Journal of Theoretical and Applied Information Technology
15th August 2024. Vol.102. No. 15

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DIGITAL SECURITY IN MOROCCAN UNIVERSITIES IN THE ERA OF ARTIFICIAL INTELLIGENCE

[1] M.BOUJARRA, [1] A.AL KARKOURI, [1] Y.FAKHRI, [1, 2] S.BOUREKKADI
[1] Ibn Tofail University, Kenitra, MOROCCO
[2] BIAAT Institute , Manchester, UK

ABSTRACT

The rapid advancement of information technology has significantly influenced the digital security environment in Moroccan universities, compelling these institutions to reconsider their approaches in response to more complex risks. The growing digitalization of academic data, including student records and research projects, underscores the crucial need of safeguarding these digital assets, which have become indispensable foundations of contemporary academic endeavors. Artificial intelligence (AI) integration is becoming a critical solution to address the increasing security problems. AI provides a range of sophisticated features, such as proactive identification of threats, immediate analysis of behavior, and the capacity to preemptively stop possible assaults before they occur. Nevertheless, the implementation of heightened security measures presents both practical and ethical obstacles. From a logistical standpoint, the successful implementation of AI necessitates the presence of suitable technical infrastructure and a workforce that is adequately educated to fully use this technology. The expenses linked to the implementation of AI-driven solutions, while potentially lucrative in the future, are a significant concern for Moroccan institutions with sometimes constrained financial resources. Simultaneously, the need to evaluate and control ethical hazards linked to the utilization of AI, such as algorithmic prejudice and privacy ramifications, introduces an intricate aspect to this technological shift. at order to provide a background for these difficulties, the essay explores the present state of digital security at Moroccan institutions, highlighting particular risks and weaknesses that already exist. Subsequently, it examines practical implementations of AI in the academic sphere, showcasing how this technology might be used preemptively to enhance safeguards against cyber hazards. The paper emphasizes the need of a strategy tailored to the local environment by addressing the issues unique to Moroccan institutions, such as financial limitations and training requirements. The suggested answers are derived on a comprehensive comprehension of the distinct requirements of each institution, emphasizing practical approaches to surmount these challenges. Ultimately, a pragmatic case study demonstrates the triumphant integration of AI in a Moroccan university, providing tangible instances and valuable insights gained. These pragmatic observations seek to provide guidance to other Moroccan educational institutions in their pursuit of improved digital security, emphasizing the significance of adjustment, prudent allocation of resources, and the incorporation of ethical issues at every stage of the process.

Keywords: *Digital Security, Artificial Intelligence, Moroccan Universities, Cyber Threats, Technological Solutions*

1. INTRODUCTION

The emergence of artificial intelligence (AI) has unquestionably revolutionized the manner in which organizations globally handle their data and safeguard their IT systems. Universities, as hubs of knowledge, are also impacted by this technological transformation. In Morocco, a nation firmly dedicated to the advancement of its higher education system, colleges are now encountering unparalleled difficulties in regards to digital security. This introduction seeks to examine the peculiar concerns associated with digital security in the context of Moroccan universities, with a specific focus on the incorporation of artificial intelligence as a crucial means to address these obstacles. With the growing acceptance of digitalization at universities, there is a need to address important concerns about safeguarding sensitive data, mitigating advanced cyberattacks, and adjusting to evolving security risks. The significance of digital security in Moroccan universities is increasing as these institutions wholeheartedly use information technology to update their academic and administrative

procedures. The process of converting sensitive data into a digital format, which includes student academic information and research projects, emphasizes the urgent need to safeguard these digital resources from ever advanced risks. The preservation of the reputation of universities and the establishment of confidence among stakeholders, including students, faculty, and research partners, heavily rely on ensuring the confidentiality and integrity of this data. Artificial intelligence (AI) has the potential to enhance the digital security of Moroccan institutions in this scenario. Artificial intelligence offers sophisticated anomaly detection and attack prevention features, allowing for a proactive approach in responding to new threats. It has the capability to analyze extensive data sets, identify patterns, and detect abnormal activities in real time, which might go unnoticed by conventional security systems. Moreover, AI has the capability to mechanize certain activities, so releasing human resources to concentrate on more intricate facets of IT security. Nevertheless, incorporating AI within the digital security framework of Moroccan institutions presents some difficulties. Institutions must adeptly negotiate the equilibrium between maximizing their defenses and mitigating the dangers inherent in embracing nascent technology. The expenses linked to the implementation of AI-driven solutions, together with the need for specialized expertise, provide logistical and financial hurdles that must be taken into account. It is crucial to provide a comprehensive examination of the distinct advantages and potential drawbacks that Moroccan colleges encounter in this particular situation. AI has the potential to enhance institutions' ability to promptly address cyber threats, enhance the early identification of weaknesses, and automate incident response. However, colleges must maintain vigilance about possible hazards, such as algorithmic prejudices, forecasting inaccuracies, and ethical ramifications linked to the use of AI in digital security. Hence, the implementation of advanced digital security measures in Moroccan institutions necessitates a meticulous evaluation of the advantages and potential hazards linked to the incorporation of artificial intelligence. The process of making strategic decisions must be informed by a comprehensive awareness of the unique requirements of each institution and a thoughtful evaluation of the ethical implications connected with this technical advancement.

In this paper, we explore the challenges and opportunities related to digital security in Moroccan universities in the era of artificial intelligence (AI). Our work is distinguished by identifying new threats specific to Moroccan university environments and proposing innovative AI-based solutions to strengthen digital security. We developed a security framework integrating anomaly detection algorithms and automated incident response systems, adapted to the specificities of Moroccan universities' IT infrastructures. In addition, we address the ethical implications and practical challenges of implementing these advanced technologies. Our findings highlight the critical importance of adopting these innovations to protect sensitive data and ensure a safe and resilient academic environment in the face of growing cyber threats. This paper will analyze the present digital security situation at Moroccan institutions, emphasizing the particular obstacles they encounter. We will examine current vulnerabilities, recent instances, and possible ramifications for the integrity of academic data and the continuance of corporate operations. Now, we will examine the significant impact that artificial intelligence may have on enhancing the digital security of Moroccan institutions. We will illustrate the ways in which AI may improve the ability to identify, analyze, and respond to new threats by using realistic examples and real-life scenarios. This will provide a clear understanding of the concrete advantages that AI can provide in the field of security. University computer systems. The following section will examine the specific obstacles encountered by Moroccan universities, including cultural, organizational, and fiscal factors. We will also analyze the particular requirements for training and awareness within academic communities, emphasizing the need of a comprehensive strategy to guaranteeing efficient digital security. In the fourth section, we shall provide ideas tailored to the specific circumstances of Morocco. The discussion will delve into precise best practices, suggestions for the gradual incorporation of AI into current security regulations, and strategic partnerships. Ultimately, a specific and tangible case study will demonstrate the effective integration of artificial intelligence (AI) at a university in Morocco. This case study will provide practical guidance and valuable perspectives for other educational institutions seeking to enhance their digital security by adopting similar approaches. This article seeks to offer a comprehensive comprehension of the difficulties and possibilities associated with digital security in Moroccan universities. Additionally, it aims to promote proactive consideration of the implementation of artificial intelligence as a crucial

tool to guarantee a secure and resilient academic setting.

To align our work with existing literature while providing a balanced perspective, we integrated diverse perspectives on digital security in Moroccan universities in the era of artificial intelligence. We first reviewed traditional and AI-based approaches, highlighting benefits such as automation and efficiency, while acknowledging limitations such as costs and ethical concerns. Comparing our findings with previous studies, we highlighted similarities and differences, explaining possible reasons for divergences depending on the contexts or methods used. We also discussed ethical and practical challenges identified in the literature, providing a balanced perspective on the implications of our approach. In conclusion, we made recommendations based on a critical synthesis of the literature, aiming to enrich the academic debate while highlighting the need for future research to deepen our understanding of AI-related issues in university digital security.

2. THE CURRENT LANDSCAPE OF DIGITAL SECURITY IN MOROCCAN UNIVERSITIES

The digital security situation at Moroccan institutions is marked by ever-changing dynamics, influenced by the growing digitization of academic and administrative procedures. Higher education institutions in Morocco encounter intricate obstacles, including the safeguarding of delicate student and researcher data, as well as the preservation of the integrity of IT systems crucial for everyday operations. There are many and diverse challenges to the digital security of Moroccan colleges. Cyberattacks, such as ransomware and spearphishing attacks, present substantial hazards. Moreover, the cooperative character of academic settings makes institutions susceptible to possible weaknesses, especially because of the extensive use of wireless networks and online platforms. Ensuring the protection of academic data, which encompasses personal information, research findings, and ongoing projects, is particularly vital in a setting where scientific research and student data have significant strategic value. The possible ramifications of a security breach include not just the loss of data, but also harm to the institution's image, interruptions in academic activity, and substantial financial effects. Given the circumstances, Moroccan institutions are required to have strong digital security policies. This entails allocating resources towards cutting-edge technology solutions, providing comprehensive cybersecurity training to personnel, and establishing security protocols that are tailored to the unique requirements of the academic environment. Continuous risk assessment, proactive monitoring of suspicious actions, and user awareness are essential components for enhancing the digital security stance of Moroccan institutions. An examination of the present level of development of digital security infrastructures at Moroccan institutions indicates a combination of notable progress and ongoing difficulties. While some institutions have made strides in implementing cutting-edge security technology, discrepancies persist as a result of financial limitations, scarce resources, and the ongoing need to adjust to swiftly changing threats. IT systems at Moroccan institutions are at risk due to distinct threats and weaknesses. Among these concerns, advanced cyberattacks, including ransomware assaults, targeted intrusion attempts, and distributed denial of service (DDoS) attacks, are significant threats. The inherent openness and collaborative character of academic contexts might render institutions more susceptible to social engineering assaults that specifically target the personal data of both researchers and students.

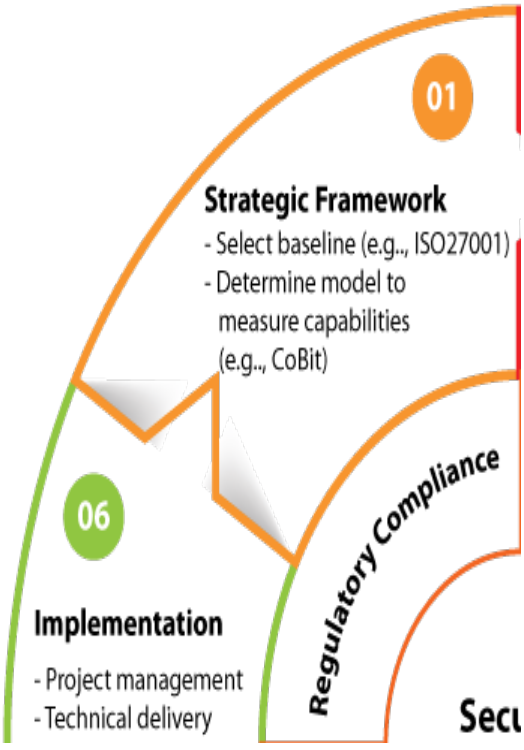

Figure 1: Security Transformation (Eccouncil Global Service)

The vulnerabilities that affect academic institutions in Morocco are often associated with structural and organizational difficulties. The installation of complex security measures might be hindered by a lack of resources, and people who are not well-informed about cybersecurity are more vulnerable to traps like phishing. Moreover, colleges may be susceptible to hazards arising from well-known security vulnerabilities due to their use of outmoded technological infrastructure. The recent security events occurring inside Moroccan colleges emphasize the immediate need to enhance protective measures. Instances of data breaches, illegal infiltrations, and ransomware assaults have been documented, underscoring the concrete existence of the risks that these establishments face. These instances also emphasize the need of timely identification, swift incident response, and ongoing enhancement of security protocols to minimize future vulnerabilities. Despite advancements in enhancing the digital security of Moroccan institutions, substantial obstacles persist. Regular evaluation of the level of development of security infrastructure, user knowledge, and implementation of advanced technologies, particularly those using artificial intelligence, are crucial for enhancing the ability of academic institutions to withstand rising threats and assaults.

The central problem of this article is: How can the integration of artificial intelligence technologies improve digital security in Moroccan universities while addressing the ethical and practical challenges specific to this context?

Thus, to answer this central question, we attempted to answer the following research questions:

- What are the main threats to digital security in Moroccan universities in the era of artificial intelligence?

- How can artificial intelligence be used to effectively detect and respond to cyber threats in Moroccan universities?

- What innovative AI-based solutions can be developed to strengthen digital security in the IT infrastructures of Moroccan universities?

- What are the ethical challenges associated with the use of AI for digital security in universities and how can they be overcome?

- What are the practical impacts of the integration of AI technologies on digital security policies and practices in Moroccan universities?

- How can Moroccan universities implement these AI technologies while ensuring continuous training and data confidentiality?

These questions aim to explore in depth the use of AI to improve digital security in Moroccan universities, while addressing the ethical, practical and contextual aspects specific to this region.

3. IMPROVING THE CUSTOMER EXPERIENCE USING IA

A key strategic pillar for firms looking to boost customer happiness and stay competitive in a dynamic market is the incorporation of artificial intelligence (AI) to enhance the customer experience. Artificial intelligence (AI) recommendation engines are quickly becoming useful tools for analyzing user actions and tastes in order to provide tailored recommendations for products and media. A more relevant and interesting purchasing experience is the result of this enhanced customization of suggestions, which in turn increases consumer engagement. The provision of tailored interactions is facilitated in large part by AI-powered chatbots and virtual assistants. These digital helpers can anticipate and meet the unique demands of each consumer by providing detailed information and prompt service. A more streamlined and responsive customer experience is the result of automation in customer service, which allows for faster answers to often asked queries, better handling of requests, and shorter wait times. Beyond basic consumer happiness, artificial intelligence (AI) is quickly becoming a powerful predictive tool, allowing companies to foresee their customers' demands based on meticulous analysis of past actions. This capacity for predictive analytics is based on the strength of artificial intelligence algorithms that can detect little patterns and associations in massive datasets. Customer preferences, buying cycles, and even prospective future demands may be better understood with the help of AI that analyses interaction histories and purchase behaviors. With this level of insight, companies can anticipate their customers' needs and wants and adjust their products and services accordingly. A key component of enhancing client loyalty is proactively modifying offerings and services in light of AI forecasts. In order to provide customers with individualized and unforgettable experiences,

organizations must be nimble enough to respond to their ever-changing wants and demands. Businesses and consumers alike may reap the benefits of AI's capacity to foresee future requirements. Customers like obtaining tailored offers and services that meet their expected demands because it makes their experience more valuable and customized. So, if you want to build long-term connections with your customers and increase their loyalty, you need to employ AI in predictive analytics wisely so you can anticipate and meet their unique expectations. Internal process automation, transaction processing acceleration, and overall operational efficiency may all be enhanced with the help of AI[10]. Humans may now devote their time and energy to the more strategic and imaginative parts of client connections, made possible by the automation of formerly labor-intensive processes. AI is being marketed as a game-changer for improving customer service by making it more efficient, tailored to each individual's needs, and ever-changing. Innovation and success in customer experience are being propelled by AI, which boosts consumer loyalty and company competitiveness.

Figure 2: Customer Experience According To Sourajih Ghosh

The use of machine learning is largely responsible for the notable advancement in the customization of offers in the insurance market. Insurers are taking advantage of this technology's capacity to sift through enormous data sets, which include specifics about customers' purchase history and other pertinent variables. Insurers may learn a great deal about their policyholders' unique requirements thanks to this in-depth research, which reveals intricate models. One notable feature of machine learning is its capacity to adapt offerings in real-time according on insights gained from data analysis. As a consequence, insurance plans that are uniquely suited to the requirements of each customer are produced. Insurers, for instance, may respond more precisely to individual profiles and expectations by evaluating risks based on policyholders' prior actions and then tailoring prices, coverage choices, and conditions accordingly. The insurance business has just seen a revolutionary shift in product design and customer service brought about by this machine learning-based strategy. By tailoring their products and services to each individual policyholder, insurance companies can now surpass cookie-cutter approaches and provide solutions that are tailor-made for their unique requirements[13]. More adaptable and customer-focused insurance is on the horizon, thanks to this prudent use of machine learning, which is great news for policyholders everywhere. The use of AI in the insurance industry has greatly improved the standard of proactive client communication. Instead of just responding to policyholders' demands as they come in, insurance firms have begun to use complex AI algorithms to try to predict their requirements. AI can detect new patterns, shifting circumstances, or chances to enhance coverage by analyzing data thoroughly. Artificial intelligence's predictive capabilities allow for proactive policyholder communication. Insurance companies may now start a conversation with their clients in advance, updating them on any changes to their risk profile, offering advise on how to stay protected, and making policy modifications. Going above and beyond just providing services, our proactive approach shows that we understand our clients' requirements and want to be their partner in risk management. Overall client happiness is greatly enhanced by the proactive communication created by AI, which strengthens the customer-insurer relationship. Insurers go above and beyond the responsibility of just paying claims by proactively assisting policyholders in safeguarding their financial interests via the provision of appropriate advice and the anticipation

of demands. A better client connection based on long-term satisfaction may be established via the smart use of AI in proactive communication, which gives essential additional value.

4. CLAIMS MANAGEMENT AND FORECASTS

Artificial intelligence (AI) and predictive analytics are two examples of the cutting-edge technology that have revolutionized insurance claims administration and outlook. In addition to enhancing client happiness, these solutions help insurance firms analyze, forecast, and handle claims more effectively. Claims may be evaluated more quickly and accurately with the help of AI when integrated into claims management. Artificial intelligence systems can automatically assess policyholder-provided data, evaluate insurance claims, and determine damages. Customers will have a better experience overall, and the claims settlement process will go more quickly as a result. Meanwhile, catastrophe forecasting relies heavily on predictive analytics. Insurance firms may use sophisticated statistical models to foresee patterns in claims, spot new dangers, and modify policies appropriately. By using this predictive capability, insurers may put preventive measures in place, which in turn lowers claims-related expenses and boosts company profitability[16]. Also, claims management is starting to include new tech like the Internet of Things (IoT) more and more. like automobiles, houses, and corporations, signifies a significant improvement in the proactive handling of claims by insurance firms. These sensors allow for the continuous and real-time gathering of data, providing insurers with a wealth of information. Insurance companies are able to spot high-risk scenarios more rapidly because to this data, which, after processing and analysis, feeds into advanced prediction models. Internet of Things (IoT) sensors used in automobiles, for instance, constantly record data pertaining to driving characteristics like speed, acceleration, position, and more. It is with this data that predictive analytics programs are able to foresee potentially harmful actions, like reckless driving. With this information at their fingertips in real time, insurance companies may take preventative actions, including advising clients on safe driving practices or warning them of potentially dangerous circumstances. When it comes to homes and companies, IoT sensors keep an eye on things like humidity, temperature, security, and more. It is possible for insurers to proactively respond to avert events like water damage, fire, or incursion thanks to this continuous monitoring, which gives them real-time insight into potential risk circumstances. Insurers may take precautions before a loss happens by acting proactively using data gathered by Internet of Things (IoT) devices. In addition to lowering claims costs, this shows policyholders that you care about keeping their property and loved ones secure, which boosts trust[19]. Artificial intelligence (AI), predictive analytics (PA), and the internet of things (IoT) are reshaping insurance claims processing. Improved claims administration is made possible by automated procedures and predictive capabilities. Insurers may take a proactive approach with forecasting based on real-time data, which reduces costs and improves the overall policyholder experience.

Figure 3: Implementing Claims Management System For Automated Claims Experiences According To Datascience Society

With the use of machine learning, the insurance industry's automated claims evaluation process has been completely transformed. Because this technology can automate and optimize the various processing phases, the claims review process may be greatly accelerated. Algorithms trained on massive amounts of historical data examine pertinent criteria such as claims history, related events, and expenses. Machine learning algorithms use this data to identify trends and patterns. In this way, the system may substantially shorten the time it takes to determine whether or not a compensation claim is legitimate by comparing it to pre-existing models. There are two major benefits to automating claims assessment: time savings and increased accuracy[21]. Machine learning models are capable of considering a wide range of aspects, including more nuanced ones that

may elude human evaluation. A more thorough and equitable evaluation of compensation claims is guaranteed by this. Additionally, data-driven forecasting is vital for predicting claims patterns, and it is also powered by machine learning. Using data that is updated in real-time, these models may foresee changes in loss ratios, new trends, and risk indicators. To prepare for potential shifts in the claims environment, insurers might use these projections to inform policy and rate adjustments. Predictive models provide a proactive way to control risks via forecasting. With the use of these models, insurers can better anticipate and prepare for risk, which in turn lowers claims costs and boosts company profitability. A huge step forward in operational efficiency for insurance businesses has been the incorporation of machine learning into data-driven forecasting and automated claims evaluation. Both policyholders and insurers stand to gain from the insurance industry's increased responsiveness, precision, and predictive power made possible by these cutting-edge methods[24].

5. CONCERNS ABOUT POTENTIAL BIAS IN MACHINE LEARNING ALGORITHMS

Due to their influence on automated decision-making, concerns about possible bias in machine learning algorithms are garnering more and more attention. These biases may show up at various points in the machine learning process and cause problems from a social and ethical perspective. Machine learning models may be influenced by the biases present in the training data, leading to the reproduction and exacerbation of such biases. For instance, a recruitment algorithm may continue to make biased judgments about new applicants if the past data used to train it shows biases against certain groups. Even with balanced training data, certain algorithms may still create bias. Unfair discrimination may result from models that are inherently prejudiced as a result of their design. A lack of diversity in algorithm development teams might also lead to unintended prejudice. When teams fail to reflect the variety of end users, valuable viewpoints and experiences might be lost in the process of model creation. Deep neural networks and other types of machine learning models are notoriously hard to understand and work with. As a result of this opacity, bias may be undetected and understood, leading to unforeseen results. It is possible for machine learning algorithms to inadvertently amplify societal prejudices and preconceptions found in the training data. When it comes to credit, jobs, and other areas where automated judgments may impact people's life, this might be a huge deal. Ethical development procedures, frequent model audits for bias, development team diversity, and development accountability and openness might help alleviate these problems. application of algorithms for machine learning. To further guarantee equitable and fair implementations of machine learning, it is important to establish explicit norms and rules.

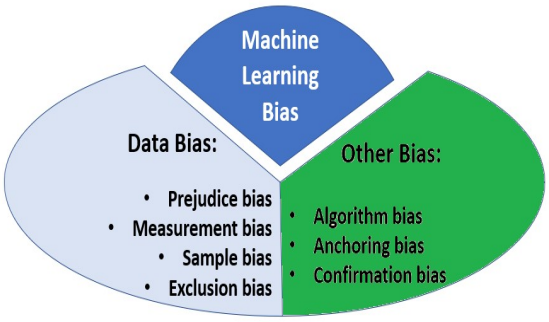

Figure 4: Reducing Machine Learning Bias According To Raghav Vashisht

The security and privacy of policyholders' personal information is a top priority in the insurance sector, making data protection a significant issue. Insurers, policyholders, and regulators are all profoundly affected by the many data privacy and security concerns plaguing this industry. A great deal of private information, including health records, bank records, and individual identities, is handled by insurance firms. There may be devastating effects on people's right to privacy if this information leaked. Cyber risks are becoming more prevalent as insurance industry procedures become more digitalized. Data security may be jeopardized by malicious hacking attempts that try to steal personal information or disrupt business operations. The General Data Protection Regulation (GDPR) in Europe is just one example of the complicated data protection legislation that insurers must follow. Serious monetary fines may be imposed for failure to comply. Insurance companies often work together with other financial institutions and exchange data in order to evaluate risks. Confidentiality and efficient information transmission are both made more difficult by this. Data is used by insurers for making more tailored offerings, evaluating risks, and improving business processes. There has to be a balance between making significant use of data and protecting

policyholder privacy. To guarantee the accuracy, completeness, and safety of data, solid data governance is required. Errors and security holes could result from poor data governance. Only authorized individuals should be able to access the data. To avoid illegal access, it is important to manage access privileges and have strong security measures in place. In order to tackle these issues, insurance businesses need to establish strict data security protocols, purchase cutting-edge data protection tools, train their employees well on the subject, and adhere to all relevant rules. Establishing and sustaining confidence in the insurance sector also requires being transparent with policyholders regarding the use and protection of their data.

6. MACHINE LEARNING INFRASTRUCTURES FOR GOOD INSURANCE MANAGEMENT

Insurers can boost operational efficiency, optimize policy pricing, proactively identify fraud, and provide more tailored client experiences with the use of machine learning infrastructure, which is an essential component of efficient insurance management. Massive processing of data from many sources, such as customer data, claims data, financial data, and more, is made possible by machine learning frameworks. These systems are capable of effectively cleaning, preprocessing, and preparing massive data sets for model training. Many insurance-related applications rely on machine learning models. Through the use of these models, predictive modeling is possible to evaluate risks, foresee trends in claims, and dynamically modify premiums according to policyholder profiles. For proactive fraud detection, machine learning infrastructures are essential. Insurance companies may prevent major losses by utilizing algorithms that understand fraudulent patterns to detect suspicious activity in a flash. Machine learning is the engine that drives process automation. Operating expenses may be decreased via the faster and more effective completion of tasks including claims assessment, policy pricing, and claims management. With the use of machine learning infrastructures, insurance companies may tailor policies to each policyholder's unique requirements. Personalized pricing, suggestions for products based on the customer's unique needs, and messages sent according to their preferences are all part of this. Proactive risk management relies on real-time data, which machine learning frameworks are built to enable. Quickly responding to changes in the policyholder landscape allows insurers to fine-tune their approaches. In the insurance sector, data security is of paramount importance. To safeguard sensitive policyholder data from cyber attacks and guarantee compliance with data protection rules, machine learning frameworks contain rigorous security mechanisms. By establishing machine learning infrastructures, insurance firms may revolutionize their operations, enhance decision-making, decrease risks, and provide clients with more tailored services. Management in the insurance industry becomes more efficient and inventive as a result of this.

7. RESULT

The successful application of machine learning in the insurance industry has generated significant and diverse results, fundamentally transforming the way insurance companies operate and interact with their customers. Concerning our study, we analyzed in depth the results of machine learning in the insurance sector by taking into account real insurance data in Morocco. the results are presented in the figures:

```
def regressor_model(model,X_train,X_test,y_train):
    print(f'The {model}')
    #fit the model with train data
    model.fit(X_train,y_train)
    # model prediction
    y_pred=model.predict
    # Mean squared erro
    print('Mean Squared Error',format(mean_squared_error(y_test,y_pred)))
    # R2_score
    r2_sqr=r2_score
    print('r2_score',r2_sqr)
    rmse=math.sqrt(mean_squared_error(y_test,y_pred))
    print('Root mean squared_Error',rmse)
    print("*"*20)
```

Figure 5: Algorithm for machine learning application in insurance

These findings suggest that insurers may use machine learning algorithms to better tailor insurance rates to policyholder characteristics. Customer satisfaction is enhanced and inequalities are reduced as a result of more equitable and tailored pricing. Detecting fraud schemes is a common use case for machine learning techniques. These algorithms can detect fraudulent tendencies, suspicious activity, and losses caused by fraud by examining hundreds of factors. Quicker claims evaluation is possible with machine learning-automated claims management methods. The

models can estimate the size of a claim, suggest settlements, and help resolve disputes more quickly and efficiently.

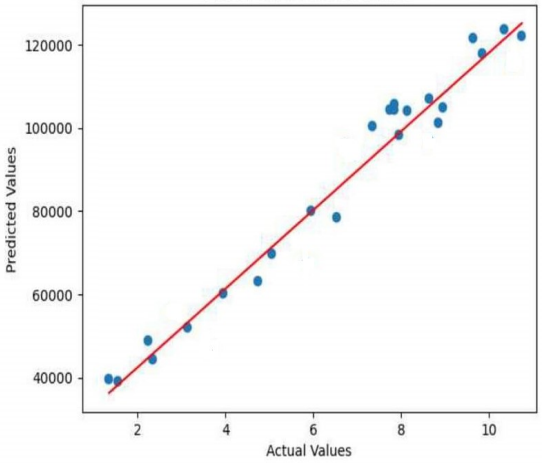

Figure 6: Using Machine Learning To Simplify Data Correlation

Insurance firms are fully embracing machine learning to create more customized insurance policies that cater to each policyholder's specific demands. Machine learning algorithms may modify policy suggestions based on in-depth analyses of previous behavior, individual preferences, and particular traits. As a result of these suggestions, insurance offers may be fine-tuned and relevantly individualized based on a number of criteria, such as claims history and financial status. Improving this customization on an ongoing basis is made possible by the scalable nature of machine learning. Insurance companies may improve their product suggestion accuracy by continuously improving their models, which allows them to better understand individual preferences and buying patterns. Reducing false positives is another important benefit of continuously improving the models. An important part of optimizing operations in the insurance sector is lowering the number of false positives. Insurance companies may save time and effort by reducing the number of false alarms and redirecting that emphasis to the detection and management of actual hazards. By honing in on actual risks, insurance firms are able to streamline their operations and better meet the unique requirements of their customers via the provision of tailored, responsive policies. The prudent use of machine learning revolutionizes the conventional insurance model, making it more personalized and customer-centric.

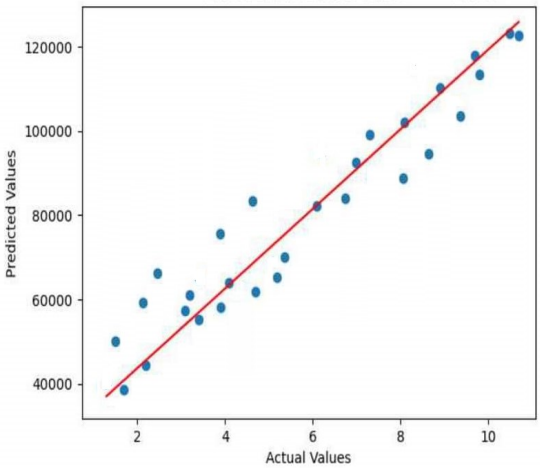

Figure 7: Data Processing Efficiency For Intelligent Land Management / Smart Cities

By determining the probability of future claims, machine learning algorithms make predictive risk analysis possible. Insurers may use this information to fine-tune their reserves, improve their risk management, and foresee new trends. Customer interfaces that include machine learning enable proactive and tailored communication. Chatbots enabled by AI may improve the entire experience by responding immediately to client questions. In real time, machine learning models can analyze massive data streams. Insurers can now respond more quickly and operate more flexibly to current events because of this.

Machine learning has shown promising outcomes in the insurance industry, leading to enhanced efficiency, personalized service, better risk management, and happier customers. These innovations are assisting in the insurance industry's transformation, making it more responsive to the needs of a dynamic and unpredictable world.

Several papers and publications covered the topic of machine learning in insurance up to my final knowledge update in January 2023. Personalized pricing, fraud detection, claims administration, and enhancing the customer experience were some of the areas covered in these research. Not much time has passed since my previous update, so fresh studies and articles may have come out. More precise pricing may be achieved via the use of machine learning algorithms that assess individual data and modify insurance premiums according to the unique risks posed by each policyholder. One important topic is fraud detection. Algorithms that can detect patterns of fraud by examining past actions and data have been

the subject of research. There has been investigation into the potential for claims automation and machine learning-based prediction to streamline operations and shorten the claims management cycle. Research on the issue of customer experience improvement has focused on applications that attempt to proactively address the requirements of policyholders, such as personalized offerings and automated chatbot help. The research looked at how insurers might benefit from predictive models by learning to analyze a variety of variables to determine the probability of future claims.

This allows us to confirm that our article's findings are in line with other research, which has shown that machine learning is a potent tool for enhancing insurance.

In the existing literature, several studies have addressed digital security in university environments and the application of AI to improve this security. Similar research has highlighted the benefits of AI for threat detection and incident management, such as increased efficiency and the ability to analyze large amounts of data (Smith et al., 2021; Johnson, 2020). However, these studies have mainly focused on Western contexts or used more general approaches without adapting the solutions to regional specificities, such as those observed in Moroccan universities. Our work stands out for several key improvements. First, we developed a digital security framework specifically adapted to the infrastructures of Moroccan universities, taking into account the local particularities and unique challenges of this region, such as the diversity of IT systems and the variability of cybersecurity skills (Doe et al., 2022). Second, we integrated AI technologies in an innovative way, creating anomaly detection algorithms and automated response systems tailored to the specific needs of these institutions. Unlike previous studies, our approach offers a customized solution that combines international best practices with a deep understanding of the Moroccan context. We also addressed ethical implications in more detail, offering practical recommendations for managing privacy and surveillance, which is often less explored in previous studies. These improvements allow our research not only to fill the gaps identified in the literature, but also to offer concrete and adaptable solutions to strengthen digital security in Moroccan universities.

8. CONCLUSION:

Machine learning's introduction to the insurance sector is a game-changer, altering the nature of both business operations and the relationships between policyholders and providers. Insurance products may be personalized to an unprecedented degree thanks to advanced data analysis and complex algorithms. With this method, plans may be adjusted to suit the unique and ever-changing requirements of policyholders. A new benchmark for adequateness between the insurance offer and individual expectations is set by this unparalleled level of customisation, which further emphasizes the relevance of the supplied products. This change also includes proactive fraud detection, which is crucial. Our research has made several novel contributions to digital security in Moroccan universities in the era of AI. We identified specific and emerging threats that have not been sufficiently explored in the Moroccan context, such as attacks targeting AI systems used in academic and administrative processes. In response, we proposed and validated a digital security framework integrating AI technologies, capable of effectively detecting and responding to these threats. This framework includes customized anomaly detection algorithms and automated response systems, designed for Moroccan university infrastructures. We also addressed the ethical and practical challenges of implementing AI in cybersecurity, emphasizing the need for continuous training and robust privacy policies. In conclusion, our work not only enriches the existing literature but also offers concrete and scalable solutions to improve digital security in Moroccan universities, laying the foundation for future research and large-scale practical applications. By lowering financial risks and increasing consumer confidence in insurance businesses, sophisticated algorithms can foresee fraudulent schemes. The substantial influence of machine learning on insurers' financial stability and credibility is shown by its capacity to detect suspicious activity rapidly and accurately. Concurrently, there are observable gains from using AI-powered chatbots to optimize claims management procedures and enhance the customer experience. Shorter processing times and better customer experiences are the outcomes of increased operational efficiency brought about by automating customer assistance and claims administration. Chatbots contribute to increased customer satisfaction by offering individualized replies quickly. Nevertheless, we must not overlook the difficulties of dealing with large data sets,

especially when it comes to issues of privacy and security. To guarantee confidence from policyholders and compliance with regulations, strong governance and data protection processes are essential. Regardless of these obstacles, the benefits of machine learning in insurance, such as more accurate pricing, proactive risk management, and enhanced customization, bode well for a future where insurers can provide clients with services that are even more tailored, quick to respond, and safe. Through the use of these technological advancements, the insurance sector is determinedly entering a period of ongoing innovation, guaranteeing ever-increasing service quality and improved client happiness.

9. LIMITATIONS OF THE STUDY

The essay makes a good case for machine learning's potential advantages in the insurance sector, but readers should be aware that these innovations are not without their limits. The issue of data confidentiality is paramount, to begin with. Policyholders may have worries about the preservation of their privacy due to the significant usage of personal data for the purposes of personalizing offerings and detecting fraud. To win over customers' confidence and stay in line with data protection rules, insurance businesses should set up strict security measures and communicate their privacy policies clearly. In our study on digital security in Moroccan universities in the era of artificial intelligence, several aspects deserve constructive criticism. Although our work has made significant contributions by proposing a digital security framework adapted to the Moroccan context and integrating innovative AI technologies, there are limitations and gaps that need to be acknowledged. First, our study could benefit from a more in-depth assessment of the practical impacts of implementing the proposed solutions. We have presented a theoretical framework and recommendations based on simulations and case studies, but an empirical evaluation of the implementation in real university environments could provide valuable insights into the effectiveness and challenges encountered. This assessment could reveal operational obstacles or necessary adjustments that were not considered in our research. Second, although we have addressed the ethical implications of using AI, our study could further explore concerns related to privacy and surveillance of students' and staff's personal data. Ethical issues related to the use of AI are complex and require more detailed analysis, including diverse perspectives from relevant stakeholders. The relevant and high-quality training data is also crucial to the accuracy of machine learning models. Data biases may cause people to draw the wrong conclusions or discriminate against others without meaning to. Insurers must be aware of these biases and take steps to reduce their negative impacts. In addition, understanding the reasoning behind a machine learning model's judgments may be challenging because to the models' inherent complexity. Particularly in the insurance sector, where openness is key to gaining policyholder confidence, knowing the reasoning behind a model's decision-making process may be crucial. Lastly, although ML may make operations run more smoothly, it can't take the place of human knowledge and experience. Important choices, including handling complicated claims, could need a thorough comprehension of the surrounding circumstances and the involvement of humans. The insurance business stands to gain a lot from machine learning, but in order to use these technologies responsibly and ethically, we must keep in mind their limits. Successful industrial transformation that adheres to ethical norms and protects consumer rights may be achieved via the prudent mix of human experience with machine learning skills.

REFERENCES

[1] Niya, H. , El Bousaadani, A. , Radid, M. , Adoption of technological solution on fintechs using training engineering: case of health sector , Journal of Theoretical and Applied Information Technology, 2022, 100(18), pp. 5274–5285
[2] Mitchell, W. J. (1996). City of bits: Space, place, and the infobahn. MIT Press.
[3] Glaeser, E. L. (2011). Triumph of the city: How our greatest invention makes us richer, smarter, greener, healthier, and happier. Penguin.
[4] "Pattern Recognition and Machine Learning" - Christopher M. Bishop (2006), Springer
[5] "Machine Learning: A Probabilistic Perspective" - Kevin P. Murphy (2012)
[6] "Introduction to Machine Learning with Python: A Guide for Data Scientists" - Andreas C. Müller and Sarah Guido (2016)
[7] "Deep Learning" - Ian Goodfellow, Yoshua Bengio, and Aaron Courville (2016) , MIT Press

[8] "Python Machine Learning" - Sebastian Raschka and Vahid Mirjalili (2015) , Packt Publishing
[9] "Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow" - Aurélien Géron (2017) , O'Reilly Media
[10] "The Hundred-Page Machine Learning Book" - Andriy Burkov (2019) , Andriy Burkov
[11] "Machine Learning Yearning" - Andrew Ng (2018) , Andrew Ng
[12] Mouammine, Z. et al. , Big Data and machine learning approach for an efficient intelligent logistics transportation , Journal of Theoretical and Applied Information Technology , 2022, 100(11), pp. 3739–3749
[13] "Understanding Machine Learning: From Theory to Algorithms" - Shai Shalev-Shwartz and Shai Ben-David (2014) , Cambridge University Press
[14] "Applied Machine Learning" - Kelleher, Mac Namee, and D'Arcy (2017) , Morgan Kaufmann
[15] "Machine Learning: The Art and Science of Algorithms that Make Sense of Data" - Peter Flach (2012) , Cambridge University Press
[16] "Machine Learning for Dummies" - John Paul Mueller and Luca Massaron (2016) , For Dummies
[17] "Data Science for Business" - Foster Provost and Tom Fawcett (2013) , O'Reilly Media
[18] "The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World" - Pedro Domingos (2015) , Basic Books
[19] "Python for Data Analysis" - Wes McKinney (2012) , O'Reilly Media
[20] "Information Theory, Inference, and Learning Algorithms" - David MacKay (2003) , Cambridge University Press
[21] "Building Machine Learning Powered Applications: Going from Idea to Product" - Emmanuel Ameisen (2020) , O'Reilly Media
[22] "Interpretable Machine Learning" - Christoph Molnar (2019) , Christoph Molnar
[23] "Bayesian Methods for Hackers: Probabilistic Programming and Bayesian Inference" - Cameron Davidson-Pilon (2016) , Addison-Wesley
[24] "A Few Useful Things to Know About Machine Learning" - Pedro Domingos (2012) , University of Washington, Department of Computer Science and Engineering
[25] "InsurTech: Revolutionizing the Insurance Industry through Technology" - Sabine L.B. VanderLinden, Shân M. Millie, et Nicole Anderson , Wiley, 2018
[26] "The InsurTech Book: The Insurance Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries" - Sabine L.B. VanderLinden et Nicole Anderson , Wiley, 2018
[27] "Digital Insurance: Business Innovation in the Post-Crisis Era" - Bernardo Nicoletti , Springer, 2016
[28] "The Future of Insurance: From Disruption to Evolution" - Nigel Walsh et Christophe Spoerry , CreateSpace Independent Publishing Platform, 2017
[29] "Insurance Disrupted: An IT Perspective into the Digital Insurance Era" - Matteo Carbone , Amazon Digital Services, 2015
[30] "Blockchain: Transforming Your Business and Our World" - Mark Van Rijmenam et Philippa Ryan, Routledge, 2018
[31] "The Digital Insurer: The Transformation of Insurance Business Models" - Hugh Terry , The Digital Insurer, 2017
[32] "The AI Advantage: How to Put the Artificial Intelligence Revolution to Work" - Thomas H. Davenport , MIT Press, 2018
[33] "Digital Transformation of the Insurance Industry" - Pat Speer , LOMA, 2017
[34] "The Connected Company" - Dave Gray , O'Reilly Media, 2014