Quest Journals
Journal of Software Engineering and Simulation
Volume 9 ~ Issue 3 (2023) pp: 16-23
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Smart Watch Fraud Detection System Using Machine Learning and Internet of Things.

[1] Philips Seth .O., [2]Igbe C.M., [3]Amanze B.C.,[4]Agbasonu V.C., [5]Agbakwuru A.O
[1,2,3,4,5]*Department of Computer Science, Faculty of Physical Sciences, Imo State University, Owerri, Nigeria*

ABSTRACT
The objective of this paper is to develop a Smart Watch Detection System for detecting and preventing financial fraud in online transactions, especially credit card transactions using the Supervised Machine Learning algorithm to facilitate learning in various components/devices of the Internet of Things (IoT) network to make them automatic and self-standing; also to analyze data generated over time with the aim of finding out the past trends and be more efficient in detecting and preventing financial frauds. The motivation of this paper is due to the high rate of financial fraud; that is the illegal use of a mobile transaction platform through identity theft or credit card stealing to obtain money fraudulently. The methodology adopted in this work is the Object Oriented Analysis and Design Methodology. We adopted this methodology because, by the object-oriented approach, requirements are organized around objects which integrate both behaviors (processes) and states (data) modeled after real world objects that the system interacts with. The objects in the proposed system include the Bank Customers and the Bank Staffs. Meanwhile the adopted methodology above suits the proposed system development processes because it is a technical approach for analyzing and designing a system by applying object-oriented programming as well as using visual modeling throughout the software development process to improve communication. The system used Supervised Machine Learning and IoT as the techniques. The programming languages applied for this work are Python v3 and Java SE v19, and the Database Management System used is MySQL v8. The result of the proposed system shows a high level of accuracy in financial fraud detection in IoT environment, using the Supervised Machine Learning algorithm.

Keywords: *Credit card, machine learning, IoT, Customers and Staff*

Received 23 Feb., 2023; Revised 03 Mar., 2023; Accepted 05 Mar., 2023 © The author(s) 2023.
Published with open access at www.questjournals.org

I. INTRODUCTION

The growth in information and communication technology (ICT) is greatly revolutionizing the business world; braking barriers and digitalizing almost all transactions. Payment system has moved from analog way to digital (e-payment). This has helped to boost online shopping and e-payment system. With the growth of technologies, Internet of Things (IoT) platform has appeared strongly in the banking sector, and it has changed the banking processes as it offers many opportunities that benefit banks by improving efficiencies which in turn enhance performance, and makes systems smart. The Internet of Things (IoT) is defined as a way for devices which can communicate and exchange information by connecting to the internet [1]. With emergence of Wi-Fi (faster speeds of internet) at lower costs, IoT has emerged as a method to exchange information rapidly by connecting various electronic devices across different locations. This is also called 'Inter-Networking' as it is absolutely based on the internet. This makes transactions seamless and smart, but at the same time opening-up gateways for financial fraud. Financial fraud under IoT environment is the fast-growing issue since the mobile channel can facilitate nearly any type of payments. Due to the rapid increase in mobile commerce and the expansion of the IoT environment, financial fraud in mobile payment has arisen and becomes more common. More than 87% of merchants support either mobile site or a mobile application for online shopping or both [2]. Supporting for mobile wallets also helps to increase the overall occurrence of financial fraud under IoT environment. Financial fraud can occur in several ways, but the most frequent case is an unauthorized use of mobile payment via credit card number or certification number. Financial fraud via credit card can be classified into two main categories based on the presence of a credit card: the physical card and the virtual card. To commit credit card fraud with a physical card offline, an attacker has to steal the credit card to carry out the fraudulent transactions. The online credit card fraud that does not require the presence of a credit card mainly

occurs under IoT environment, since the payment under IoT environment does not require the presence of a physical payment tool; instead, it needs some information such as card number, expiration date, card verification code, and pin number to make the fraudulent payment. For this reason, financial fraud which usually takes place under the IoT environment is the most frequent type of financial fraud that involves taking or modifying credit card information. To address the problem of rapidly arising fraud under IoT environment, financial institutions employ various fraud prevention tools like real-time credit authorization, address verification systems (AVS), card verification value, positive and negative list, etc. [3]. However, existing detection systems depend on defined criteria or learned records, which makes it difficult to detect new attack patterns. Therefore, various methods using Machine Learning and Artificial Neural Networks have been attempted to capture new financial fraud. The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction [4]. An entire IoT system integrates four distinct components: sensors/devices, connectivity, data processing, and a user interface. Below briefly explain each component and what it does.An intelligent system is a system that learns during its existence i.e. it senses its environment and learns from each situation and considers that action that is relevant to the existing condition. Thus we can say that artificial intelligent system is that system that functions in a same way a biological brain works. Artificial intelligence has a wide range of applications in today's world including medicine, stock trading, science, robotics, discovery, telecommunication, banking and many more.

Use of Artificial Intelligence and Machine Learning in the Financial Sector

As banks increasingly apply machine learning (ML) to their processes, achieving gains in quality and efficiency, challenges might emerge. These are often cited dilemma, appropriate data quality, model testing and validation standards, and finally the correct implementation into banks' processes [5]. The paper aimed to outline the most relevant issues to be considered when reviewing supervisory expectations for the use of machine learning. The approach taken here follows the potential new risks. It keeps in mind that balanced and differentiated requirements are needed for legal certainty but also for practicability in order to profit from the potential advantages of machine learning. We are acting as a risk oriented enabler of machine learning in response to industry demand for guidance on the use and regulation of machine learning. Artificial intelligence has become a widespread marketing term that implies high levels of predictive power and efficiency. Supervisors need to understand the features and characteristics of artificial intelligence in order to assess the associated challenges, issues and limitations. Importantly, a key element of artificial intelligence solutions in the supervisory context is machine learning and the aspect of learning, where the machine predominantly performs the training process of a model without pre-defining hypotheses and rules.

The paper work outlines considerations including potential supervisory expectations for machine learning by the Bundesbank's Directorate General Banking and Financial Supervision, with a focus on the financial sector [5]. Successful machine learning applications represent an important building block of digitalization they are able to improve analysis depth, reaction times, operating quality and cost efficiency. In other words banks must continue to maintain a sound risk management environment, including processes to identify and control relevant and material risks. The main supervisory focus should be on features of machine learning which are current regulation and supervisory practices. The characteristic, potential data quality issues or challenges within the model learning process are among the key issues. Even when machine learning depends heavily on data and learning algorithms, it seems that the supporting processes become more important in banks' control environment. Data preparation, model validation, monitoring and escalation procedures become more relevant to maintaining the ability to control model quality.

Secured E-Banking System using Artificial Intelligence

The issue of design and security is very predominant in any financial and business organization, especially such organization as a bank [6]. Therefore, they intend to aid in security of the bank by bringing in an Artificial intelligence system that involves an individual to get an access to some items using face and voice recognition security system. The AI system is not just a normal password lock system that requires a user to insert password and gain access to some items, it is a system that has an administrative authentication. In addition, with this kind of security authentication system they intend to implement, a highly secured AI feature, which enables the user with assured and highly secured transactions using their personal frame. Here an individual have to provide the face and voice authentication, which uses different algorithms, and is read by the AI server for clarification and verification. From the project, they hope to build an alternative and highly verified security for banks. Fraud is a crime of deceiving somebody in order to get money or goods illegally. [7] described fraud as a conscious premeditated action of a person or group of persons with the intention of altering the truth or facts for selfish personal monetary gain.

II. REVIEW OF RELATED WORKS

[8] stated that the application of machine learning algorithms to the detection of fraudulent credit card transactions is a challenging problem domain due to the high imbalance in the datasets and confidentiality of financial data. This implies that legitimate transactions make up a high majority of the datasets such that a weak model with 99% accuracy and faulty predictions may still be assessed as high-performing. To build optimal models, four techniques were used in their research to sample the datasets including the baseline train test split method, the class weighted hyper-parameter approach, and the under-sampling and oversampling techniques. Three machine learning algorithms were implemented for the development of the models including the Random Forest, XGBoost and TensorFlow Deep Neural Network (DNN). The observation is that the DNN is more efficient than the other 2 algorithms in modeling the under-sampled dataset while overall; the three algorithms had a better performance in the oversampling technique than in the under-sampling technique. However, the Random Forest performed better than the other algorithms in the baseline approach. After comparing the results with some existing state-of-the-art works, they achieved an improved performance using real-world datasets.[9] are of the opinion that human activity recognition (HAR) with wearable Internet of Things (IoT) sensors can be beneficial for the elderly and patients monitoring. Smartwatches are the most accessible IoT devices that play an important role in human activity monitoring. The structure of an activity recognition system involves a platform that holds wearable sensors. Under the background, many platforms such as distributed sensors and smartphones and the combination of them have been investigated but platforms are still one of the main research challenges. Smartwatches can be more comfortable for the elderly and patients; therefore the research was focused on a smartwatch as an emerging IoT platform and machine learning method. The smartwatch attached to arm as the main position then was compared to other positions. They considered machine learning methods to present the smartwatch as a reliable platform in order to recognize activities; also they considered k-nearest neighbor and decision tree as two popular machine learning methods for activity recognition. They evaluated the performance with the confusion matrix and then used accuracy and f1-score metrics for the result of our experiment. The metrics show accuracy and f1-score almost 99% as the performance of smartwatch on arm position. The research was majorly on health records but used the techniques that were proposed in this study. [10] in a paper titled "An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation" defined financial fraud under IoT environment as the unauthorized use of mobile transaction using mobile platform through identity theft or credit card stealing to obtain money fraudulently. Financial fraud under IoT environment is the fast-growing issue through the emergence of smartphone and online transition services. In the real world, a highly accurate process of financial fraud detection under IoT environment is needed since financial fraud causes financial loss. Therefore, they surveyed financial fraud methods using machine learning and deep learning methodology, mainly from 2016 to 2018, and proposed a process for accurate fraud detection based on the advantages and limitations of each research. Moreover, the approach proposed the overall process of detecting financial fraud based on machine learning and compared with artificial neural networks approach to detect fraud and process large amounts of financial data. To detect financial fraud and process large amounts of financial data, the proposed process includes feature selection, sampling, and applying supervised and unsupervised algorithms. They recommended an improvement in the accuracy and processing time of the financial fraud process in real time combined with both machine learning based process and deep artificial neural networks.[11] stated that functioning of the Internet is persistently transforming from the Internet of computers (IoC) to the 'Internet of things (IoT)'. Furthermore, massively interconnected systems, also known as cyber-physical systems (CPSs), are emerging from the assimilation of many facets like infrastructure, embedded devices, smart objects, humans, and physical environments. What the authors are heading to is a huge 'Internet of Everything in a Smart Cyber Physical Earth'. IoT and CPS conjugated with 'data science' may emerge as the next 'smart revolution'. The concern that arises then is to handle the huge data generated with the much weaker existing computation power. The research in data science and artificial intelligence (AI) has been striving to give an answer to this problem. Thus, IoT with AI can become a huge breakthrough. This is not just about saving money, smart things, reducing human effort, or any trending hype. This is much more than that – easing human life. There are, however, some serious issues like the security concerns and ethical issues which will go on plaguing IoT. The big picture is not how fascinating IoT with AI seems, but how the common people perceive it – a boon, a burden, or a threat.[12] aimed to develop a pattern recognition tool to analyze transaction patterns and detect suspicious transactions. This would in turn reduce the impact of financial crimes on mobile money transactions in terms of loss of revenue for individuals, corporations and countries by safeguarding legitimate transactions while also tying any loose ends that facilitate the transfer of illegally acquired funds over legitimate channels. The research focused on the field of Pattern Recognition in identifying and analyzing fraud in mobile money transactions. The tool applied Statistical Pattern recognition using the K-Nearest Neighbor algorithm to accurately classify transactions as fraudulent or genuine.[13] used intelligent agents for credit card fraud detection during transactions. In the system presented, Intelligent Agents aids to obtain a high fraud transaction coverage combined with low false alarm rate, thus

providing a better and convenient way to detect frauds. Using intelligent agent, customers' pattern is analyzed and any deviation from the regular pattern is considered to be a fraudulent transaction. In the paper, the intelligent agent is used to detect the fraud when transaction is in progress. The existing fraud detection techniques are not capable to detect fraud at the time when transaction is in progress. As the usage of credit card has increased the credit card fraud has also increased dramatically. The system will send a token to the customer for more security checks and ask a secret question to the customer, if answer correctly, the customer will proceed for the transaction. If fail, the transaction is a fraudulent transaction and SMS message will send to customer and bank database. The system developed was able to improve the security of credit card transactions.[14] presented an adaptive predictive financial fraud detection approach using deep learning methods on a big data platform. The work proposed a novel Big Data driven approach for fraud detection based on Deep Learning methods. A supervised Deep Learning solution leveraging Big Data was shown to be an effective Fraud predictor. Additionally, an unsupervised method based on anomaly detection using deep autoencoders was proposed for when there is few or no labeled data. The two methods presented offered adaptive and predictive Fraud detection through improved analytics. Future work will look into how the two methods can be integrated into an effective tool for enhanced fraud detection.[15] proposed two effective frameworks for fraud detection to deal with fraud challenges. The first framework consists of a novel preprocessing and sub-sampling step, which is followed by applying deep support vector data description for fraud detection. In the second framework, they introduce two versions of an ensemble of one-class classifiers. The work utilized the Bootstrapping technique to create different training datasets for various weak learners to form a more robust model in the Bagging version. In the Stacking version, the research divided the training dataset into two folds. He trained the weak learners on the first fold. Then, the predictions were added on the remaining part of the training dataset to the second fold. Finally, the Meta learner was trained on the second fold to make the final prediction. These two steps form a more robust model to deal with the imbalanced problem. Furthermore, the research work provided a trend analysis based on the size of the training, test datasets, and performance of the model using Area under the Receiver Operating Characteristic Curve (ROC-AUC), Average Precision (AP), and F1 measures as metrics based on a real-world dataset. Based on the results, both approaches outperform SVM and Random Forest as the state-of-the-art binary classifiers in different scenarios. They achieve remarkable performance in terms of AP, ROC-AUC, and F1 measures equal to 90%, 93%, and 85% (Best results), respectively.[16] said that billions of monetary losses are caused every year by fraudulent credit card transactions. The design of efficient fraud detection algorithms is key to reducing these losses, and more and more algorithms rely on advanced machine learning techniques to assist fraud investigators. However, the design of a full-proof Fraud Detection System requires high performing machine learning algorithms that are both accurate and robust enough to handle large data. This work aims to provide solutions by examining various methods previously used for fraud detection, bringing out their strengths and weaknesses. It also examines three classification machine learning algorithms employed for fraud detection (Decision Trees, Neural Networks and the Hidden Markov Model). Finally, Random Forest classification algorithm was implemented, which improves on the weaknesses of the aforementioned algorithms and fraud detection methods, meets real world working conditions and generates accurate alerts while ensuring continuous learning. The open source and statistical programming language R was used for running the algorithm. The impressive figures of accuracy of 0.999 show the power and appropriateness of the algorithm in detecting credit card fraud.

III. METHODOLOGY ADOPTED

Object-oriented analysis and design methodology (OOADM) was adopted in this paper and it is a set of standards for system analysis and application design. It uses a formal methodical approach to the analysis and design of information system. Object-oriented design (OOD) elaborates the analysis models to produce implementation specifications. The main difference between object-oriented analysis and other forms of analysis is that by the object-oriented approach we organize requirements around objects, which integrate both behaviors (processes) and states (data) modeled after real world objects that the system interacts with. For effective implementation of this project, some web application languages were used to design the knowledge based anti-money laundering using multi – agent system. These includes; Hypertext Markup Language (HTML), Hypertext Preprocessor (PHP), MySQL, Cascaded Style Sheet (CSS), Java Script, Dream weaver, and Fireworks. Dream weaver is an HTML-based application that is used to generate graphical user interfaces. The scripting language behind the development of the system is PHP and JavaScript. JavaScript is used to add functionality beyond standard HTML to a web page. It adds interactivity to website. MySQL is used together with PHP in website development and is open source software. These are the materials needed to actualize the projects objectives. Object-oriented analysis and design methodology (OOADM) will be adopted in this research work, and it is a set of standards for system analysis and application design. It uses a formal methodical approach to the analysis and design of information system. Object-oriented design (OOD) elaborates the analysis models to produce implementation specifications.

For the tools used, there are numerous development environments for PHP. These include Integrated Development Environments (IDEs) and text editors, and hybrid environments that combine multiple tools and processes into one.

IV. ANALYSIS OF PROSOPED SYSTEM

This work focused on developing a smart watch detection which is used to detect fraudulent financial activities on mobile application transaction. To do this, a dataset of mobile banking transaction records will be used. In this peculiar type, the pattern of current fraudulent usage of the bank mobile app has been analyzed with the previous transactions, by using the machine learning algorithm. The system designed will allow account holders to use a mobile app for financial transactions. The user will enter the account he/she want to transfer money to, the amount involved and the PIN code for the mobile app. Once the PIN is verified, the smart watch will be activated to monitor and classify the transaction as being valid or fraudulent.Using Machine learning (ML) in bank mobile application is one way to enable the 'learn' capability in artificial intelligence. This involves using a set of learning algorithms driven by mathematical techniques which allow machines to learn from data (financial transaction history), instead of being explicitly programmed to perform certain tasks. The training process uses the learning algorithm to derive relationships between data points from training data, which is commonly a subset of historical data in figure 1. The outputs of the training are trained machine learning models, which can perform predictions or make decisions according to the data patterns observed from the input data, or from queries provided by users.The main goal of the proposed system is to apply a set of classification algorithms to obtain a classification model in order to be used as a scanner for mobile financial transactions and embed the model in an application to be used as a discovery for the fraud transaction data. The implementation involves tasks such as data preprocessing, feature extraction, training models etc. In this research, the system developed uses machine learning classifier to classify the mobile banking transaction. The thesis proposes a methodology to create a model that will detect if a transaction is authentic or fraudulent based on its pattern, by applying supervised machine learning algorithms on an annotated (labeled) dataset that are manually classified and guaranteed. Decision Tree was used for data classifications. The decision tree is an important tool that works based on flowchart like structure that is mainly used for classification problems. Each internal node of the decision tree specifies a condition or a "test" on an attribute and the branching is done on the basis of the test conditions and result. The advantage of decision tree algorithm is that it can work with category and dependent variable. They are good in identifying the most important variables and they also depict the relation between the variables quite suitably. They are significant in creating new variables and features which is useful for data exploration and predicts the target variable quite efficiently. Tree based learning algorithms are widely with predictive models using supervised learning methods to establish high accuracy. They are good in mapping non-linear relationships. They also solve the classification or regression problems quite well.

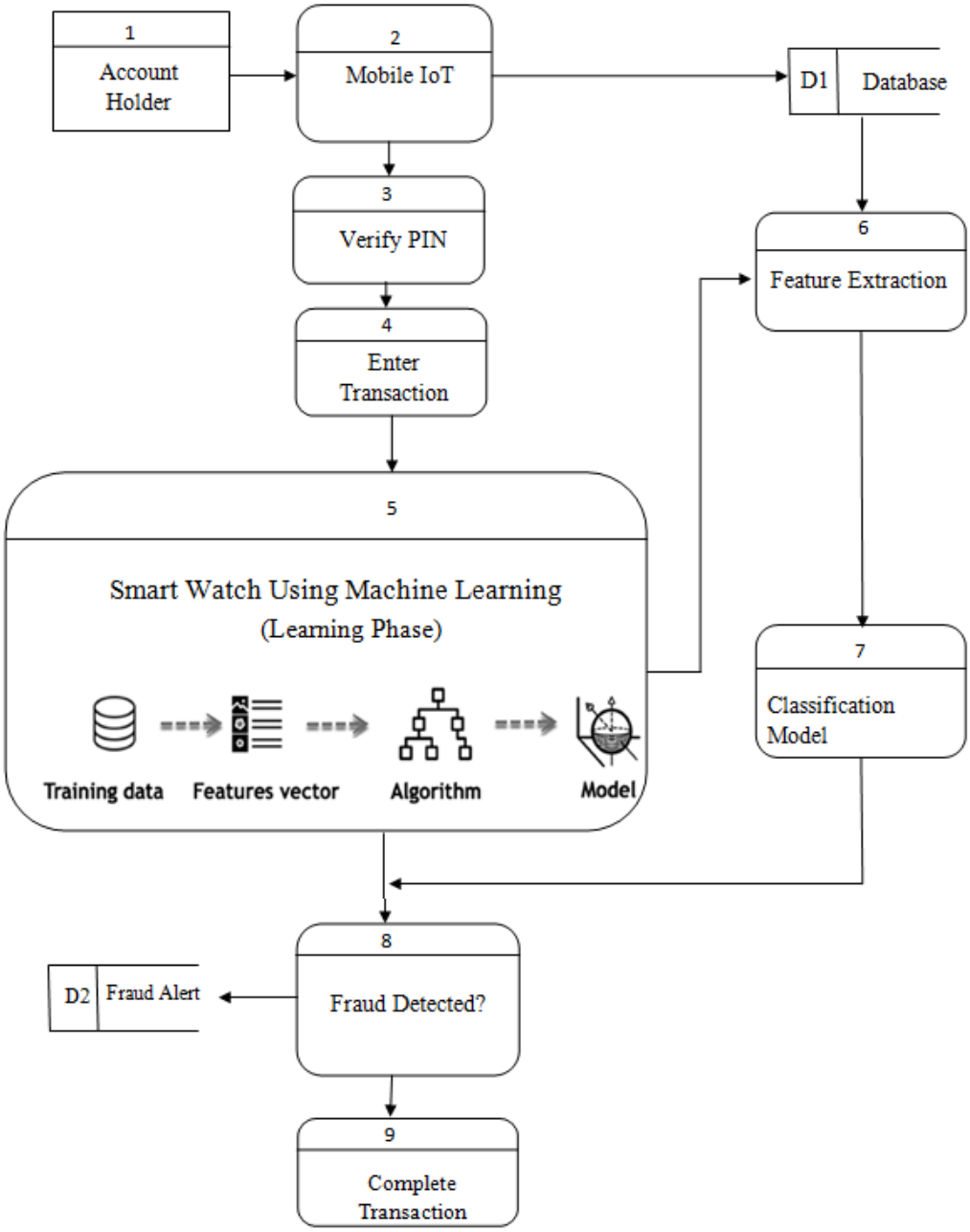

Figure 1: Data Flow Diagram of the new system

V. Result and Discussion

Performance Evaluation

The user quality assurance and performance scoring test was carried out using evaluation metrics including user friendliness (tool-tip text, soft guide notes, pop-up messages), user interface design, reliability, robustness, ease of use, flexibility (customizable features/ control to suit the user's needs) and scalability to incorporate new and advanced features. Performance assessment was carried out by 10 users of the smart watch detection system and the average performance scoring is summarized in table 2 and Figure 2.

Table 1: Performance Assessment

Assessment Tool	Score (%)
Reliability	82
User Friendly	92
Flexibility	75
Robustness	95
Security	98

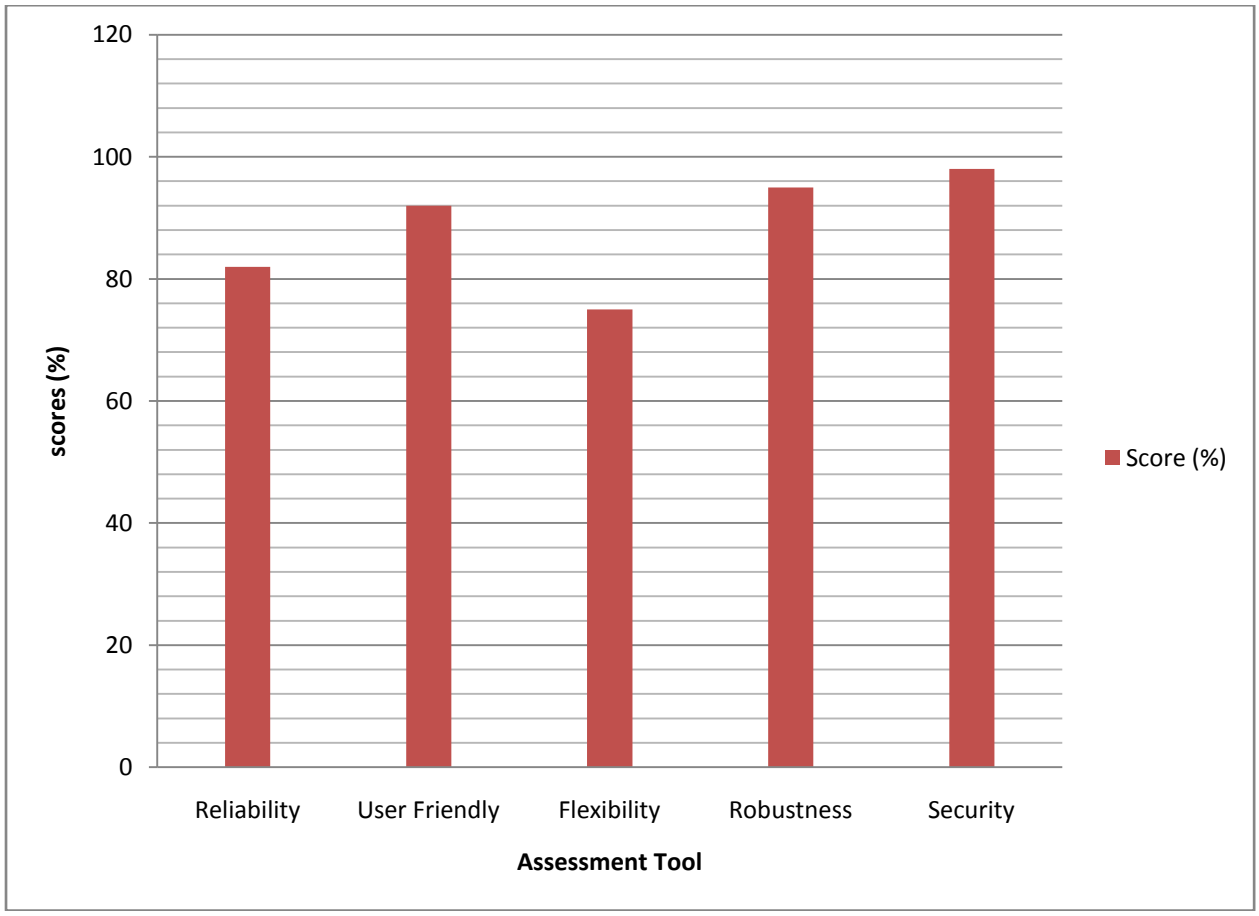

Figure 2: Performance assessment

Also a confusion matrix was used for the analysis of a machine learning model. It reflects the data for smart watch detection in connection with the true positives, false negatives, false positives, and true negatives. This KPI is used to find the classification accuracy of credit card fraud. Table 2 shows the performance grading of the proposed system.

A performance metrics can be derived from the confusion matrix as show in table 3 and equation 1, which show the accuracy (AC) of the Machine Learning Algorithm.

Table 3: **Confusion Matrix**

	Observed		
		True	**False**
Predicted	**True**	TP	FP
	False	FN	TN

$$AC = \frac{a+d}{a+b+c+d} \quad (1)$$

a = True Positive
b = False Positive
c = False Negative
d = True Negative

During the testing, 900 credit card transactions were classified on the system to see how it can accurately identify credit card fraud from the dataset.

Table 4: Confusion matrix applied to test dataset

	Observed		
		True	**False**
Predicted	**True**	850	15
	False	5	30

Table 4 shows that out of 900 credit card transactions posted on the smart watch detection platform, 850 are True Positive and were predicted correctly. Thirty (30) was credit card fraud and detected to be False positive. Fifteen (15) was detected as false negative (shows the wrong classification as credit card fraud) while it is not. Also five was detected as true negative thereby classifying the transaction as not being credit card fraud when it is credit card fraud. Finally a model of performance metrics can be derived from the confusion matrix as show in equation 1, which show the accuracy of the system.

Substituting the values we have

AC = (850+30) / (850+15+5+30)

AC = 0.97 i.e. 97% accuracy in detecting credit card fraud

Table 5: **Performance Results Obtained**

Technique Applied	**Accuracy in detectingcredit card fraud**
Machine Learning Algorithm	97%

VI. Conclusion

The innovations in technology have greatly influenced several improvements in commerce and our daily live activities. Looking at online transactions especially credit cards transactions, it creates avenue for credit card frauds, and this research work focused on improving credit card fraud detection by developing a smart watch detection system using IOT and machine learning algorithms for fraud detection. In paper, one put forth fraud detection method based on supervised learning using Decision Tree. The application developed was able to use the algorithm to classify the present credit card transaction based on the previous transaction history.

References

[1]. Kiranmai,B. N. S. S. and Aneesha, S. (2017). Internet of Things (IoT) – Underpinning the Banking. International Journal of Advanced Research in Science and Engineering. Vol. No 6 special issue (01). www.ijarse.com

[2]. Corp, k. (2016). Mobile payments fraud survey report, Javelin strategy and research 2016

[3]. Panigrahi, S., Kundu, A., Sural, S. and Majumdar, A. K. (2019). Credit card fraud detection: a fusion approach using dempstershafer theory and bayesian learning," Information Fusion, vol. 10, no. 4, pp. 354–363

[4]. Rani, S. L. (2018). Smart Banking Using IoT. Computer Science & Engineering Department

[5]. Deutsche, B. (2020). The Use of Artificial Intelligence and Machine Learning in the Financial Sector. Directorate General Banking and Financial Supervision

[6]. Augustian, R. I., Prakhar, C., Pradip, G., Rohan, G. (2018). Secured E-Banking System using Artificial Intelligence. International Journal of Emerging Technologies in Engineering Research (IJETER) Volume 6, Issue 10, October (2018) www.ijeter.everscience.org

[7]. Egu, J. (2010). The Role of Information and communication Technology (ICT) in Fraud Detection in Nigeria Banks.

[8]. Chinedu, L. U., Idongesit, E. E., Ayei, E. I. (2022). Application of Machine Learning and Resampling Techniques to Credit Card Fraud Detection. Journal of the Nigerian Society of Physical Sciences 4 (2022) 769.

[9]. Nassim, M., Javad, R., Reza, F., John, A. (2020). IOT-Based Activity Recognition with Machine Learning from Smartwatch. International Journal of Wireless & Mobile Networks (IJWMN) Vol. 12, No. 1, February 2020

[10]. Dahee, C. and Kyungho, L. (2018). An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation. Hindawi Security and Communication Networks Volume 2018, Article ID 5483472, 15 pages https://doi.org/10.1155/2018/5483472

[11]. Ashish, G., Debasrita, C., Anwesha, L. (2018). Artificial intelligence in Internet of things. CAAI Transactions on Intelligence Technology, 2018, Vol. 3, Iss. 4, pp. 208–218, India

[12]. Michelle, M. E. (2020). Detecting Financial Crimes using Pattern Recognition Techniques: Case of Mobile Money Transactions. Thesis, Strathmore University]. http://hdl.handle.net/11071/12092

[13]. Amanze, B.C., Asogwa, D.C. &Chukwuneke, C.I (2018). Credit Card Fraud Detection System Using Intelligent Agents and Enhanced Security Features. International Journal of Trend in Research and Development, Volume 5(3), ISSN: 2394-9333 www.ijtrd.com

[14]. Isa, M. I. (2016). An adaptive predictive financial fraud detection approach using deep learning methods on a big data platform. African University of Science and Technology www.aust.edu.ng.

[15]. Masoud, E. (2021). Achieving more effective Fraud Detection. Thesis submitted at the University Of New Brunswick.

[16]. Felix, U., Nwaukwa, J., Ismaila, A., Bosede, O. (2021). Analysis of Machine Learning Credit Card Fraud Detection Models. GSJ: Volume 9, Issue 8, August 2021, Online: ISSN 2320-9186 www.globalscientificjournal.com