

Revolutionizing Vault Security with Smart IoT, Weight Analytics and Machine Learning

Kemal Hajdarevic ¹

¹ Faculty of Electrical Engineering, University of Sarajevo, Bosnia and Herzegovina

Abstract – The persistent use of physical money, despite the rise of digital payment methods, poses security challenges for vaults storing banknotes and coins. Traditional vault security measures, including physical barriers, time locks, dual control systems, and surveillance, are susceptible to sophisticated attacks and insider threats. This paper introduces a novel approach to enhance vault security by incorporating smart Internet of Things (IoT) devices and machine learning algorithms to monitor the weight of banknotes on vault shelves. By tracking and analysing weight variations, this system aims to detect discrepancies and potential theft. The system employs various machine learning models, including Linear Regression, Lasso Regression, K-Nearest Neighbors (KNN), Support Vector Machines (SVM), and Random Forest, to predict the number of banknotes based on weight and denomination. The evaluation demonstrates that Linear Regression and Lasso Regression achieve the highest accuracy, making them the most effective models for this application. Challenges such as limited data, computational resource constraints, and the need for more refined features are discussed, alongside potential improvements like data augmentation and enhanced interpretability. This approach offers a significant advancement in vault security by integrating modern technology to safeguard physical money against theft and unauthorized access.

Keywords – Machine learning, IoT, smart vaults.

DOI: 10.18421/TEM141-02

<https://doi.org/10.18421/TEM141-02>

Corresponding author: Kemal Hajdarevic,
Faculty of Electrical Engineering, University of Sarajevo,
Bosnia and Herzegovina.


Email: khajdarevic@etf.unsa.ba

Received: 24 July 2024.

Revised: 09 December 2024.

Accepted: 03 February 2025.

Published: 27 February 2025.

 © 2025 Kemal Hajdarevic et al.; published by UIKTEN. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDeriv 4.0 License.

The article is published with Open Access at <https://www.temjournal.com/>

1. Introduction

Current trend is to use digital money, such as contactless payment using RFID (Radio-Frequency Identification) cards, phones and electronic currency. Besides this trend, it is a fact that physical money, namely banknotes and coins, are still in use. There is a risk referenced below that physical money can be stolen from vaults. Traditional vault security is built around different approaches and measures.

1.1. Traditional Vault Security

Basic measure includes physical barriers with reinforced concrete or steel walls to prevent breaking or cutting through and thick steel vault doors designed to withstand physical attacks and unauthorized entry. Vault doors have combination locks with mechanical or electronic locks that require a specific combination or code for access. Door locking mechanisms usually have time locks that restrict access during certain times, ensuring that vaults can only be accessed during designated hours. It also includes dual control systems that require two or more authorized individuals (with specific access credentials or keys) to open the vault, adding a layer of security. Technical and physical security is crucial part of security to deter and monitor valuables in vaults. Surveillance, CCTV cameras and alarms (vibration, movement, water, and other sensors) to monitor and alert about any suspicious activities are typically used for this part. Physical guards or security personnel are stationed to protect and monitor the vault. Glue that brings all technologies and personal together are security procedures, where it is stated who, what and when it has to be done.

1.2. Known Incidents Based on the Internet Resources

In history there are many known theft cases of physical money and Internet as a common resource is very helpful to realise future potential of financial impact based on previous incidents [1]. Most recent money theft from bank vault happened in 2024 where burglars stole as much as \$30 million from vault [2].

There was a case in 2014 in Bank of Albania [3] where vault employee stole \$6.5 million from the vault, concealing his actions by filling the empty cash boxes with books and rolls of string. Having this information, a physical money security is even in greater risk from insiders than from outsiders.

1.3. Limitations of Traditional Vault Security Measures

Incidents referenced above state that physical vault security is still vulnerable due to the limitations of traditional vault security measures. Vaults are vulnerable to sophisticated attacks such as usage of modern tools and techniques, and such as high-powered drills and cutting equipment, that can potentially breach steel doors and reinforced walls. Electronic hacking can be used to bypass digital locks and alarm systems. Human error and insiders pose a threat when incorrectly set combinations or codes can lock out authorized users or fail to secure the vault properly. Authorized personnel with malicious intent can compromise the security of the vault as explained in the case above. Traditional security of vaults has a limited fixed set of security features that may not adapt to evolving threats or technological advances.

2. Research Objective and System Delivery Goals

The research objective is to advance vault security by introducing a new level of physical protection for stored cash. This is possible by monitoring weight of sorted money on vault shelves. This paper introduces a novel approach that employs smart IoT devices and machine learning to revolutionize vault security creating smart vault shelves. First goal is to track and record changes (deposit and banknote withdrawal) in stored money weight on the shelves. Every shelf in vault in specific moment in time has a specific amount of banknotes. Based on the denomination of the weight it is easy to determine how many banknotes are on that shelf at any time. Only way to check if all banknotes are on the shelf is visual inspection. Notable discrepancies in the expected weight of money should raise alarms to check contents of the stored money. IoT technology is cheap and can be used with various connectable sensors, using wired and wireless technologies. Multiple sensors are capable to collect data and process it using machine learning algorithms.

3. Literature Review

Based on different historical and recent incidents there is clear need for physical value protection. Below, the available research papers in securing vaults and resources inside vaults are presented.

3.1. Sensors Used in Vault System Security

In the paper [4] presented a smart security system designed to protect bank vaults from theft or unauthorized access, incorporating motion sensors, laser sensors, sound sensors, and gas sensors. The study [5] introduces a security system designed to integrate facial recognition, a fingerprint scanner, a password lock, and RFID technology into a single device, aiming to provide significantly enhanced security. In [6] researchers offer two doors: The first door will feature entry via biometrics or a keypad. Upon opening the first door, a software system will be activated. Once the individual enters, they will encounter a second door equipped with a camera capable of image processing. In paper [7], researchers proposed and implemented a GSM-based advanced security system for bank vaults, integrating seven types of sensors: gas, ultrasonic, laser, vibration, sound, motion, and light sensors. In [8] the system implemented facial recognition, fingerprint, password and RFID scanner. [8] proposed bimodal biometric bank vault access control system.

3.2. IoT Technology Used in Vault System Security

An examination of IoT applications across various security domains, [9] highlights innovative approaches. [10] proposes a two-tiered bank security system utilizing an IoT-based controller. Similarly, [11] introduces a system designed with IoT technology in combination with Arduino Uno and a Bluetooth module. This system incorporates LDR, IR, and Sonar sensors for monitoring. The vault ensures security through two levels: A password-protected entry to connect with a smartphone via the Bluetooth module, and an IR sensor array for implementing a "secret gesture pattern" to unlock the door. There are two US patents [12] approved in 2022 and in 2024 [13] for smart shelves for retail and for coin management with mostly hardware specified components, but without machine learning logics or other software specifications.

3.3. Machine Learning in Anomaly Detection

Machine learning plays a pivotal role in detecting anomalies by analyzing data patterns and identifying irregularities that deviate from expected behavior [14]. These techniques leverage algorithms such as supervised learning [15], unsupervised learning [16], and reinforcement learning to uncover potential security threats, operational issues, or unusual activities. By continuously learning from data, machine learning models enhance detection accuracy over time, enabling proactive responses to mitigate risks. Examples include identifying unusual network traffic [17], detecting fraud in financial transactions [18], and recognizing potential breaches in cybersecurity systems [19].

4. Rationale and Motivations for System Delivery

So far researchers used different types of sensors and IoT technologies to enhance security of vaults. Only few available research works, if any, and take care of risk associated to security of physical money once authorised personal gain access to physical money. There is a clear risk of insiders that can manipulate with physical money once they are authorised to enter vaults. Additional level of security can be added to vaults, more specifically to shelves, so that system can monitor changes of weight on shelves where money is stored.

5. System Architecture

System is developed using hardware and software components to build scale for measuring money weight. System prompts user to enter denomination that is stored on a shelf, with a certain number of banknotes stored. System checks weight and compares it to number of banknotes.

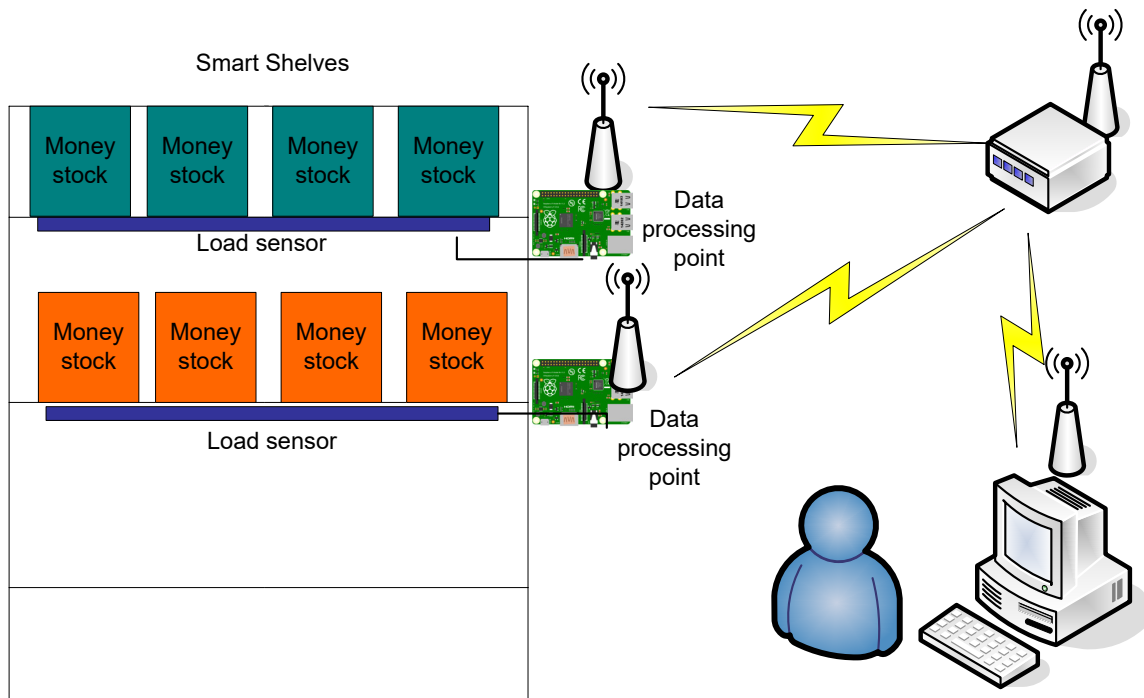


Figure 1. System architecture

5.1. Overview of System Architecture

Description of the overall system architecture is shown in Figure 1.

5.2. System Components

System has IoT Raspberry Pi nodes with HX711 and load sensor attached [20]. Load sensor uses Wheatstone Bridge Circuit which can be used for different tapes of sensors [21]. Detailed diagram of connection between Raspberry PI HX711 and load sensor is shown in Figure 2.

Hardware components that include controller (IoT device) and load sensor amplifier are used. The Raspbian operating system, designed specifically for Raspberry Pi hardware, is widely used due to its compatibility and optimization for embedded systems.

Python, a versatile and user-friendly programming language known for its extensive libraries, was utilized as the primary tool for implementing algorithms and handling data processing tasks.

5.3. Smart IoT Devices

Raspberry Pi 2 is used as a core hardware for IoT with TP-LINK TL-WN722N USB WIFI dongle for wireless communication. The HX711 amplifier with load sensor able to measure up to 10 Kg, and two plates, one as base of scale and another as a base for items measuring, are also used.

5.4. Communication Protocols

Raspberry Pi 2 communicate within the network using WIFI or wired connection and TCP/IP protocol.

5.5. Data Processing

Data collection is done by reading load sensor data. and pre-processing methods.

5.6. Machine Learning Algorithms Used

This work utilized three machine learning algorithms: K-Nearest Neighbors (k-NN), Random Forest (RF), and support vector machine (SVM), used in previous work [22]. In this paper Linear Regression and Lasso Regression were also used.

First, the Raspbian operating system was implemented on the Raspberry Pi hardware, followed by the installation of the latest Python distribution. Next Python libraries were installed: pandas, sklearn matplotlib and seaborn, numpy. These libraries support KNN, RF, SVM, Linear regression and Lasso Regression for detecting and predicting money weight based on number of banknotes, observed sensor readings and user interaction.

5.7. K-Nearest Neighbors (K-NN)

The K-NN algorithm operates based on the given dataset and a fixed parameter K. The following steps outline how the K-NN algorithm functions:

- Using a distance function, the K readings nearest to the prediction point are identified.
- The predicted output is determined by averaging the K nearest readings:

$$Y_{i+1} = \frac{1}{K} \sum_{i=1}^K y_i \quad (1)$$

- K represents the size of the neighborhood,
- y_i denotes the nearest reading.

5.8. Random Forest

The primary goal of a random forest can be observed as:

$$F(x) = \frac{1}{T} \sum_{i=1}^T f_i(x) \quad (2)$$

- $F(x)$ represents the final prediction of the ensemble,
- T denotes the total number of trees in the forest,
- $f_i(x)$ represents the prediction of the i -th tree.

5.9. Support Vector Machine (SVM)

The hyperplane equation in a D -dimensional space can be expressed as:

$$f(x) = \mathbf{w} \cdot \mathbf{x} + b \quad (3)$$

- $f(x)$ represents the decision function,
- \mathbf{w} weight vector,
- \mathbf{x} denotes the input feature vector,
- b denotes the bias term.

SVM incorporates the concept of hinge loss to penalize misclassifications. The goal is to minimize the following objective function:

$$\min_{\mathbf{w}, b} \frac{1}{2} \|\mathbf{w}\|^2 + C \sum_{i=1}^N \max(0, 1 - y_i(\mathbf{w} \cdot \mathbf{x}_i + b)) \quad (4)$$

- N is the total number of training samples,
- C is the regularization parameter that balances maximizing the margin and minimizing the loss,
- y_i represents the class label of the i -th sample.

5.10. Linear Regression

Equation:

$$y = \beta_0 + \beta_1 x + \epsilon \quad (5)$$

(where β_0 is the intercept, β_1 is the slope, and ϵ is the error term)

Multiple Variables:

$$\text{Coefficients: } y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \dots + \beta_n x_n + \epsilon \quad (6)$$

$$\text{Prediction: } \hat{\beta} = (X^T X)^{-1} X^T y \quad (7)$$

$$\hat{y} = \hat{\beta}_0 + \hat{\beta}_1 x_1 + \hat{\beta}_2 x_2 + \dots + \hat{\beta}_n x_n \quad (8)$$

5.11. Lasso Regression

Equation:

$$y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \dots + \beta_n x_n + \epsilon \quad (9)$$

Objective: Minimize the sum of squared residuals plus a penalty term:

$$\text{Loss Function} = \|y - X\beta\|^2 + \lambda \sum_{j=1}^n |\beta_j|$$

- $\|y - X\beta\|^2$: Residual sum of squares
- $\lambda \sum_{j=1}^n |\beta_j|$: L1 penalty term (shrinkage) (10)

Penalty: Controls regularization strength (λ):
Large λ : More regularization (more coefficients shrink to zero),

Small λ : Less regularization,

Coefficients: Estimated by solving the above objective function.

5.12. Accuracy of Data Model Used

The accuracy of the algorithms was determined using the following formula:

$$\text{Accuracy} = \frac{TP}{N} \quad (11)$$

- TP represents the count of true positives, which are instances correctly classified where the actual class matches the predicted class.
- N refers to the total number of instances in the testing set.

6. Implementation

Implementation is performed using hardware and software components.

Software components are Raspbian operating software, Python libraries and two software programs tailored for this project.

6.1. System Prerequisites

The experimental setup utilized various Python libraries, including Adafruit for hardware interfacing, Pandas for data manipulation, Scikit-learn for implementing machine learning algorithms, Matplotlib and Seaborn for data visualization, and NumPy for numerical computations, HX711 library to work with HX711 amplifier, sys and time libraries.

6.2. Hardware Setup

In Figure 2 the schematic connections between two HX711 sensors and the GPIO pinouts of the Raspberry Pi 1 are illustrated, showcasing the connection scheme employed in this study.

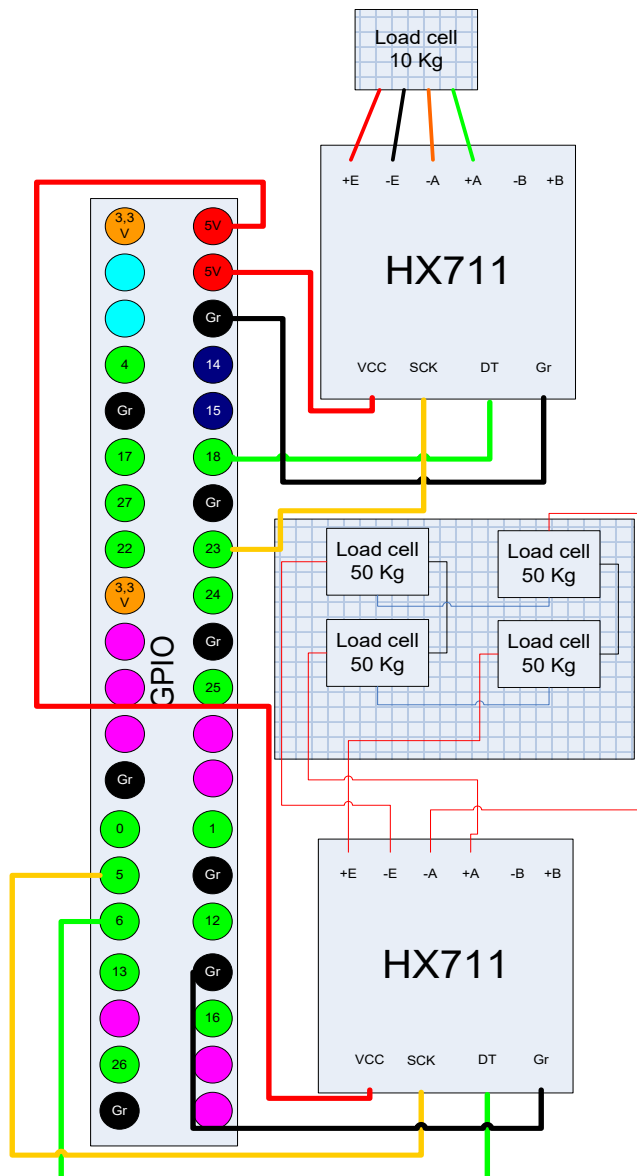


Figure 2. Connection scheme between two HX711 sensors, load weight for 10Kg and Raspberry Pi 2 GPIO pinouts

6.3. Software Development

System software logic is developed through two parts shown in Figure 3. First part is measuring and counting actual data of weight of specific denomination, and how many banknotes were in specific set of measured money amounts.

Second part is learning and prediction part using machine learning algorithms: KNN, SVM, Linear Regression and Lasso Regression.

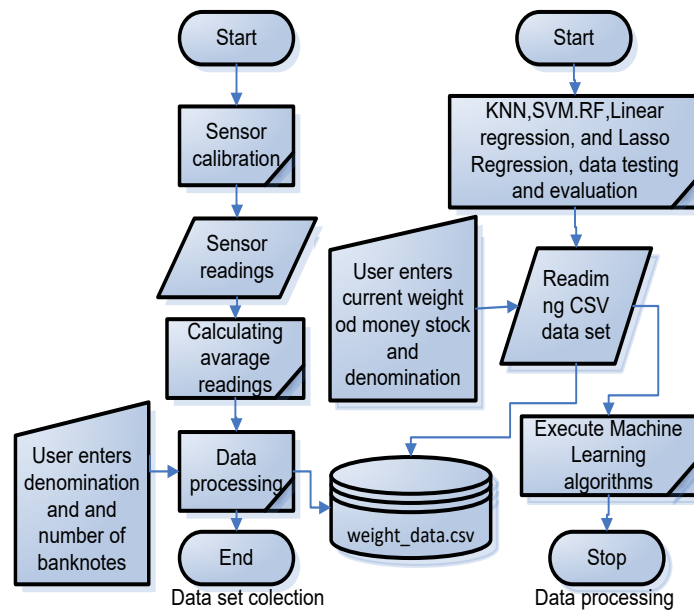


Figure 3. System algorithm logic

7. Experimental Setup and Results

In this section the experimental environment and gathered results are explained.

7.1. Testing Environment

Prior to banknote, measurement commercial products, which declared weight were used. For experimenting with banknotes and coins different currencies were used. For testing purposes 50 Euro banknote was used, recorded and system was trained using this banknote.

7.2. Data Collection

Python program was designed and coded being capable to measure current weight placed on load sensor. The user would be given prompt to enter denomination, and count or number of banknotes was shown in Figures: Figure 4 - training and evaluation, Figure 5 - learning process, and Figure 7 - program output.

Program for evaluation was designed and coded in a way to ask user to prompt current weight and denomination stored on shelves – shown in Figure 5.

6.4. System Integration

Combining hardware Raspberry Pi, HX711 amplifier, and load sensor connection diagram are shown in Figure 2, and software design in Figure 3. System is integrated so that user can decide if money stored on shelves should be as it is predicted based on current weight status. This integrated system components provide cohesive security solution.

7.3. Model Training, Evaluation and Validation

Training machine learning models and validating their accuracy was performed on limited set of measurement and data, as shown Figure 4.

```
# Train models
linear_model.fit(X_train, y_train)
knn_model.fit(X_train, y_train)
svm_model.fit(X_train, y_train)
rf_model.fit(X_train, y_train)
lasso_model.fit(X_train, y_train)

# Evaluate models
def evaluate_model(model, X_test, y_test, model_name):
    y_pred = model.predict(X_test)
    r2 = r2_score(y_test, y_pred)
    mse = mean_squared_error(y_test, y_pred)
    print(f'{model_name} R^2 score: {r2}')
    print(f'{model_name} Mean Squared Error: {mse}\n')

print("Model Evaluation:")
evaluate_model(linear_model, X_test, y_test, 'Linear Regression')
evaluate_model(knn_model, X_test, y_test, 'KNN')
evaluate_model(svm_model, X_test, y_test, 'SVM')
evaluate_model(rf_model, X_test, y_test, 'Random Forest')
evaluate_model(lasso_model, X_test, y_test, 'Lasso Regression')
```

Figure 4. Training and evaluation

Model training and evaluation was performed automatically using Python functions shown in Figure 4. Training and evaluation. Validation was done manually during learning process.

7.4. Performance Metrics

The KNN mean square errors were 9, RF was 1, SVM was 11, Linear regression 0,008, and Lasso Regression 0,009. Data set was small and response time was not relevant for discussion.

7.5. Analysis of Experimental Results

Results of measuring weight using load cell and amplifier shows maximum, +/- 2 gram measurement error is shown in Figure 5.

```
kemal@raspberrypi:/hx711py $ sudo python test.py
Calibrating the baseline...
Baseline weight: 1370.492 grams
Enter the denomination of the banknotes (e.g., 50 for 50 euros): 50
Enter the expected number of banknotes: 9
Adjusted Weight: 9.449000000000296 grams
Adjusted Weight: 9.48199999999971 grams
```

Figure 5. Learning process

All measurement were stored in weight_data.csv file, shown in Figure 6:

```
time_stamp,weight,denomination,count
2024-07-24 08:47:38,7.615500000000338,50.0,7
2024-07-24 08:47:48,7.559000000000424,50.0,7
2024-07-24 08:47:58,7.654000000000451,50.0,7
2024-07-24 08:51:23,4.304499999999962,50.0,4
2024-07-24 08:51:32,4.309999999999718,50.0,4
2024-07-24 08:53:50,4.393999999999778,50.0,4
2024-07-24 08:54:18,10.465289345223254,50.0,10
2024-07-24 08:55:05,11.789299992022277,50.0,11
2024-07-24 08:56:13,12.638200878444022,50.0,12
```

Figure 6. Weight_data.csv

Afterwards, the data of multiple samples were recorded in weight_data.csv file – Figure 6. weight_data.csv.

```
kemal@raspberrypi:/hx711py $ sudo python analiza_podataka.py
Index(['time_stamp', 'weight', 'denomination', 'count'], dtype='object')
Model Evaluation:
Linear Regression R^2 score: 0.9986696965908176
Linear Regression Mean Squared Error: 0.008314396307389853

KNN R^2 score: -0.4399999999999995
KNN Mean Squared Error: 9.0

SVM R^2 score: -0.9027883578959341
SVM Mean Squared Error: 11.892427236849588

Random Forest R^2 score: 0.8059999999999998
Random Forest Mean Squared Error: 1.2125000000000001

Lasso Regression R^2 score: 0.9984690248999096
Lasso Regression Mean Squared Error: 0.00956859437556501

Enter data for predicting the number of banknotes:
Weight of the money (in grams): 582
Denomination of the money: 50

Prediction Results:
Predicted number of banknotes (Linear Regression): 581.7780074390969
Predicted number of banknotes (KNN): 27.0
Predicted number of banknotes (SVM): 7.989890226977877
Predicted number of banknotes (Random Forest): 74.08
Predicted number of banknotes (Lasso Regression): 581.1898190554538
```

Figure 7. Program output

Another program (Figure 7: Program Output) was used to test KNN, SVM, Linear Regression, and Lasso Regression. It utilized the weight_data.csv file along with real-time measurements from the smart shelf. The user was prompted to enter the current weight of the banknotes on the shelf and specify their denominations.

8. Discussion

Furthermore, the strength and weaknesses of proposed model for predications with its effectiveness and with challenges and possible improvements are explained.

8.1. Effectiveness

Linear Regression and Lasso Regression both provide highly accurate predictions with minimal error, making them the most suitable models for this task. The poor performance of KNN and SVM suggests that these models are not well-suited to the problem at hand, likely due to issues related to model complexity, hyper parameter tuning, or feature representation. Random Forest offers a good alternative but shows more variability in predictions compared to Linear and Lasso Regression.

Overall, for the given problem of predicting the number of banknotes based on weight and denomination, Linear Regression and Lasso Regression stand out as the most reliable models.

8.2. Challenges

Limited set of data and testing was challenging and future work will be focused on this part of system development. Computational resources are an issue because of time needed to execute program. There is problem with drift in precise measurement over time and sensors have to be maintained and recalibrated.

8.3. Improvements

Collecting more data or generating synthetic data can help improve model performance. Experimenting with different features and applying techniques like normalization and scaling can enhance model effectiveness. Current improvement is deploying 200 kg sensors. Using techniques to interpret and visualize model predictions can aid in understanding and trust. Using cloud computing or optimized algorithms can address resource constraints.

9. Case Studies

Below are examples how presented system can be used in real world applications.

9.1. Real-World Applications

This type of system can be used in bank vault security systems by enhancing theft detection by monitoring weight changes in vault shelves. The system can detect discrepancies indicative of theft or tampering. This provides an additional layer of security beyond traditional physical barriers and alarm systems. It can help in insider threat mitigation, where system can identify unusual weight fluctuations that may suggest insider theft, offering a safeguard against unauthorized actions by trusted personnel. Cash handling in retail implemented through inventory management where retailers can use similar technology to monitor the weight of cash drawers or safe deposit boxes, ensuring that the recorded amounts match physical counts and reducing the risk of internal theft. It can help in fraud prevention by integrating weight-based verification with cash handling procedures, retailers can detect counterfeit or altered banknotes, enhancing overall security. It can be used in government and institutional security in securing storage of sensitive materials.

Institutions dealing with large sums of physical currency or valuable materials can implement this system to safeguard their assets, ensuring that discrepancies are detected promptly.

The system can assist in meeting regulatory requirements for secure cash handling and storage, providing audit trails and evidence of compliance. Museums, galleries, and financial institutions dealing with high-value physical assets can use weight-based monitoring to ensure that valuable items are secure and accounted for. Integration with existing security measures provides an additional safeguard against theft or mismanagement. In banknote processing facilities system can be used to automate the reconciliation process in facilities that handle and sort large volumes of banknotes, reducing manual errors and improving efficiency. Automated systems can provide real-time updates and alerts regarding the state of cash handling, facilitating prompt responses to anomalies. Banks and financial institutions can deploy this technology in their vaults to ensure the integrity of stored cash and detect any potential issues early. Integration with broader fraud detection systems can enhance the ability to identify and respond to suspicious activities involving physical cash.

10. Comparison with Traditional Methods

This paper explores the limitations of traditional vault security measures and presents an innovative IoT-based weight-monitoring system as a solution. Traditional methods often rely on physical barriers, mechanical locks, and surveillance, which, while effective against external threats, can fall short in detecting more arduous forms of tampering or insider threats.

10.1. Enhanced Detection of Unauthorized Access

Traditional Methods: Conventional vault security primarily relies on physical barriers, such as reinforced concrete and steel, combined with mechanical or electronic locks, and alarm systems. These methods are effective against direct physical breaches but may not detect subtler forms of tampering or theft, especially when insiders are involved. **Proposed System:** The weight-based monitoring system provides an additional layer of security by detecting discrepancies in the weight of banknotes. This method can identify unauthorized withdrawals or tampering even if physical security measures are not breached.

10.2. Mitigation of Insider Threats

Traditional Methods: Traditional vault security can be compromised by insiders with knowledge of security codes or access mechanisms. Although dual control systems and surveillance can mitigate this risk, they are not fool proof.

Proposed System: By monitoring weight changes, the system can detect anomalies that may indicate insider theft or fraud, offering a safeguard against internal threats that might evade traditional security measures.

10.3. Real-Time Monitoring and Alerts

Traditional Methods: Traditional systems often involve periodic checks and manual inspections, which may lead to delays in detecting issues. Alarms and sensors may not always provide immediate or actionable insights. **Proposed System:** The IoT-based solution allows for real-time monitoring and automatic alerts based on weight discrepancies. This enables faster detection and response to potential issues, enhancing overall security.

10.4. Cost and Complexity

Traditional Methods: High-quality vaults and security systems can be expensive and complex to install and maintain. They often require significant infrastructure and ongoing operational costs. **Proposed System:** The use of IoT devices and load sensors is relatively cost-effective and can be implemented with existing hardware like Raspberry Pi. The system's scalability allows for gradual upgrades, making it more affordable and adaptable.

10.5. Adaptability to Evolving Threats

Traditional vault security or traditional methods may have limitations in adapting to new threats and technological advancements. Fixed security features might not address emerging risks effectively. The proposed system's use of machine learning algorithms allows it to evolve with changing patterns of behaviour and threats. By incorporating new data, the system can improve its predictive capabilities and adapt to evolving security needs.

10.6. Integration with Existing Systems

Integration with existing security systems can be challenging, especially when adding new layers of protection or technology. The weight-based monitoring system can be integrated with current security infrastructure, enhancing overall security without completely overhauling existing measures. It complements rather than replaces traditional methods.

10.7. Ease of Implementation

Installing and configuring traditional security systems can be complex and require specialized knowledge. With the use of readily available IoT components and software, the proposed system can be set up with minimal technical expertise. This ease of implementation makes it accessible for various applications beyond high-security vaults.

11. Conclusion

The proposed system addresses these gaps by incorporating weight-monitoring technology to detect anomalies, such as unauthorized access or tampering.

Looking ahead, future developments aim to refine the system's accuracy, scalability, and usability through advanced data collection, machine learning optimization, and integration with other security measures. These enhancements will ensure adaptability to diverse security environments, making the system a robust and comprehensive solution for safeguarding physical assets in vaults. This paper presents a novel approach to enhancing physical vault security through the integration of smart IoT devices and machine learning algorithms. The proposed system introduces an additional layer of security by monitoring and analyzing the weight of banknotes stored on vault shelves. Future work will focus on enhancing weight measurement to test the system with 50 kg x 4 sensors. The dataset will be expanded to include a larger variety of denominations, weights, and banknote conditions to improve the robustness and accuracy of the predictive models. Machine learning algorithms will be refined to improve prediction accuracy and reduce errors. A more comprehensive security system will be created by integrating weight-based monitoring with other security measures. Efforts will be made to ensure that the system can be scaled to handle larger vaults or multiple vaults within a facility. The user experience will be enhanced, making the system more accessible to operators. The system will be designed to meet industry standards and regulatory requirements. The economic viability of the proposed system will be assessed in various applications. Finally, the system's performance will be evaluated in practical, real-world scenarios. By focusing on these areas, future work will enhance the effectiveness, adaptability, and integration of the proposed security system, ultimately providing a more robust solution for safeguarding physical money in vaults.

References:

- [1]. MoneyWise. (2023). *The 10 biggest bank robbery of all time, including who got caught and who got away*. MoneyWise. Retrieved from: <https://moneywise.com/life/entertainment/the-biggest-bank-robberies-of-all-time> [accessed: 10 May 2024]
- [2]. Alonso, M., & Campbell, J. (2024). *Burglars steal \$30 million in cash from a Los Angeles money storage facility – one of the city’s largest cash heists*. CNN US. Retrieved from: <https://edition.cnn.com/2024/04/04/us/la-bank-heist-money-storage-facility/index.html> [accessed: 12 May 2024].
- [3]. Koleka, B. (2014). *Betting the bank - the Albanian gambler who robbed the national vault*. Reuters. Retrieved from: <https://www.reuters.com/article/business/betting-the-bank-the-albanian-gambler-who-robbed-the-national-vault-idUSKBN0IS08S/> [accessed: 13 May 2024].
- [4]. Dutta, M., et al. (2020). Bank vault security system based on infrared radiation and GSM technology. *Intelligent Data Communication Technologies and Internet of Things: ICICI 2019*, 120-127. Springer International Publishing.
- [5]. Moon, M. M. H., et al. (2019). Design and implementation of a vault security system. *2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT)*, 1-6. IEEE.
- [6]. Bhatt, R., et al. (2018). 3 Tier Bank Vault Security. *2018 International Conference on Smart City and Emerging Technology (ICSCET)*, 1–4. IEEE.
- [7]. Chowdhury, T., Afrah, U., & Alam, J. F. M. J. (2020). A well-designed secure model for bank vault system. *Computer Science & Telecommunications*, 58(1).
- [8]. Okokpujie, K., et al. (2018). A bimodal biometric bank vault access control system. *International Journal of Mechanical Engineering and Technology*, 9(9), 596-607.
- [9]. Abdulla, A. I., et al. (2020). Internet of things and smart home security. *Technol. Rep. Kansai Univ*, 62(5), 2465-2476.
- [10]. Manohar, V. J., Paul, B., & Pranathi, M. S. (2023). A Novel Two Level Bank Security System using IoT based Controller. *2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 1282-1287. IEEE.
- [11]. Joy, M. H. C., et al. (2023). An IoT Based Smart Vault Security and Monitoring System with Zero UI. *2023 3rd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, 95-100. IEEE.
- [12]. Dobbins, A. H., & Henry, J. M. (2022). *Tamper detecting and inventory monitoring retail safe*. (U.S. Patent No. US11486188B2). United States Patent and Trademark Office. Retrieved from: <https://patentimages.storage.googleapis.com/bf/4a/44/a9d7de4019cc29/US11486188.pdf> [accessed: 04 June 2024].
- [13]. Trakhimovich, M. (2024). *System and method for weighing products on a shelf*. (U.S. Patent No. US11971293B2). United States Patent and Trademark Office. Retrieved from: <https://patentimages.storage.googleapis.com/64/35/11/7d1dfa7ebb5c64/US11971293.pdf> [accessed: 07 June 2024].
- [14]. Chan, P. K., Mahoney, M. V., Arshad, M. H. (2003). *A machine learning approach to anomaly detection (CS-2003-06)*. Melbourne, FL. Florida Institute of Technology.
- [15]. Gui, J., et al. (2024). A Survey on Self-supervised Learning: Algorithms, Applications, and Future Trends. *IEEE Transactions on Pattern Analysis and Machine Intelligence*.
- [16]. Bröker, F., et al. (2024). Demystifying unsupervised learning: how it helps and hurts. *Trends in cognitive sciences*.
- [17]. Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2024). Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms. *Sensors*, 24(2), 713.
- [18]. Adusumilli, S. B. K., Damancharla, H., & Metta, A. R. (2020). Machine learning algorithms for fraud detection in financial transactions. *International Journal of Sustainable Development in Computing Science*, 2(1).
- [19]. Ahsan, M., et al. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning— A Review. *Journal of Cybersecurity and Privacy*, 2(3), 527-555.
- [20]. Jamil, U. (2023). Load cell with Arduino Uno using HX711 amplification. *Peppe8o*. Retrieved from: <https://peppe8o.com/load-cell-with-arduino-uno-using-hx711-amplification/> [accessed: 18 June 2024].
- [21]. Asilian, A., & Zanjani, S. M. (2024). Application of Levenberg-Marquardt Backpropagation Algorithm in Artificial Neural Network for Self-Calibration of Deflection Type Wheatstone Bridge Circuit in CO Electrochemical Gas Sensor. *Majlesi Journal of Electrical Engineering*, 18(1), 21-32.
- [22]. Hajdarevic, K. (2024). IoT-Based Machine Learning System for Physical Intrusion Detection Using Dynamic Temperature and Humidity Observations With Raspberry Pi. *sensors*, 11, 12.