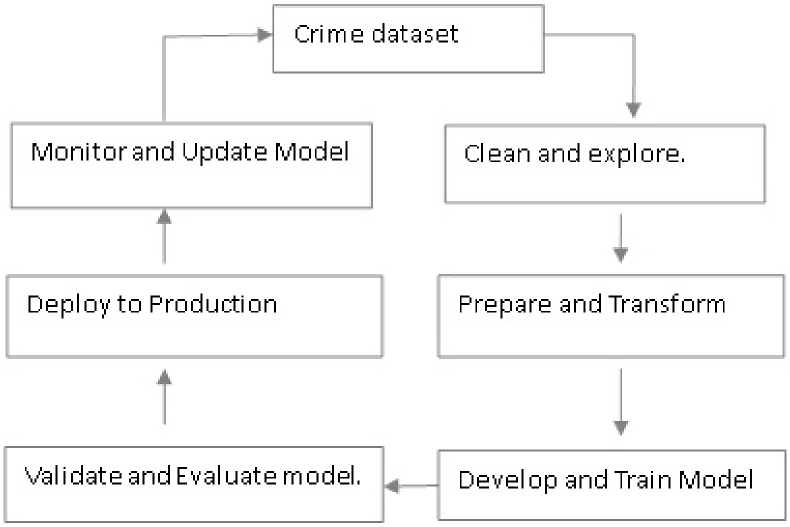


Figure 5. Machine learning workflow

The data flow diagram in Figure 6 represents various aspects of the models' processes by considering the input, the process conducted, and the output.

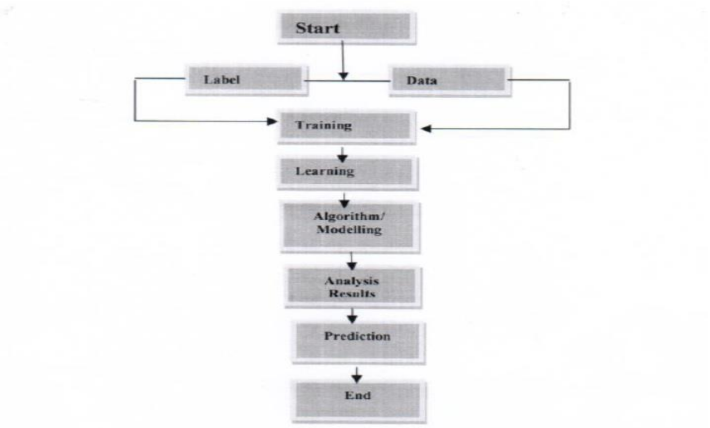


Figure 6. Flowchart diagram of the classification and prediction

3.1 *Crime datasets*

The model was developed using crime data collected from various sources including law enforcement organizations within Nairobi County and various websites sources through web scraping and stored in a CSV file on the computer's hard disk. It consisted of crime information such as 'Incident_Number', 'Incident', 'Crime_Decsription', 'Crime_code', 'Crimetype', 'Arrest',' Age', 'Gender', 'Date', 'Year', 'Month', 'Location', 'Location_code', 'Lat' and 'Long' as shown in Table 1. This dataset was a subset of a much larger dataset with feature vectors that have a higher degree of correlation for predicting crime.

Table 1. Crime dataset

Field Name	Description
Incident_Number	Identifier
Incident	Reports of crime
Crime_Decsription	Offense description
Crime_code	Offense description code
Crimetype	Class of the crime
Arrest	Whether the suspect was apprehended or not
Age	Age of the offender
Gender	Whether male or female
Date	Occurrence date
Year	Year of offense occurrence
Month	The month of offense occurrence
Location	Areas where crime incidents happened
Location_code	Code of the crime occurrence location
Lat	Latitude of the location
Long	Longitude of the location

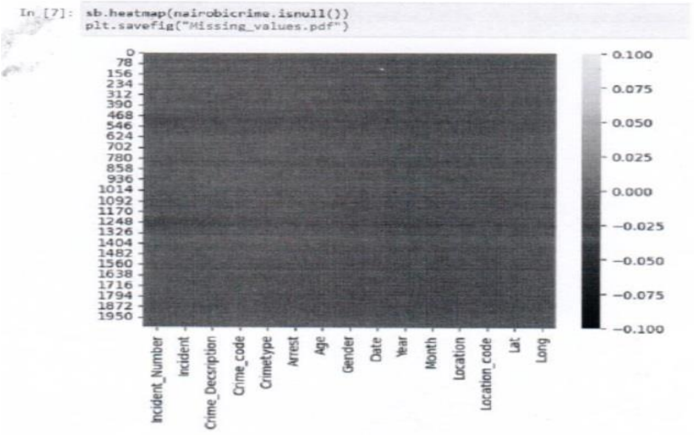
The dataset consisted of fifteen (15) predictors (columns) and two thousand and fifty-nine (2059) rows/instances that were read and viewed in Python (Jupiter Notebook IDE) using the Pandas functions 'PD.read_csv()'. The data provided the necessary information about crime in Nairobi County which assisted in identifying types of crime and their occurrence locations.

3.2 *Data preprocessing*

Data cleaning is the process of adding missing values, reducing noise, identifying outliers, and fixing errors in the dataset before the machine learning approach is applied to it. Data preparation is the act of transforming raw data into an appropriate form. The dataset was cleaned and unnecessary data was removed using the following techniques.

3.2.1 *Interpolation of missing values*

The missing values were replaced through interpolation. This was achieved using the seaborn function 'sb. heatmap (df, IsNull())' that checked for any missing values in the DataFrame as shown in Figure 7.

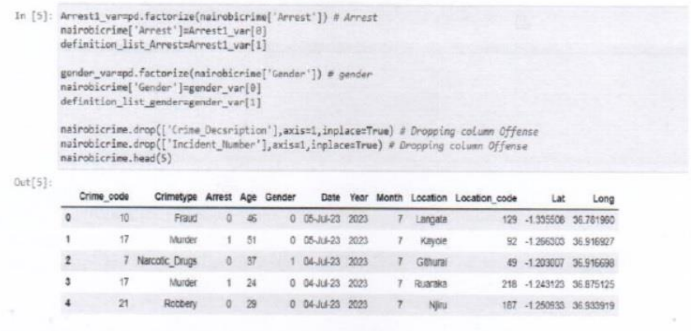


```
In [7]: sb.heatmap(nairobicrime.isnull())
        plt.savefig("Missing_values.pdf")
```

Figure 7. Heatmap for missing values

3.2.2 *Dropping of missing values and unnecessary columns.*

The necessary columns were retrieved from the data frame by dropping rows that had missing/null values using functions ‘df.dropnat ()’ and ‘df.drop([‘column’],axis=1)’ as shown in Figure 8.



```
In [5]: Arrest1_var=pd.factorize(nairobicrime['Arrest']) # Arrest
        nairobicrime['Arrest']=Arrest1_var[0]
        definition_list_Arrest=Arrest1_var[1]

        gender_var=pd.factorize(nairobicrime['Gender']) # gender
        nairobicrime['Gender']=gender_var[0]
        definition_list_gender=gender_var[1]

        nairobicrime.drop(['Crime_Decsription'],axis=1,inplace=True) # Dropping column Offense
        nairobicrime.drop(['Incident_Number'],axis=1,inplace=True) # Dropping column Offense
        nairobicrime.head(5)
Out[5]:
   Crime_code      Crimetype  Arrest  Age  Gender       Date  Year  Month  Location  Location_code        Lat       Long
0          10          Fraud       0   46       0  05-Jul-23  2023      7   Langata            129  -1.335506  36.781960
1          17         Murder       1   51       0  05-Jul-23  2023      7    Kayole             92  -1.266303  36.916927
2           7  Narcotic_Drugs      0   37       1  04-Jul-23  2023      7  Githurai             49  -1.203007  36.916698
3          17         Murder       1   24       0  04-Jul-23  2023      7   Ruaraka            218  -1.243123  36.875125
4          21        Robbery       0   29       0  04-Jul-23  2023      7     Njiru            187  -1.250933  36.933919
```

Figure 8. Sample dataset with the dropped column

3.2.3 *Converting categorical data into numerical values.*

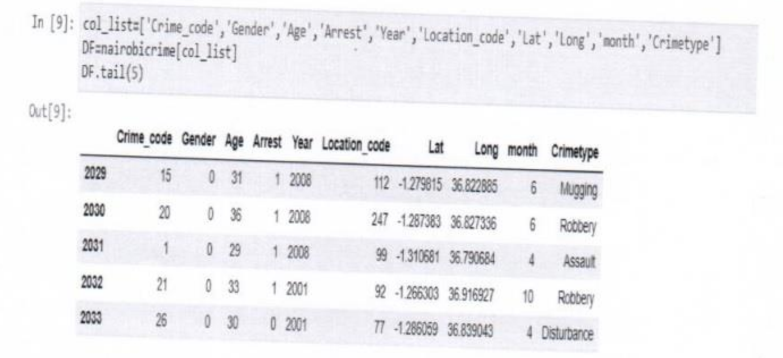
This is a process of transforming data by mapping values to concept labels. The Label Encoder was used to convert the categorical columns into numerical values to extract valuable information from the dataset as shown in Figure 8 above.

3.2.4 *Converting the date column to the month*

The date column was converted to month (number) and month name using the function ‘pd.to_datetime()’.

3.3 *Classification*

The classification was done by categorizing the dataset into two classes namely independent features (X) and dependent features (y). Dependent feature (y) is often referred to as target, label, or category, the column ‘Crimetype’ was used to hold dependable features as shown in Figure 9.



```
In [9]: col_list=['Crime_code','Gender','Age','Arrest','Year','Location_code','Lat','Long','month','Crimetype']
        DF=nairobicrime[col_list]
        DF.tail(5)
Out[9]:
      Crime_code  Gender  Age  Arrest  Year  Location_code        Lat       Long  month   Crimetype
2029          15       0   31       1  2008            112  -1.279815  36.822885      6     Mugging
2030          20       0   36       1  2008            247  -1.287383  36.827336      6     Robbery
2031           1       0   29       1  2008             99  -1.310681  36.790684      4     Assault
2032          21       0   33       1  2001             92  -1.266303  36.916927     10     Robbery
2033          26       0   30       0  2001             77  -1.286059  36.839043      4  Disturbance
```

Figure 9. Sample of the cleansed dataset

The classification of data was done to distinguish the types of crime and the prevention measures to be used in each crime occurrence because different crimes require different treatment.

3.3.1 *Visualizing target variable*

The seaborn function "sns.countplot(DF['Crimetype'])" was used to plot the graph to visualize the target/class variables used for classification and prediction tasks as shown in Figure 10 below.

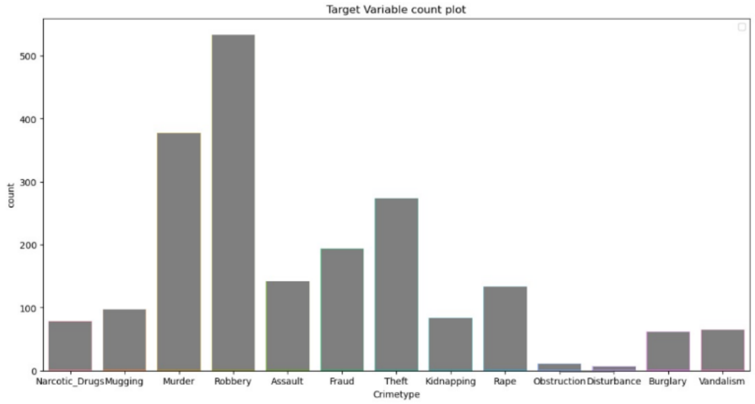
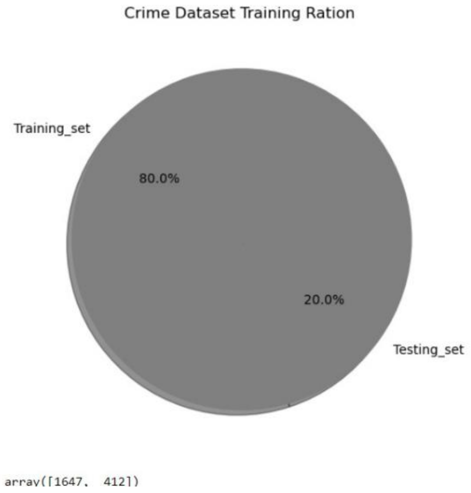


Figure 10. Target variable count

3.3.2 *Splitting the dataset into the training and test sets*

The dataset was split into training sets, and test sets using 'train_test_split()' function. The split was done in the ratio of eighty percent (80%) for training and twenty percent (20%) for testing. As a result, the train size was one thousand six hundred and forty-seven (1647) data points while the test size was four hundred and twelve (412) data points as shown in Figure 11. The training was done to teach (train) the algorithm to perform classification and prediction tasks while the validation was done to test the generalization ability of the model on the unseen dataset.



```
array([1647, 412])
```

Figure 11. Training and test set

3.4 *Model building and training*

Various algorithms were imported from sklearn library to build the models using the training data. The algorithms built were Decision Tree (DT), Random Forest (RF), Naive Bayes (NB), KNeighbors (KNN), and Support Vector Machines (SVM).

3.4.1 *Decision trees*

After dividing the dataset into random training and test sets, the Decision Tree was constructed to forecast the target column. The dataset was divided using the splitting criterion "Entropy." This classifier was built by importing the 'DecisionTreeClassifier' from the 'sklearn.tree' library and fitted to the training set using the function 'dt_clf.fit(X_train,y_train)'. The validation was done by predicting the test set results.

3.4.2 *Random Forest*

With the Random Forest ensemble learning method, many learners are combined to improve the performance of the machine learning model. Decision Trees' propensity to overfit the training dataset is rectified by Random Forest classifiers. It builds several trees throughout training period and produces mean and mode predictions for classification and regression, respectively. The classifier selects the majority judgement of the trees as the final choice. This classifier was built by importing the 'RandomForestClassifier' from the 'sklearn. Ensemble' library and fitted to the training set using the function 'rf_clf.fit(X_train,y_train)'. The validation was done by predicting the test set results.

3.4.3 *Naïve Bayes*

This classification technique makes the premise that predictors are independent based on the Bayes Theorem. It makes the assumption that a feature's inclusion in a class has nothing to do with the inclusion of any other features. This classifier was built by importing the 'GaussianNB' from the 'sklearn.naive_bayes' library and fitted to the training set using the function 'nb_clf.fit(X_train,y_train)'. The validation was done by predicting the test set results.

3.4.4 *K-Nearest Neighbors*

This algorithm classifies a data point according to the categorization of its neighbours. A similarity metric is used to categorise new cases and store all of the existing cases. K-Nearest Neighbors is a parameter that specifies how many of the closest neighbours should be considered when casting a majority vote. In K-Nearest Neighbors, the best accuracy was achieved by selecting the right value of K, that is 3 or 5, or 7. This classifier was built by importing the 'KNeighborsClassifier' from the 'sklearn.neighbors' library and fitted to the training set using the function 'knn_clf.fit(X_train,y_train)'. The validation was done by predicting the test set results.

3.4.5 *Support Vector Machine*

The Support Vector Machine algorithms locate a hyperplane that clearly categorises the data points in an N-dimensional space (where N is the number of characteristics). However, the SVM's drawback is that non-linearly separable data cannot be used with it. This classifier was built by importing the 'SVC' from 'sklearn.svm' library and fitted to the training set using the function 'sv_clf.fit(X_train,y_train)'. The validation was done by predicting the test set results.

3.5 *Prediction*

The prediction was carried out using 'model.predict(xtest)' function. The accuracy was calculated using accuracy_score imported from metrics – metrics.accuracy_score (ytest, predicted).

3.5.1 *Model evaluation*

The test set was used to evaluate and select the best model for crime prediction. The confusion matrix was deployed to check the performance of each model. A confusion matrix is an N x N matrix used for evaluating the performance of a classification model, where N is the number of target classes. It summarized the number of correct and incorrect predictions yielded by models. The accuracy of the models was determined by looking at the diagonal values for counting the number of accurate classifications. This was obtained by summing all the total numbers in the diagonal and then dividing it by the total number of all observations. For instance, according to the heatmap, the random forest's classification accuracy was determined to be (97%) or 0.973301 as shown in Figure 12.

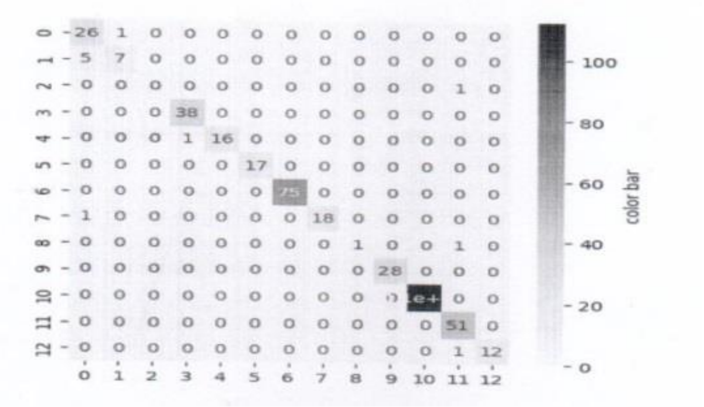


Figure 12. Random Forest (RF) model accuracy heatmap

3.5.2 *Data visualization tools*

The matplotlib, seaborn, and folium libraries were utilized to build the data visualization that presented data points in graphs, pie charts, and maps as shown in section 4.

3.6 *Ethical considerations*

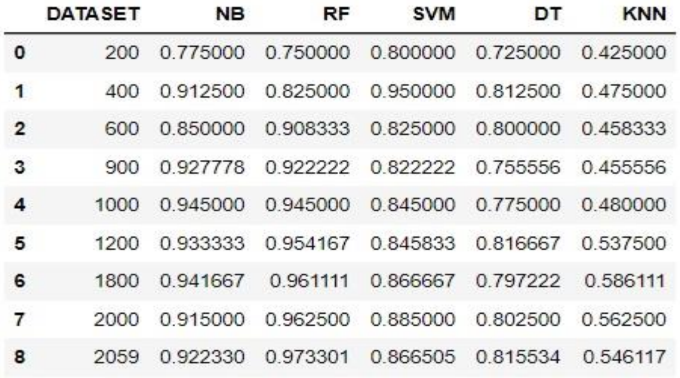
Given the sensitivity of the subject of crime, this research adhered to ethical principles of secrecy, anonymity, informed consent, and data protection. In all phases of the research procedure, including the voluntary nature of involvement, the freedom to withdraw at any time, and the measures used to preserve and anonymize data, ethical permission was obtained.

4. Results and discussions

This section presents implementation results and comparative analysis of Decision Tree (DT), Random Forest (RF), Naïve Bayes (NB), KNeighbors (KNN), and Support Vector Machine (SVM) on the crime dataset described in the previous sections.

4.1 *Comparative analysis of the machine learning algorithms*

The developed algorithms included Decision Tree (DT), Random Forest (RF), Naïve Bayes (NB), KNeighbors (KNN), and Support Vector Machines (SVM) were tested for performance accuracy using a confusion matrix. The preliminary experiments were conducted on nine (9) datasets of different instances such as 200, 400, 600, 900, 1000,1200, 1800, 2000, and 2059. Each of the five (5) machine learning models was applied to each dataset and their performance accuracy was computed and recorded as shown in Figure 13 below.



	DATASET	NB	RF	SVM	DT	KNN
0	200	0.775000	0.750000	0.800000	0.725000	0.425000
1	400	0.912500	0.825000	0.950000	0.812500	0.475000
2	600	0.850000	0.908333	0.825000	0.800000	0.458333
3	900	0.927778	0.922222	0.822222	0.755556	0.455556
4	1000	0.945000	0.945000	0.845000	0.775000	0.480000
5	1200	0.933333	0.954167	0.845833	0.816667	0.537500
6	1800	0.941667	0.961111	0.866667	0.797222	0.586111
7	2000	0.915000	0.962500	0.885000	0.802500	0.562500
8	2059	0.922330	0.973301	0.866505	0.815534	0.546117

Figure 13. The models' performance accuracy

The validation was done by predicting the test set and examining the accuracy score on the existing dataset with two thousand and fifty-nine (2059) rows/instances. The confusion matrix checked and visualized the performance of each model through the heat map as shown in Figure 3.8 above. The performance of individual machine learning algorithms was analyzed and presented as shown in Table 2.

Table 2. Algorithms' performance comparison

S/No.	Model	accuracy	Score (%)	Limitations
1	Random Forest (RF)	0.973301	97%	It makes predictions with high accuracy for huge datasets, but if there are too many trees, the algorithm may be too sluggish and inefficient to generate predictions in real time. Even when a significant amount of data is absent, accuracy can still be maintained. It requires less time to train than other models.
2	Naïve Bayes (NB)	0.922330	92%	The Naïve Bayes model will give it zero probability and won't be able to make any predictions if your test data set contains a categorical variable of a category that wasn't present in the training data set. It can, however, outperform other models and needs considerably less training data if its premise about the independence of characteristics is correct. It works better with category input variables than it does with numerical ones.
3	Support Vector Machine (SVM)	0.866505	87%	It has low performance on a large dataset. However, It doesn't perform well when classes are not distinct.It can handle large feature sets efficiently
4	Decision Tree (DT)	0.815534	82%	They are unstable; a minor alteration in the data can result in a significant alteration in the structure thereby affecting its performance. - it causes instability if there is any change in the data.Not suitable for large datasets
5	K-Nearest Neighbors (KNN)	0.546117	55%	Data-filling algorithms need to be added to increase accuracy for example adjusting the value of K. It doesn't work well with large datas ets. It doesn't handle categorical features very well

The accuracy of each model was calculated using the function accuracy_score by importing metrics.accuracy_score (y_test, predicted) from sklearn's metrics function and presented the scores using a multiple-line graph as shown in Figure 14 below.

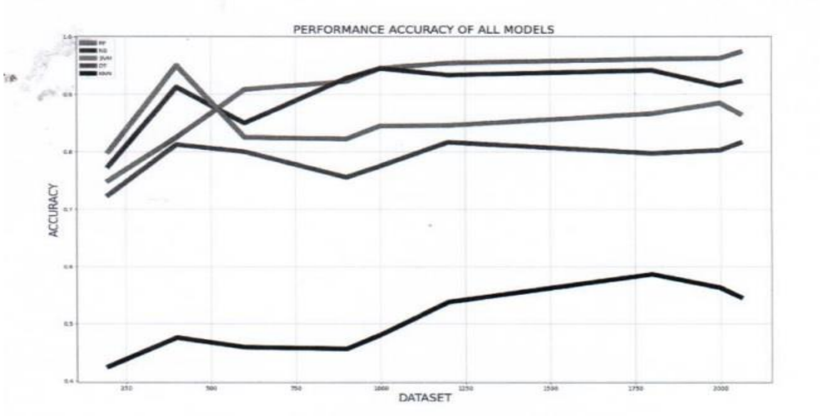


Figure 14. Algorithms performance using a line graph

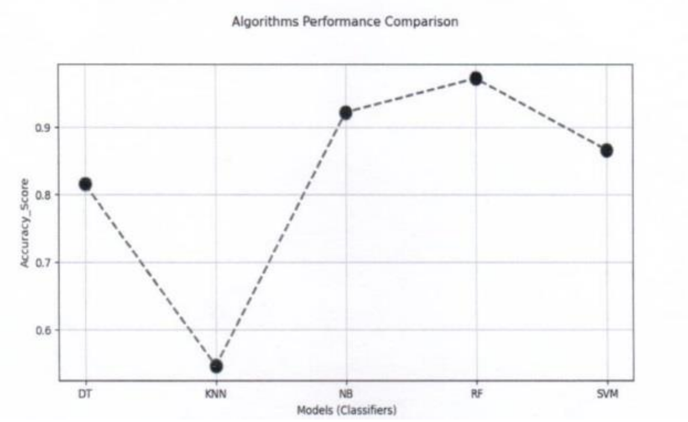
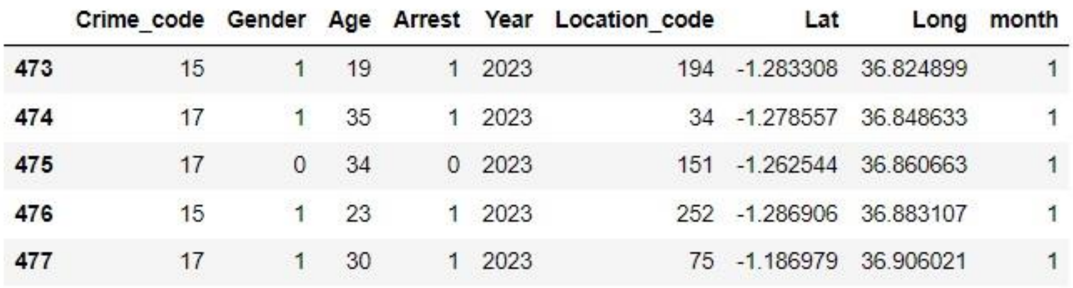


Figure 15. Algorithms performance comparison

4.2 *Model deployment*

Model deployment is the action of implementing machine learning models. The model was applied to an existing dataset of four hundred and seventy-eight (478) instances and nine (9) columns collected from January 2023 to July 2023 as shown in Figure 16 and evaluated under increasing production conditions by iteratively running the tasks.

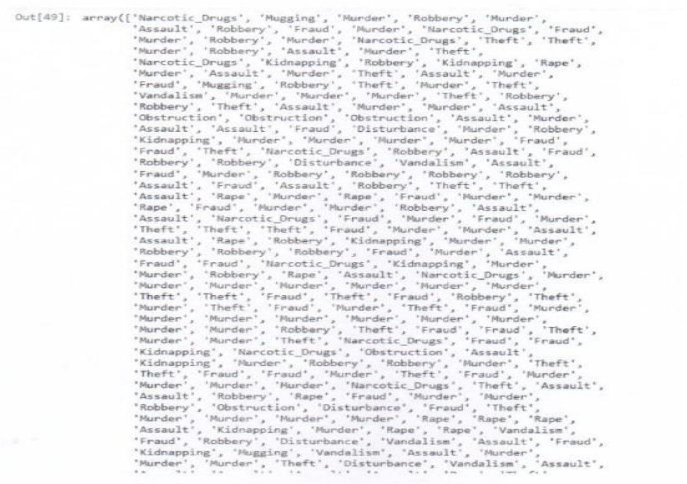


	Crime_code	Gender	Age	Arrest	Year	Location_code	Lat	Long	month
473	15	1	19	1	2023	194	-1.283308	36.824899	1
474	17	1	35	1	2023	34	-1.278557	36.848633	1
475	17	0	34	0	2023	151	-1.262544	36.860663	1
476	15	1	23	1	2023	252	-1.286906	36.883107	1
477	17	1	30	1	2023	75	-1.186979	36.906021	1

Figure 16. Existing dataset between January 2023 to July 2023

4.2.1 *Crime prediction*

The prediction was done by feeding the following attributes, 'Crime_code', 'Gender', 'Age', 'Arrest', 'Year', 'Location_code', 'Lat', 'Long' and 'Month' into the model to predict and fetch different categories of crime as shown in Figure 17. The 'model. predict(xtest)' function was used to carry out the prediction tasks.

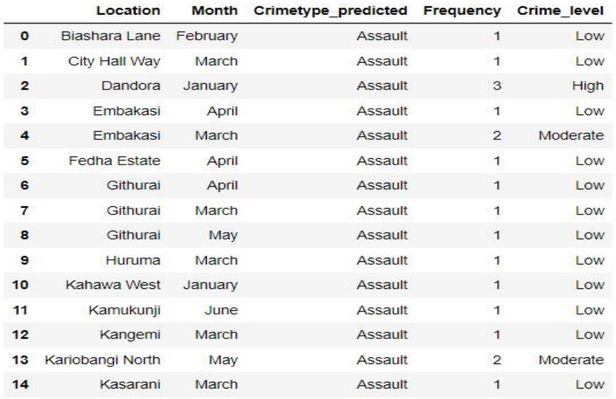


```
Out[49]: array(['Narcotic_Drugs', 'Mugging', 'Murder', 'Robbery', 'Murder',
                'Assault', 'Robbery', 'Fraud', 'Murder', 'Narcotic_Drugs', 'Fraud',
                'Murder', 'Robbery', 'Murder', 'Narcotic_Drugs', 'Theft', 'Theft',
                'Murder', 'Robbery', 'Assault', 'Murder', 'Theft',
                'Narcotic_Drugs', 'Kidnapping', 'Robbery', 'Kidnapping', 'Rape',
                'Murder', 'Assault', 'Murder', 'Theft', 'Assault', 'Murder',
                'Fraud', 'Mugging', 'Robbery', 'Theft', 'Murder', 'Theft',
                'Vandalism', 'Murder', 'Murder', 'Murder', 'Theft', 'Robbery',
                'Robbery', 'Theft', 'Assault', 'Murder', 'Murder', 'Assault',
                'Obstruction', 'Obstruction', 'Obstruction', 'Assault', 'Murder',
                'Assault', 'Assault', 'Fraud', 'Disturbance', 'Murder', 'Robbery',
                'Kidnapping', 'Murder', 'Murder', 'Murder', 'Murder', 'Fraud',
                'Fraud', 'Theft', 'Narcotic_Drugs', 'Robbery', 'Assault', 'Fraud',
                'Robbery', 'Robbery', 'Disturbance', 'Vandalism', 'Assault',
                'Fraud', 'Murder', 'Robbery', 'Robbery', 'Robbery', 'Robbery',
                'Assault', 'Fraud', 'Assault', 'Robbery', 'Theft', 'Theft',
                'Assault', 'Rape', 'Murder', 'Rape', 'Fraud', 'Murder', 'Murder',
                'Rape', 'Fraud', 'Murder', 'Murder', 'Robbery', 'Assault',
                'Assault', 'Narcotic_Drugs', 'Fraud', 'Murder', 'Fraud', 'Murder',
                'Theft', 'Theft', 'Theft', 'Fraud', 'Murder', 'Murder', 'Assault',
                'Assault', 'Rape', 'Robbery', 'Kidnapping', 'Murder', 'Murder',
                'Robbery', 'Robbery', 'Robbery', 'Fraud', 'Murder', 'Assault',
                'Fraud', 'Fraud', 'Narcotic_Drugs', 'Kidnapping', 'Murder',
                'Murder', 'Robbery', 'Rape', 'Assault', 'Narcotic_Drugs', 'Murder',
                'Murder', 'Murder', 'Murder', 'Murder', 'Murder', 'Murder',
                'Theft', 'Theft', 'Fraud', 'Theft', 'Fraud', 'Robbery', 'Theft',
                'Murder', 'Theft', 'Fraud', 'Murder', 'Theft', 'Fraud', 'Murder',
                'Murder', 'Murder', 'Murder', 'Murder', 'Murder', 'Murder',
                'Murder', 'Murder', 'Robbery', 'Theft', 'Fraud', 'Fraud', 'Theft',
                'Murder', 'Murder', 'Theft', 'Narcotic_Drugs', 'Fraud', 'Fraud',
                'Kidnapping', 'Narcotic_Drugs', 'Obstruction', 'Assault',
                'Kidnapping', 'Murder', 'Robbery', 'Robbery', 'Murder', 'Theft',
                'Theft', 'Fraud', 'Fraud', 'Murder', 'Theft', 'Fraud', 'Murder',
                'Murder', 'Murder', 'Murder', 'Narcotic_Drugs', 'Theft', 'Assault',
                'Assault', 'Robbery', 'Rape', 'Fraud', 'Murder', 'Murder',
                'Robbery', 'Obstruction', 'Disturbance', 'Fraud', 'Theft',
                'Murder', 'Murder', 'Murder', 'Murder', 'Rape', 'Rape', 'Rape',
                'Assault', 'Kidnapping', 'Murder', 'Rape', 'Rape', 'Vandalism',
                'Fraud', 'Robbery', 'Disturbance', 'Vandalism', 'Assault', 'Fraud',
                'Kidnapping', 'Mugging', 'Vandalism', 'Assault', 'Murder',
                'Murder', 'Murder', 'Theft', 'Disturbance', 'Vandalism', 'Assault',
```

Figure 17. Predicted types of crime

4.2.2 *Observed values vs. predicted values*

The observed values are the actual values that are obtained by observation while the predicted values are the values of the variable predicted based on the classification. The predicted values are contained in the column named "Crimetype_predicted" as shown in Figure 18.



	Location	Month	Crimetype_predicted	Frequency	Crime_level
0	Biashara Lane	February	Assault	1	Low
1	City Hall Way	March	Assault	1	Low
2	Dandora	January	Assault	3	High
3	Embakasi	April	Assault	1	Low
4	Embakasi	March	Assault	2	Moderate
5	Fedha Estate	April	Assault	1	Low
6	Githurai	April	Assault	1	Low
7	Githurai	March	Assault	1	Low
8	Githurai	May	Assault	1	Low
9	Huruma	March	Assault	1	Low
10	Kahawa West	January	Assault	1	Low
11	Kamukunji	June	Assault	1	Low
12	Kangemi	March	Assault	1	Low
13	Kariobangi North	May	Assault	2	Moderate
14	Kasarani	March	Assault	1	Low

Figure 18. Observed values vs predicted values

4.3 *Data visualization*

The crime dataset was analyzed using data visualization tools mentioned in the previous section to examine the relationships between attributes that would make it possible to predict crime occurrences. Different categories of crime were depicted using markers of different colors in a heat map. The data analysis was done using matplotlib, seaborn, and folium functions, and the results were presented as follow:

- Types of crime indicators;
- Types of crime committed over time between January 2023 to July 2023;
- Trends in crime in Nairobi County;
- Crimes that are committed across different locations;
- The pattern of crime occurrences by locations.

4.3.1 *Types of crime indicators*

Table 3 shows the overall number of crimes predicted based on new cases reported between January 2023 and July 2023. Murder, Robbery, Theft, Fraud, and assault recorded a high number of cases that occurred within various locations within Nairobi County.

Table 3. Predicted crime indicators

Crimetype	Total_Occurence	Percentage
Murder	83	20.6
Robbery	75	18.61
Theft	56	13.9
Assault	54	13.4
Fraud	49	12.16
Rape	19	4.71
Narcotic_Drugs	17	4.22
Vandalism	16	3.97
Kidnapping	10	2.48
Obstruction	8	1.99
Mugging	7	1.74
Disturbance	5	1.24
Burglary	4	0.99

According to Figure 19 below, Murder led with 20.6 % of all predicted crimes, followed by Robbery at 18.61%, Theft at 13.09 %, Assault at 13.4%, Fraud at 12.16%, and the rest of the crimes were predicted to occur below 5%.

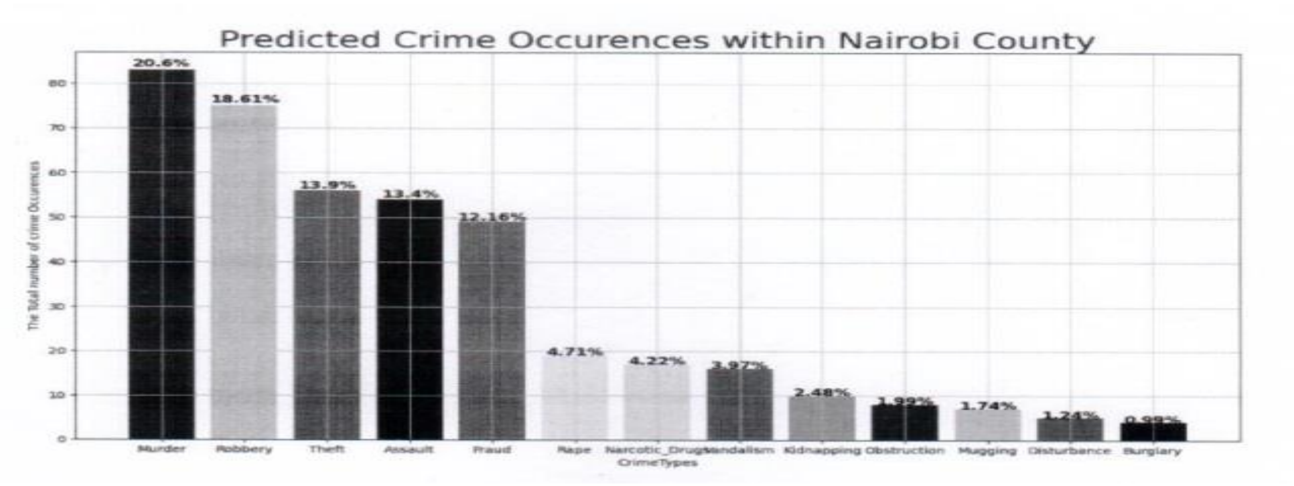


Figure 19. Total number of crime cases predicted

4.3.2 *Types of crime committed over time between January 2023 to July 2023*

According to Table 4 and Figure 20 below, the month of April 2023 recorded a high number of crime cases at (88) accounting for 21.84% of all crime cases that were likely to occur between January 2023 and July 2023. It was followed by March with (86) cases accounting for 21.34% of the total crime cases predicted. The month of February had (59) cases at 14.64%, May had (58) cases at 14.39%, January had (54) at 13.4%, June had (41) at 10.17% and July had (17) at 4.22%.

Table 4. Predicted crime occurrences by time

Month	Total	Percentage
January	54	13.4
February	59	14.64
March	86	21.34
April	88	21.84
May	58	14.39
June	41	10.17
July	17	4.22

The other coming months were projected to record less than 15% likelihood of crime occurring.

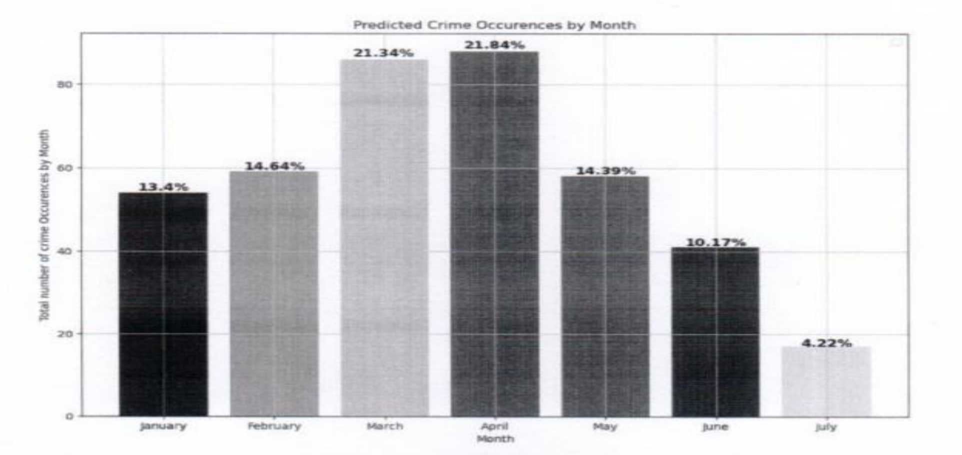


Figure 20. Predicted crime over time

4.3.3 *Trends in crime in Nairobi County*

There was an upward trend from January through to April 2023, this was probably due to the erratic nature of crime then reduced from April 2023 to July 2023 as shown in Figure 21 below. The reduction was probably based on measures the government put in place to mitigate crime from the month of April 2023. If such trends continue, then during the following months after July 2023, many residents of Nairobi County are likely to experience fewer criminal activities.

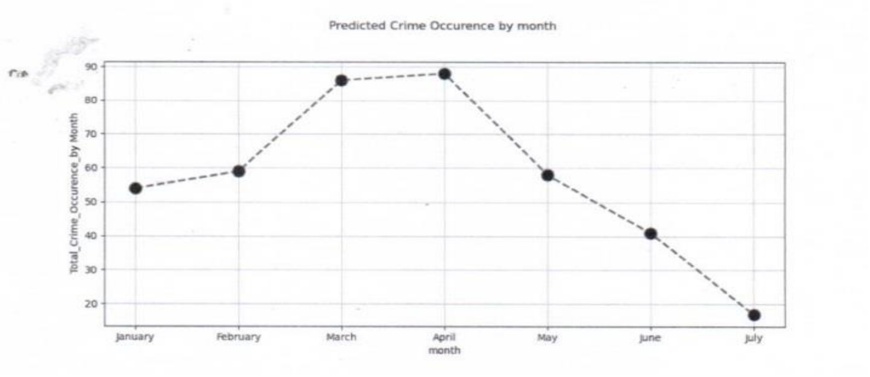
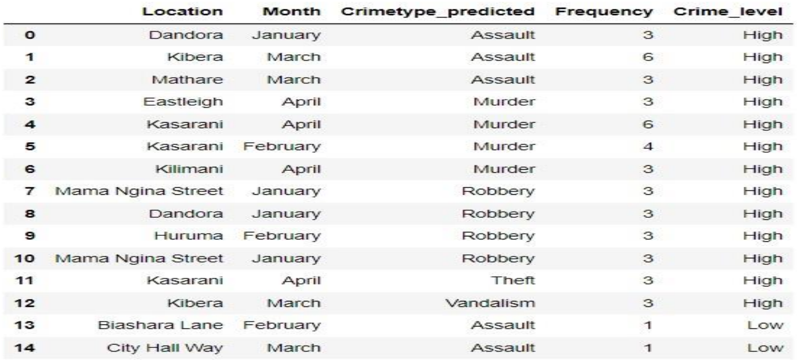


Figure 21. The trend in crime every month

4.3.4 *Crimes committed across different locations.*

Figure 22 below indicates the crime levels based on place, time, and nature of the crime. The level of crimes such as Assault, Robbery, Murder, Theft, and Vandalism were high in Dandora, Kibera, Mathare, Eastleigh, Kasarani, Kilimani, Huruma, and Mama Ngina Street, between the months of January 2023 and April 2023.



	Location	Month	Crimetype_predicted	Frequency	Crime_level
0	Dandora	January	Assault	3	High
1	Kibera	March	Assault	6	High
2	Mathare	March	Assault	3	High
3	Eastleigh	April	Murder	3	High
4	Kasarani	April	Murder	6	High
5	Kasarani	February	Murder	4	High
6	Kilimani	April	Murder	3	High
7	Mama Ngina Street	January	Robbery	3	High
8	Dandora	January	Robbery	3	High
9	Huruma	February	Robbery	3	High
10	Mama Ngina Street	January	Robbery	3	High
11	Kasarani	April	Theft	3	High
12	Kibera	March	Vandalism	3	High
13	Biashara Lane	February	Assault	1	Low
14	City Hall Way	March	Assault	1	Low

Figure 22. Crime levels

From the research findings, areas with high crime levels as shown in Figure 23 require constant Police intervention such as heightened patrols, police crackdowns, neighborhood watch, and community policing to reduce the level of crime to low or moderate.

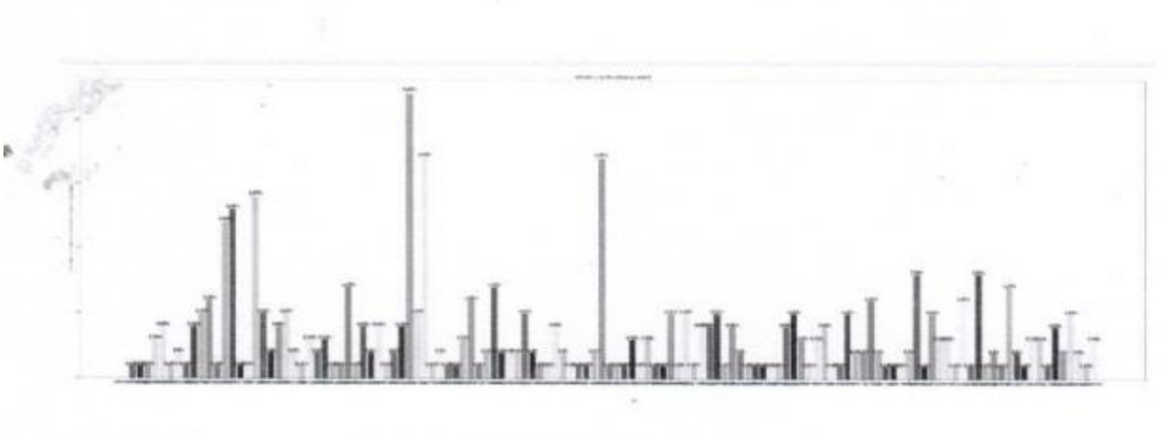
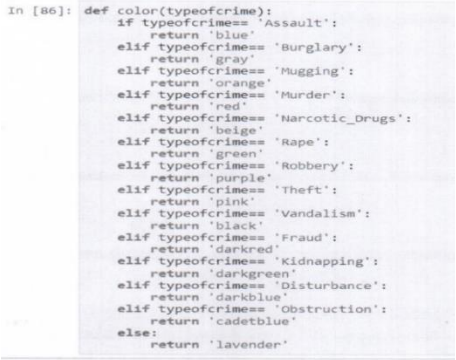


Figure 23. Areas with high crime levels

4.3.5 *The pattern of crime occurrences by locations*

A crime pattern is a considerable change in crime occurrences within a given geographical area over time. Crime cases reported between January 2023 and July 2023 were linked with information to a map to present the pattern of crime occurrences. This was done to aid in tracking crime from location to location and recognizing the patterns in them in real time. Markers of different colors were used to represent different types of crime on a map. The markers colors that were added to the map included 'red', 'blue', 'green', 'purple', 'orange', 'dark red',' light red, 'beige', 'dark blue', dark green', 'cadet blue', dark purple', 'white', 'pink', 'light blue', 'light green', 'gray', 'black', 'light gray', as shown in Figure 24 below.



```
In [86]: def color(typeofcrime):
             if typeofcrime== 'Assault':
                 return 'blue'
             elif typeofcrime== 'Burglary':
                 return 'gray'
             elif typeofcrime== 'Mugging':
                 return 'orange'
             elif typeofcrime== 'Murder':
                 return 'red'
             elif typeofcrime== 'Narcotic_Drugs':
                 return 'beige'
             elif typeofcrime== 'Rape':
                 return 'green'
             elif typeofcrime== 'Robbery':
                 return 'purple'
             elif typeofcrime== 'Theft':
                 return 'pink'
             elif typeofcrime== 'Vandalism':
                 return 'black'
             elif typeofcrime== 'Fraud':
                 return 'darkred'
             elif typeofcrime== 'Kidnapping':
                 return 'darkgreen'
             elif typeofcrime== 'Disturbance':
                 return 'darkblue'
             elif typeofcrime== 'Obstruction':
                 return 'cadetblue'
             else:
                 return 'lavender'
```

Figure 24. Marker colors for distinct types of crime

From the research findings, Figure 25 above shows different types of crime committed in different locations and the markers of different colors reveal the patterns of each crime occurrence as shown in Figure 4.12 below. For instance, a murder that occurred in one location might be a match for a murder that would probably occur in another location in the future. The areas with high crime levels provided an enabling environment for crime to thrive. This is probably because it could take a long time to arrest criminals because of the large population. This delay allowed crimes to occur without being detected.

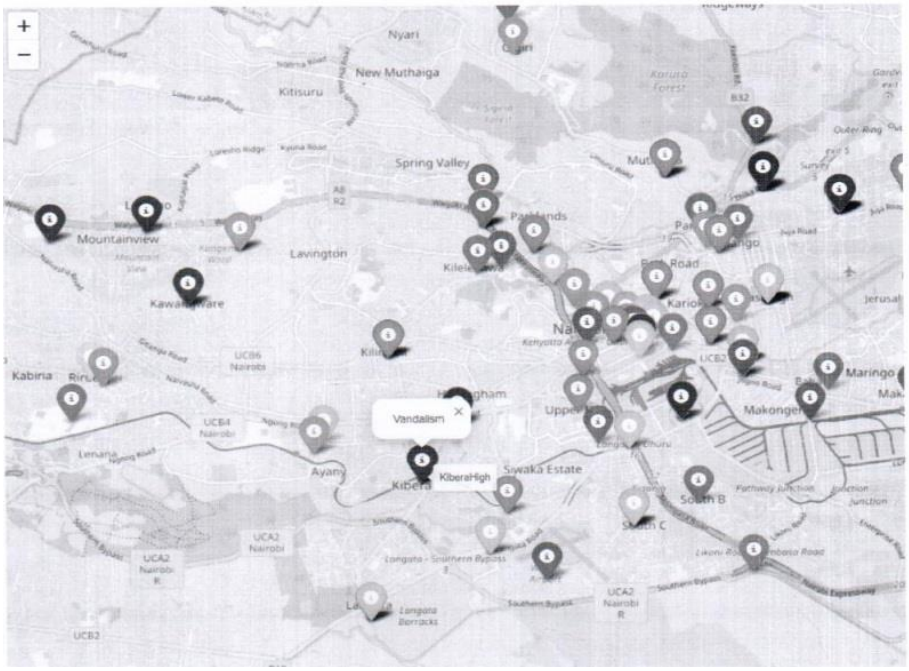


Figure 25. Pattern of crime occurrences

5. Conclusion

Crime prediction and mapping is one of the current developments in crime prevention and the goal is to lower the number of crimes that occur. This was achieved by collecting raw datasets from various sources including law enforcement organizations within Nairobi County and various websites sources through web scraping and stored in a CSV file on the computer's hard disk. The dataset was then pre-processed and transformed into a proper form for further processing. Different machine learning, naive such as Decision Tree (DT), KNeighbors (KNN), Support Vector Machine (SVM), Naïve Bayes (NB), and Random Forest (RF) were developed and evaluated using a confusion matrix, and based on the results of the experiments, the Random Forest model was found to be the best method for estimating the likelihood of a crime occurring in a specific place, with a classification accuracy of 97%. The prediction was done by feeding the following attributes, 'Incident_Number', 'Incident', 'Crime_Decsription', 'Crime_code', 'Crimetype', 'Arrest',' Age', 'Gender', 'Date', 'Year', 'Month', 'Location', 'Location_code', 'Lat' and 'Long', into the best model to predict and fetch different categories of crime. The longitude and latitude features were used to tag the specific locations of crime occurrences on a map. Markers of different colors were used to reveal the patterns of each crime occurrence. Data visualization was done to identify types of crime that might have occurred in a specific location under a variety of parameter constraints. Various interactive plots such as bar graphs, line graphs, and pie charts were created to present the data points. The experimental results from the research findings showed that every location is known with a particular crime type and hence, crime prediction and mapping intend to identify the types of crime that are likely to take place in a location at a particular time. This information can be used to distinguish the types of preventive measures to be used for each type of crime.

The future enhancement of the model is to integrate crime with an interactive user interface like a web portal so that the model can be easily accessible by anyone intending to report a crime. The web portal will enable users to report crimes by entering details of the crime in the database in real time as opposed to the current methods of manual input or recordings. The aim is to make this model a centralized system that connects all law enforcement offices across the country to report crime online. This would be quite easier to predict crimes in a location and recognize the patterns in them in real-time.

Acknowledgements

This research did not receive any specific grant from funding agencies in the public commercial, or not-for-profit sectors.

The authors declare no competing interests.

References

Dikananda, et al. (2022). Comparison of decision tree classification methods and gradient boosted trees. *TEM Journal*, *11*, 316-322 https://doi.org/10.18421/TEM111-39

Kanimozhi, et al. (2021). Crime type and occurrence prediction using machine learning algorithm. In *International Conference on Artificial Intelligence and Smart Systems (ICAIS)*. Coimbatore, India. https://doi.org/10.1109/ICAIS50930.2021.9395953

Llaha, O. (2020). Crime analysis and prediction using machine learning. In *43rd International Convention on Information, Communication and Electronic Technology (MIPRO)*. Opatija, Croatia. https://doi.org/10.23919/MIPRO48935.2020.9245120

Mohamed, et al (2022). *Supervised machine learning techniques*. https://www.researchgate.net/publication/363870735_Supervised_Machine_Learning_Techniques_A_Comparison.

Mahmud, et al. (2021). Crime rate prediction using machine learning and data mining. In S. Borah, S., Pradhan, R., Dey, & N., Gupta, P. (Eds.). Soft computing techniques and applications. *Advances in Intelligent Systems and Computing*, Vol. 1248. https://doi.org/10.1007/978-981-15-7394-1_5

National Police Service (NPS)(2022). Annual report.

Nguyen, et al. (2018). Applying Random Forest Classification to map land use/land cover using Landsat 8 oli, Int. Arch. Photogramm. Remote Sens. Spatial Inf. Sci., XLII-3/W4, pp 363-367. https://doi.org/10.5194/isprs-archives-XLII-3-W4-363-2018

Pratibha, et al. (2020). Crime prediction and analysis. *2nd International Conference on Data, Engineering and Applications (IDEA),* Bhopal, India. https://doi.org/10.1109/IDEA49133.2020.9170731

Rim, P., & Liu, E. (2020). Optimizing the C4.5 Decision Tree Algorithm using MSD-Splitting, *International Journal of Advanced Computer Science and Applications (IJACSA)*, *11*(10). http://dx.doi.org/10.14569/IJACSA.2020.0111006

Saraiva, et al. (2022). Crime prediction and monitoring in Porto, Portugal, using machine learning, spatial and text analytics. *ISPRS Int. J. Geo-Inf.* https://doi.org/10.3390/ijgi11070400

Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. *SN Comput. Sci.* 2. https://doi.org/10.1007/s42979-021-00592-x

Sen, J., & Engelbrecht, A. (2021). Machine learning – Algorithms, models and applications. *IntechOpen*. https://doi.org/10.5772/intechopen.94615

Tahir, et al. (2021). Crime prediction using Naïve Bayes Algorithm. *International Journal of Advance Research, Ideas, and Innovations in Technology*, *7*(4), V7I4-1713. www.IJARIIT.com.

Theng, M., & Theng, D. (2020). *Machine learning algorithms for predictive analytics: A review and new perspectives*. https://www.researchgate.net/profile/Dr-Theng/publication/342976767_Machine_Learning_Algorithms_for_Predictive_Analytics_A_Review_and_New_Perspectives/links/5f0ff31fa6fdcc3ed70b5f3e/Machine-Learning-Algorithms-for-Predictive-Analytics-A-Review-and-New-Perspectives.pdf.

Veena, et al. (2022). Cybercrime: Identification and prediction using machine learning techniques. *Computational Intelligence and Neuroscience*, 1-10. https://doi.org/10.1155/2022/8237421

Viet, et al. (2021). The Naïve Bayes Algorithm for learning data analytics, *Indian Journal of Computer Science and Engineering*, 12, 1038-1043. https://doi.org/10.21817/indjcse/2021/v12i4/211204191

Wasim, et al. (2020). Crime analysis and prediction using the K-Means clustering technique. *Epra International Journal of Economic and Business Review*, 05, 277-280.

Yoganand, et al. (2020). An user-friendly interface for data preprocessing and visualization using machine learning models. *International Research Journal of Engineering and Technology (IRJET)*, *7*(3), 948-951.

Zeineddine, et al. (2020). Enhancing prediction of student success: Automated machine learning approach. *Computers & Electrical Engineering*. 89.

COAS

Center for Open Access in Science ▪ https://www.centerprode.com/ojit.html
Open Journal for Information Technology, 2024, *7*(1), 43-54.
ISSN (Online) 2620-0627 ▪ https://doi.org/10.32591/coas.ojit.0701.04043m

The Role of Artificial Intelligence in Education

Elyjoy Micheni
Tom Mboya University, Homa Bay, KENYA

Jackson Machii & Julius Murumba
The Technical University of Kenya, Nairobi, KENYA
School of Business and Management Studies

Received: 23 May 2024 ▪ Revised: 20 August 2024 ▪ Accepted: 4 September 2024

Abstract

The use of artificial intelligence (AI)-powered educational tools is growing over time and has the potential to completely transform the manner that education is provided. This paper looks at the pedagogical ramifications of artificial intelligence applications utilized in educational institutions. The study is qualitative research that analyzes an array of research on artificial intelligence-powered educational technologies using articles from peer-reviewed journals and conference proceedings. Content analysis is used to examine the literature to establish, the use of artificial intelligence in education, including its capabilities in educational processes, its pedagogical implications, and its challenges. The paper discusses how artificial intelligence could transform educational settings and educational resources, creating opportunities for services to be made scalable both inside and outside of the classroom. The paper concludes that while integrating artificial intelligence (AI) into education brings benefits to the education landscape, there are also significant risks. To fully utilize AI's technological innovation for educational purposes, ethical considerations must be taken into account.

Keywords: artificial intelligence, education, pedagogy.

1. Introduction

Advances in information and communication technology have had an important influence on artificial intelligence. Crompton and Burke (2023) in their study found that applications of AI are currently utilized in several fields including governments, education, business, medicine, communication, aviation, and engineering. These technological Innovations have permeated teaching and learning, as well as other sectors of academia, fostering effectiveness and efficiency (Chen, Chen & Lin, 2020). Education now benefits from the use of artificial intelligence, which also offers new challenges in academic practices (Ouyang & Jiao, 2021; Crompton & Burke, 2023). Applications of AI in education are frequently utilized in teaching, learning, and administration. AI applications support social learning in many ways such as summarizing conversations that a teacher can use to guide students toward course goals and objectives in college courses, supporting integrated group teaching based on learning models, and facilitating participation in online communities. Artificial intelligence refers to the ability of machines, especially computer systems, to simulate human intelligence processes. It is a body of

Correspondence: Jackson Machii, The Technical University of Kenya, School of Business and Management Studies, Nairobi, KENYA.

computational techniques inspired by how humans sense, perceive, learn, and act through their nervous system and/or body. According to Chiu et al. (2023), artificial intelligence (AI) is the ability of digital machines to accomplish tasks typically carried out by intelligent beings. Artificial intelligence is associated with various technological disciplines, including computer vision, speech recognition, machine learning, big data, and natural language processing. Aldosari (2020) explains artificial intelligence as the scientific study of producing intelligent machines that behave like people. It includes the following fields: expert stems, speech recognition, neural networks, robotics, and natural language processing. AI is divided into different branches, including big data, machine learning, computer vision, speech, and natural language processing. According to Chen et al. (2020), artificial intelligence in education has been incorporated into administration, teaching, and learning. As used in this study, artificial intelligence (AI) in education refers to the application of AI technologies, such as chatbots, robots, intelligent tutoring systems, and automated assessment of all types of digital artifacts that enhance and augment education.

1.1 *Organization of this paper and its contribution*

This paper looks into studies examining artificial intelligence's applicability in educational settings and how it's affecting learning. The uses of AI in education, their pedagogical consequences, benefits, and challenges are all covered in this paper. This study advances our understanding of the educational ecosystem by examining the pedagogical effects of AI applications in the classroom and how AI is likely to develop in the future.

2. Artificial intelligence in education

Artificial intelligence (AI) has the potential to transform the educational landscape by automating administrative tasks, providing prompt feedback, and customizing teaching strategies to meet individual student needs. Furthermore, it can aid with assessment and grading, allowing educators to concentrate on designing curricula and delivering exceptional instruction. It is expected of institutions of learning to innovate in teaching and learning to keep up with new technological advancements (Aldosari, 2020). Artificial intelligence techniques, including machine learning, deep learning, artificial neural networks, natural language processing, and genetic algorithms, have enabled the development of intelligent learning environments that support behavior detection, model construction, and personalized recommendations for learning materials (Ouyang & Jiao, 2021). The principal objective of artificial intelligence is to facilitate machine information processing that approaches problem-solving as closely as possible to that of human beings. Artificial intelligence is impacting education in two primary ways, according to Aldosari (2020; Klutka, Ackerly & Magda, 2021): (1) Curriculum designed with AI in mind, which can be customized to fit the unique requirements of every learner. AI systems can create individualized learning pathways by analyzing student data, including learning preferences, skills, and shortcomings; (2) Automation of Administrative duties: By automating administrative duties, AI can free up educators' valuable time so they can concentrate on instructional activities and student engagement. Regular administrative duties like assigning grades, setting up classes, and maintaining student records can be performed by AI-powered systems: AI-generated emails can notify students of upcoming deadlines, encourage them to sign up for classes, turn in assignments on time, and pay fees on schedule. Furthermore, AI-based software is getting better at identifying plagiarized assignments. Artificial intelligence is currently being used in a variety of educational activities. A summary is presented in Table 1.

Table 1. Application of AI in the educational processes

	Technology	**Application Area**
1	Intelligent Tutoring Systems	Intelligent tutoring systems leverage artificial intelligence (AI) to deliver individualized learning experiences, making them increasingly powerful educational tools. These computer programs are made to provide students with tailored education and feedback. Through the use of AI approaches, these systems provide a learning environment that adjusts to each student's demands, resulting in a personalized educational experience.
2	Adaptive Courseware	Using artificial intelligence and machine learning techniques, adaptive learning software allows for real-time "adaptation" of a student's learning path, making learning more personalized. Furthermore, by examining the data gathered by adaptive learning software, educators and administrators can assess the needs of particular students or groups of students in a course (Klutka, Ackerly & Magda, 2021).
3	Students Grading	In artificial intelligence (AI) grading, assignments, projects, quizzes, and presentations are assessed and graded using computer algorithms and machine learning. Rule-based and data-driven algorithms are the two main types of algorithms used in AI grading. AI grading may give teachers and students rapid feedback, consistent standards, and tailored recommendations.
4	Administrative Tasks	Systems powered by artificial intelligence (AI) can execute tasks like resource and assignment distribution, attendance monitoring, and grade tabulation very quickly.
5	Global Classroom Possibility	Artificial Intelligence (AI) has the potential to dismantle classroom barriers, facilitating information sharing and worldwide learning opportunities for students (Aldosari, 2020).
6	Learning and instruction	With the aid of AI, educators can grade assignments and provide underachieving pupils with the support they require to succeed.
7	Administrative Support	Artificial intelligence (AI) tools are being used by colleges and universities to power a variety of administrative processes, including scheduling, budgeting, maintenance, information technology (IT), transportation, and student record systems. Additionally, statistics on recruitment, admission, and retention efforts are interpreted using these techniques to determine whether or not there is a chance that students will drop out of or fail a course. Consequently, to help and handle a student's issues before they arise, faculty members are informed of possible issues.
8	The FAQ Chatbot	Chabot's are applications that automate a variety of processes with machine learning (ML) and artificial intelligence (AI), leveraging the experience of educators to free up more time for more crucial facets of teaching. If a college responds slowly, the procedure of contacting them with a query may occasionally be slowed down or even stopped altogether. As a result, chatbots are always active, even when no one is there to answer queries.
9	Learning models	The main focus of this has been on creating learner profiles and building models of instructional behavior based on the academic goals' path-level expectations.

3. Artificial intelligence capabilities in educational processes

AI-powered products and services are a part of daily life for educators. Examples include voice assistants in their homes, grammar checkers, essay writers, and phone apps that organize travel automatically. Therefore, educators see opportunities to use AI-driven features, such as speech recognition, to increase the support provided to students with disabilities, multilingual learners, and other groups that could benefit from the improved customization and adaptability of digital learning resources. To better support multilingual students, students with disabilities, and other learners who could benefit from more personalization and adaptability in digital learning tools, teachers see opportunities to use AI-driven features like speech recognition, leverage artificial intelligence (AI) and machine learning (ML) to automate a range of tasks. Thus, educational processes are progressing beyond their original attempts at digital transformation, which include digitizing workflows, automating daily chores, building increasingly sophisticated information, and building dashboards to enhance analytics. These days, institutions are utilizing AI to do tasks more effectively rather than just employing technology to complete the same tasks more efficiently. Education systems use a variety of AI techniques, including Decision Trees, Fuzzy Logic (FL), Genetic Algorithms, Bayesian Systems, Neural Networks, and Hidden Markov Systems. Fomunyam (2020) points out that many changes are expected to occur in the realm of education as a result of this cutting-edge technology, including the ability for computers to provide personalized lectures to individual students, which will relieve teachers of a substantial amount of their workload. Many predictive scenarios, including grade prediction, student success prediction, student retention, and student-teacher pairing, can be predicted with multiple model systems that are now under development.

AI can also be used to customize and modify instruction to each student's needs. AI helps instructors determine how well their students understand their lectures gives them the ability to provide the right hints, and works as a teacher for the students and makes them learn concepts easily. Furthermore, initiatives powered by artificial intelligence offer helpful feedback to instructors and students alike. Learners are empowered to tailor their learning to meet their own needs because of the simple and adaptable structure of these AI-influenced environments. Thus, artificial intelligence (AI) is a well-designed technology that can give teachers and students the chance to pursue learning effectively by offering a flexible arrangement, opportunities for cooperation, options, and control over the learning process (Jain & Jain, 2019). Generative AI is one of the most prevalent types of AI influencing educational processes. This is described as artificial intelligence (AI) that can replicate data without duplicating it by learning from preexisting information to create new, realistic material. New language and media, including text, speech, video, music, pictures, and software code, can be produced using generative AI. ChatGPT, a conversational model that can compose essays, explain artwork, and hold conversations with the user, is one contemporary example of generative AI. The capabilities of generative AI include the creation and augmentation of textual content, question answering, tone-based text manipulation, text summarization and simplification, software code creation, translation, and explanation. and improve the functionality of Chabot's.

4. Pedagogical implications of artificial intelligence in education

The industry relies on educational systems to produce graduates who are well-educated, well-trained, and possess the necessary skills to fulfill the demands of the modern workplace. As such, training and education should be more responsive to the needs of the job market. According to Jain and Jain (2019), the rise of AI is making many jobs obsolete, necessitating the need for whole new skill sets. Learning and teaching are being revolutionized by the AI era, which offers a paradigm shift in the field of education. Through pedagogy, educators can understand the most effective strategies to implement in a classroom. They can better adapt their classes to meet the needs of their pupils by understanding how various students absorb information and learn. To prepare students for the future, it is crucial to develop an AI education for educational institutions. AI technology is progressing quickly, and in the years to come, it is likely to play a bigger role in society. Academic institutions that provide training in the field to both students and teachers can guarantee that graduates are ready to contribute to the development of AI and handle the ethical, social, and economic issues that are likely to arise as AI becomes more widely used. AI can detect students who might be having difficulty early on and notify parents or instructors so that remedial measures can be taken to assist them catch up. AI can help with curriculum planning by helping to create and optimize plans based on student needs, educational standards, and accessible resources. Education institutions that use AI in their curricula become leaders in their fields and stand to gain from it as well.

When AI is incorporated into educational systems, a dynamic new world with significant pedagogical and ethical implications is created. Using AI tools in instruction can improve learning outcomes from a pedagogical standpoint. The capacity to deliver personalized feedback in a manner that encourages dialogue and assists students in refining their grammar is linked to virtual learning tutors and sophisticated chatbots. All students may learn more easily when they use technology-driven resources, even those with time and location restrictions that may arise in traditional learning environments. Students can learn whenever it is most convenient for them thanks to online learning platforms and programs, which give them more flexibility over when and how they learn. The availability of AI chatbots for learners at any time and on any device, including smartphones, is ascribed to the technology's capacity to build a virtual library that functions as a potent learning aid (Alghamdy, 2023). An opportunity to expose students to real-world, authentic systems of learning was presented using AI-powered virtual reality (VR) and augmented reality (AR). When VR techniques and AI are combined, the efficiency of EFL sessions is significantly improved (Li et al., 2020). VR and AI technologies can virtually take students to different cultural contexts, enabling them to have first-hand encounters with language in real-world settings. Using such a method increases learners' motivation and enhances the learning process. For instance, learners could virtually experience a busy street in Washington, DC, a bustling market in South Africa, and a beach in the Bahamas, giving them a glimpse of the diverse cultures where English is spoken and how the language applies to different situations. AI offers unique resources that converge remarkable flexibility and adaptability in creating learning experiences for students, including those with special needs. Not everyone can speak to communicate. People with speech-related disabilities need appropriate ways of self-expression. Using AI makes learning experiences personalized and tailored to the aptitude and place of each learner (Alghamdy, 2023). Artificial Intelligence (AI) offers several benefits to educational environments, such as customized learning, automated grading, and focused feedback, particularly for students with special needs. By analyzing student data and accounting for each student's unique learning preferences and competency level, AI algorithms may deliver individualized recommendations and evaluations.

The application of AI raises certain issues, nevertheless, such as the loss of the opportunity to teach critical and creative thinking. Human-computer interaction and critical thinking, two cornerstones of any learning process, are threatened by AI-learning technologies. The fact that learning is a constructed and evolving process is not acknowledged or embraced by the majority of those who employ artificial intelligence (AI) in teaching and learning. Instead, they have imposed a particular teaching methodology based on behaviorism and an objectivist epistemology, which fails to adequately capture the complexity of learning in educational processes. This is especially true for those with a background in computer science. Alghamdy (2023) links it to potential biases arising from the usage of AI software and the potential dehumanization of educational processes. For the sake of upholding ethical norms and safeguarding educational goals, there must always be a balance when implementing AI in educational contexts. Not only can it free up educators from the stress of marking hundreds of projects, but it can also offer personalized, adaptable, and interactive learning experiences that allow them to concentrate on what matters. i.e. teaching with empathy.

Educational artificial intelligence is a new field of research that has the potential to revolutionize both our methods and our students' learning. More advanced technology and resilient algorithms are liberating people's imaginations and holding out new possibilities like far less work and nearly free maintenance of more fruitful interactions. Artificial intelligence (AI) and other technologies can be used in education at various levels. In the case of educational processes, proposals have focused on two dimensions, i.e. institutional or strategic applications and facilitation of educational activities (Bates, Cobo, Mariño & Wheeler, 2020). Through process optimization, improved learning outcomes, and readiness for the needs of a world that is changing quickly, education could be significantly enhanced by artificial intelligence (AI). To be successful, though, it must carefully balance utilizing technology and keeping the fundamental human components of education. In the qualitative analysis research of their narratives, Han, Nawaz, Buchanan, and McKay (2023) uncover students' beliefs that Artificial Intelligence in education may disrupt learner autonomy, instructional strategies, linkages and interactions, and roles in education.

5. Challenges

Alghamdy (2023) highlights that implementing artificial intelligence (AI) in education has some benefits, but also challenges that call for a thoughtful and methodical approach. Artificial intelligence applications present several kinds of issues, particularly regarding the traditional responsibilities of human resources. A study found that many institutions are facing a significant challenge due to the emergence of innovative information technologies, which calls for the planning, development, and implementation of digital skills to better prepare professionals who can comprehend the technological environment and shape it to suit their needs (Aldosari, 2020).

Education typically lags when it comes to new technologies, which is another reason why AI hasn't had much of an impact on teaching and learning in educational procedures up to this point. The integration of modern technologies into all facets of education is hampered by people's reluctance to take chances, embrace new inventions, and provide financing for anything other than conventional teaching techniques. When faced with new technologies, the education industry seems to be conservative, according to Bates, Cobo, Mariño and Wheeler (2020), because a significant number of educators must be persuaded that a novel idea may enhance or expand learning objectives as well as interactions. The growing use of text-generating AI in academic contexts, as demonstrated by ChatGPT, Bing, and Microsoft's recent addition to its Office suite, Co-Pilot, has come under increased scrutiny. One of the primary concerns about the application of AI technologies in educational settings is the potential for students to engage in academic dishonesty, such as cheating or plagiarism, using generative AI techniques. To address this issue, instructors should receive training in incorporating AI technologies into their teaching methods. However, there is also a risk that educators and students may become overly reliant on AI-powered tools, which could impede students' critical thinking skills and hinder their learning process. Similarly, teachers may also face this challenge in their practice.

While examining the various types of prejudice and moral dilemmas related to AI implementations in educational environments, Akgun and Greenhow (2022) highlighted many issues in their study, including privacy, surveillance, autonomy, bias, and discrimination. They therefore argued that the ethical issues and difficulties that teachers encounter differ according to the grade level and developmental stage of their students. Although AI can generate lesson plans quickly, speed and quality are not always related. Instead of taking the time to analyze and improve the material for the optimal learning outcome, educators may be more likely to accept the information that AI initially provides. Furthermore, students must undergo training on academic integrity to guarantee that they comprehend the significance of upholding ethical standards in their jobs. The absence of data security and privacy in AI systems is also an issue. Massive volumes of data, including private student and teacher information, are generated and gathered by AI systems. Cyberattacks and security breaches must be prevented on this data. As such, to safeguard this data, it is imperative to implement strong data privacy rules and security protocols (Rodrigues, 2020; Shahriar, Allana, Hazra & Dara, 2023; Xiao, Wu, Chiti, Manshaei & Ateniese, 2022). One of the biggest issues with AI in education is the digital divide, where certain students cannot use AI technologies because they do not have access to technology or the web. For this reason, it is imperative to guarantee that every student, regardless of socioeconomic status, has access to AI tools (Fung & Stein, 2023; Hwang, Xie, Wah & Gašević, 2020). Many country's spending on education will increase as a result of incorporating artificial intelligence into the educational system. There will be a significant amount of money spent on schools. Those nations who are unable to adjust to the innovation will ultimately fall behind.

Few studies on the effects of AI in education have looked at socio-emotional outcomes; the majority have focused on cognitive outcomes and adaptive learning, according to Chiu, Xia, Zhou, Chai and Cheng (2023). Research on AI's applications in social science, engineering, and law has extensively examined ethical concerns; nevertheless, education has not benefited from this discourse. Therefore, more investigation is required into the moral dilemmas raised by AI in education. Lack of education perspectives on AI in education research, according to Chiu, Xia, Zhou, Chai and Cheng (2023), is resulting from the reality that most artificial intelligence in education researchers have strong engineering backgrounds and, as a result, tend to take an engineering approach to the field, focusing on technological design and development. The viewpoints of educators and educational researchers are not adequately represented by this methodology. Future studies should look into novel research techniques to do multidisciplinary research on artificial intelligence in education that actively engages all academicians as AI is an interdisciplinary field. Because of this, research on AI in education must develop new techniques for assessing the effectiveness of AI systems.

Table 2. Benefits and challenges

Users	**Benefits**	**Challenges**
Administration	– AI facilitates administrative tasks such as scheduling, enrollment, and resource allocation. – Chatbots and virtual assistants allow administrative staff to work on more complex chores by providing answers to frequently asked questions. – With AI, organizations can make data-driven decisions by processing and analyzing large amounts of data at a very fast and accurate pace	– When it comes to new technologies, education usually lags. – There is the challenge of Insufficient funds and a reluctance to embrace novel ideas or take risks – Education typically falls behind when it comes to new technological advancements. – One issue is a lack of funding and a reluctance to adopt new ideas or take chances. – Because technology is changing so quickly, educators must constantly learn new things and adjust to the possibility of biases emerging when using algorithms. continuous instruction on the application of AI in the classroom for teachers
Faculty	– Predictive analytics facilitates the early identification of students facing learning difficulties and equips them with the requisite resources for success. – Grading assignments is a time-consuming activity for teachers that can be accelerated with the assistance of AI technologies. AI technology also can grade essays and assignments and	– Educators must constantly learn new things and adjust to the continuously changing landscape of technology – Utilizing an algorithm carries the risk of biases manifesting themselves – Because technology is changing so quickly, educators must constantly learn new things and adjust to the possibility of biases emerging when using algorithms.

	give feedback to students on things like grammar, vocabulary, and content.	– continuous instruction on the application of AI in the classroom for teachers
Students	– One of the greatest benefits of AI in education is that it can be easily adapted to different learning methods and individual learning preferences. – AI can maintain students' attention on the material they are studying and make it fascinating. Chat Bots are one way that educators can employ AI in the classroom	– As students get used to using technology to solve problems, an over-reliance on artificial intelligence (AI) could hinder their capacity for critical thought and problem-solving. – Issues surface about data privacy, moral implications, and the possible influence on interpersonal communication during the learning process.

6. The future with AI

Research on AI in education has not yet kept up with the quick development of AI technology, making it difficult to offer evidence-based recommendations and support for AI applications in the classroom, according to Zhang and Aslan (2021). There are still not enough educational perspectives on AI in education research, despite the field's rapid advancements in educational technologies. Furthermore, it is essential to progress through new techniques including data visualization, text mining, learning analytics, and educational data mining (Zhang & Aslan, 2021). Within the fields of education and artificial intelligence, ambitious and bold predictions have been made.

Schiff (2021) observes that advocates for AI in education firmly believe that AI will revolutionize education, allowing students and groups to learn far more effectively than they could from a single human teacher in global classrooms. Intelligent tutoring systems, the main AI-based educational tool available at the moment, are also expected to play a significant role in education going forward. Akinwalere and Ivanov (2022) argue that AI is bound to foster innovation and boost national competitiveness; hence, countries will continue to compete in this burgeoning and rapidly evolving field. Natural language processing (NLP)-enabled adaptive language instruction allows educational materials created in one nation to be utilized in another. Robotics and artificial intelligence (AI) can be utilized to help kids acquire hard skills and spark their interest in STEM fields

Artificial intelligence (AI) is developing so quickly that it can already mimic and even surpass many of our cognitive abilities. As a result, humans may have less motivation to constantly study and develop. The serious concern is that we would thereafter lose our education and our ability to make decisions about the future. Humanity may lose its ability to reason critically because machine guidance is so excellent – almost like an oracle – that learning and independent thought will become useless. To determine if the benefits of AI outweigh the risks, Chen et al. (2020) contend that we must carefully weigh these risks to determine whether we should stick or twist and lessen the likelihood that we will sleepwalk to an undesirable place from which we will be unable to escape.

There is a growing interest in the application of AI systems and algorithms in education. Consequently, enormous amounts of training data that AI requires will significantly increase the value of data and change the way we think about data protection. Achieving widely shared safety and prosperity with this revolutionary technology will require prudent global governance. Efficiency, benefits, security, and many other factors must be balanced as educational systems experiment with AI in traditional classrooms, online, and through mobile learning management systems (Zhang & Aslan, 2021).

The implementation of robotic and technological innovations has educators worried that it may leave them more open to cyber-attacks. Additionally, there is generally a lack of flexibility in solutions offered for problems, as well as financial obstacles to achieving those solutions. Many individuals are not happy with the unequal situation that arises from AI-driven power centralizations in education, which appear to be favoring the otherwise privileged and disadvantageous to the otherwise disadvantaged. The importance of artificial intelligence in enhancing learning and process efficiency, however, cannot be ignored by educators.

As with all aspects of the future, Selwyn (2022) believes that the use of artificial intelligence (AI) in education is unclear, unpredictable, and fundamentally unknown. While most colleges and universities still just have a passing interest in artificial intelligence (AI), many arguments should be carefully considered in the coming years due to the ways that early adopters of AI-driven tools and technology have already affected educational procedures and practices. Selwyn (2022) states that five main points of contention could encourage more thorough discussion and decision-making in light of the rapidly expanding popular, political, and professional discourses surrounding artificial intelligence (AI) and education. These include addressing AI and related to (1) hyperbole, (2) limitations, (3) social harms, (4) ideology, and (5) environmental sustainability.

7. Conclusion

The purpose of this article was to examine how artificial intelligence is used in education, including its potential for use in learning processes, its pedagogical consequences, and the challenges. A content analysis was used in the qualitative study to examine literature from peer-reviewed journals and conference proceedings. AI has the potential to revolutionize education by offering numerous benefits, such as improved effectiveness and personalized learning. By leveraging AI, students can develop critical thinking and problem-solving skills, which are essential in the twenty-first century. Furthermore, AI can provide students with unique and engaging learning experiences. However, integrating AI into education also poses risks, including potential biases and data privacy issues. Therefore, it is crucial to balance technological progress with political, ethical, and other emergent considerations to fully utilize AI for enhancing education.

Acknowledgements

This research did not receive any specific grant from funding agencies in the public commercial, or not-for-profit sectors.

The authors declare no competing interests.

References

Akgun, S., & Greenhow, C. (2022). Artificial intelligence in education: Addressing ethical challenges in K-12 settings. *AI and Ethics*, 2, 431-440.

Akinwalere, S. N., & Ivanov, V. (2022). Artificial intelligence in higher education: Challenges and opportunities. *Border Crossing, 12*(1), 1-15.

Aldosari, S. A. (2020). The future of higher education in the light of artificial intelligence transformations. *International Journal of Higher Education, 9*(3). https://doi.org/10.5430/ijhe.v9n3p145

Alghamdy, R. Z. (2023). Pedagogical and ethical implications of artificial intelligence in EFL context: A review study. *English Language Teaching, 16*(10), 87-98.

Archibald, M. M., & Clark, A. M. (2023). ChatGTP: What is it and how can nursing and health science education use it? *Journal of Advanced Nursing*, 1-4.

Bates, T., Cobo , C., Mariño, O., & Wheeler, S. (2020). Can artificial intelligence transform higher education? *International Journal of Educational Technology in Higher Education*.

Chen, L., Chen, P., & Lin, Z. (2020). Artificial intelligence in education: A review. *IEEE, 8*, 75264-75278. https://doi.org/10.1109/ACCESS.2020.2988510

Chiu, T. K., Xia, Q., Zhou, X., Chai, C. S., & Cheng, M. (2023). Systematic literature review on opportunities, challenges, and future research recommendations of artificial intelligence in education. *Computers and Education: Artificial Intelligence*. https://doi.org/10.1016/j.caeai.2022.100118

Crompton, H., & Burke, D. (2023). Artificial intelligence in higher education: the state of the field. *International Journal of Educational Technology in Higher Education*, 1-22.

Fomunyam, K. G. (2020). Theorising machine learning as an alternative pathway for higher education in Africa. *International Journal of Education and Practice*, *8*(2), 268-277. https://doi.org/10.18488/journal.61.2020.82.268.277

Fung , M. L., & Stein, J. (2023). Leading the Global Frontiers of IEEE humanitarian engineering and technologies programs. *IEEE Bridge Journal, 119*(3).

Han, B., Nawaz, S., Buchanan, G., & McKay, D. (2023). Ethical and pedagogical impacts of AI in education. In *International Conference on Artificial Intelligence in Education.* Tokyo: Springer.

Hwang, G.-J., Xie, H., Wah, B. W., & Gašević, D. (2020). Vision, challenges, roles and research issues of artificial intelligence in education. *Computers and Education: Artificial Intelligence, 1.*

Jain, S., & Jain, R. (2019). Role of artificial intelligence in higher education – An empirical investigation. *International Journal of Research and Analytical Reviews, 6*(2), 144z-150z.

Kahraman, H. T., Sagiroglu, S., & Colak, I. (2010). Development of adaptive and intelligent web-based educational systems. *IEEE.*

Kashefi , A., & Mukerji, T. (2023). ChatGPT for programming numerical methods. *arXiv:2303.12093*.

Klutka, J., Ackerly, N., & Magda, A. J. (2021). *Artificial intelligence in higher education: Current uses and future applications*. Learning House: Wiley Education Services.

Kwan Lo, C. (2023). What is the impact of ChatGPT on education? A rapid review of the literature. *Education Sciences*.

Nassoura, A. B. (2022). Applied artificial intelligence applications in higher education institutions: A systematic review. *Webology, 19*(3).

Ouyang, F., & Jiao, P. (2021). Artificial intelligence in education: The three paradigms. *Computers and Education: Artificial Intelligence*.

Perera , P., & Lankathilaka, M. (2023). AI in higher education: A literature review of ChatGPT and guidelines for responsible implementation. *International Journal of Research and Innovation In Social Science (IJRISS), VII*(VI), 306-314.

Rahman, M. M., & Watanobe, Y. (2023). ChatGPT for education and research: Opportunities, threats, and strategies. *Application Science, 13*, 5783.

Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology*.

Schiff, D. (2021). Out of the laboratory and into the classroom: The future of artificial intelligence in education. *AI & society*, 331-348. https://doi.org/10.1007/s00146-020-01033-8

Selwyn, N. (2022). The future of AI and education: Some cautionary notes. *European Journal of Education*, 620-631. https://doi.org/10.1111/ejed.12532

Shahriar , S., Allana , S., Hazra, S. M., & Dara, R. (2023). A survey of privacy risks and mitigation strategies in the artificial intelligence life cycle. *IEEE Access, 11*. https://doi.org/10.1109/ACCESS.2023.3287195

Slimi, Z. (2023). The impact of artificial intelligence on higher education: An empirical study. *European Journal of Educational Sciences, 10*(1), 17-33.

Torres-Rivera, A., Díaz-Torres, L., Díaz-Torres, S., & Florencio Da Silva, R. (2021). Applications of artificial intelligence in the higher education. *Proceedings of ICERI2021 Conference* (pp. 7706-7710).

U.S. Department of Education, Office of Educational Technology. (2023). *Artificial Intelligence and Future of Teaching and Learning: Insights and Recommendations*. Washington, DC.

Xiao, B., Wu, F., Chiti, F., Manshaei, M. H., & Ateniese, G. (2022). Guest editorial: Introduction to the special section on security and privacy for AI models and applications. *IEEE Transactions on Network Science and Engineering, 9*(1), 171-172. https://doi.org/10.1109/TNSE.2021.3133123

Zhang , K., & Aslan, A. B. (2021). AI technologies for education: Recent research & future directions. *Computers and Education: Artificial Intelligence*. https://doi.org/10.1016/j.caeai.2021.100025

AIMS AND SCOPE

The OJIT, as an international multi-disciplinary peer-reviewed ***online open access academic journal***, publishes academic articles deal with different problems and topics in various areas of information technology and close scientific disciplines (information society, information communication technology - ICT, information architecture, knowledge organisation and management, information seeking, information management, electronic data processing – hardware and software, philosophy of information, communication theory and studies, mass communication, information ethics, library and information science, archival science, intellectual property, history of computer technology, development of digital competencies, ICT in education and learning, ICT education, etc.).

The OJIT provides a platform for the manuscripts from different areas of research, which may rest on the full spectrum of established methodologies, including theoretical discussions and empirical investigations. The manuscripts may represent a variety of theoretical perspectives and different methodological approaches.

The OJIT is already indexed in Crossref (DOI), BASE (Bielefeld Academic Search Engine), Google Scholar, J-Gate, ResearchBib and WorldCat - OCLC, and is applied for indexing in the other bases (Clarivate Analytics – SCIE, ESCI, and SCI, Scopus, Ulrich's Periodicals Directory, Cabell's Directory, SHERPA/RoMEO, EZB - Electronic Journals Library, etc.).

The authors of articles accepted for publishing in the OJIT should get the ORCID number (www.orcid.org).

The journal is now publishing 2 times a year.

PEER REVIEW POLICY

All manuscripts submitted for publishing in the OJIT are expected to be free from language errors and must be written and formatted strictly according to the latest edition of the APA style. Manuscripts that are not entirely written according to APA style and/or do not reflect an expert use of the English language will ***not*** be considered for publication and will ***not*** be sent to the journal reviewers for evaluation. It is completely the author's responsibility to comply with the rules. We highly recommend that non-native speakers of English have manuscripts proofread by a copy editor before submission. However, proof of copy editing does *not* guarantee acceptance of a manuscript for publication in the OJIT.

The OJIT operates a double-blind peer reviewing process. The manuscript should not include authors' names, institutional affiliations, contact information. Also, authors' own works need to be blinded in the references (see the APA style). All submitted manuscripts are reviewed by the editors, and only those meeting the aims and scope of the journal will be sent for outside review. Each manuscript is reviewed by at least two reviewers.

The editors are doing their best to reduce the time that elapses between a paper's submission and publication in a regular issue. It is expected that the review and publication processes will be completed in about 2-3 months after submission depending on reviewers' feedback and the editors' final decision. If revisions are requested some changing and corrections then publication time becomes longer. At the end of the review process, accepted papers will be published on the journal's website.

OPEN ACCESS POLICY