International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 11 Issue 11 ǁ November 2023 ǁ PP. 240-244

Optimizing Overtime Management: A Hybrid Approach with System-Level Checks and AI-Driven Anomaly Detection

Karthikeyan Manikam

Abstract
This paper addresses a critical issue in workforce management: unauthorized overtime. We investigate the challenges posed by employees or administrators authorizing overtime without fulfilling necessary regular hours, leading to potential financial losses and system exploitation. The paper outlines a multifaceted approach incorporating
system-level validations and machine learning (ML) to detect and prevent such occurrences. By leveraging an Isolation Forest algorithm, an unsupervised learning model, we propose a methodology to identify anomalies in overtime requests and implement an automated alert system for proactive oversight. The aim is to enhance transparency, ensure fair compensation, and uphold labor law compliance.
Keywords: *Unauthorized Overtime, Workforce Management, Machine Learning, Isolation Forest Algorithm, Anomaly Detection, Time and Attendance Systems, Labor Law Compliance, Financial Implications, System-Level Validation, Automated Alert System.*

Date of Submission: 09-11-2023 Date of acceptance: 23-11-2023

I. Introduction

The operational integrity of time and attendance systems is paramount in ensuring fair labor practices and safeguarding against financial discrepancies within an organization. The unauthorized allocation of overtime presents a dual challenge: financial implications for the company and compliance risks with labor laws. The prevalent occurrence of unauthorized overtime necessitates a robust solution that not only detects but also prevents such incidents proactively. By integrating advanced ML techniques with system-level safeguards, this paper proposes a solution that aligns with legal standards and promotes ethical workforce management.

Unauthorized overtime

An employee or admin can request 5 hours of overtime through the UI or self-reporting options. employee can also directly reach out to the Time admin to get the overtime authorized, even without having worked the regular hours required for overtime eligibility.

This situation poses a challenge as it allows associates or admins to potentially receive authorization for overtime hours without actually fulfilling the necessary regular hours. Such a practice could result in inaccurate overtime payments and potential exploitation of the system.

Alternatively, unauthorized overtime occurs when an employee works more than 40 hours in a single workweek without having requested it or had a manager agree to it in advance. According to the Fair Labor Standards Act (FLSA), employers are required to pay for these hours, even if they were not approved in advance. This can lead to significant financial losses for the company.

The total losses due to unauthorized overtime can vary depending on the number of employees involved, the frequency of the unauthorized overtime, and the rate of pay. For instance, if an employee routinely adds 10 minutes to each time card over a five- day work week, that's almost an hour of nonproductive time paid for. If that employee works 50 weeks each year, the time theft grows to about 41 hours — more than a week's worth of work. If your total labor costs are $30 per hour, time theft by that one employee costs you $1,230 each year.

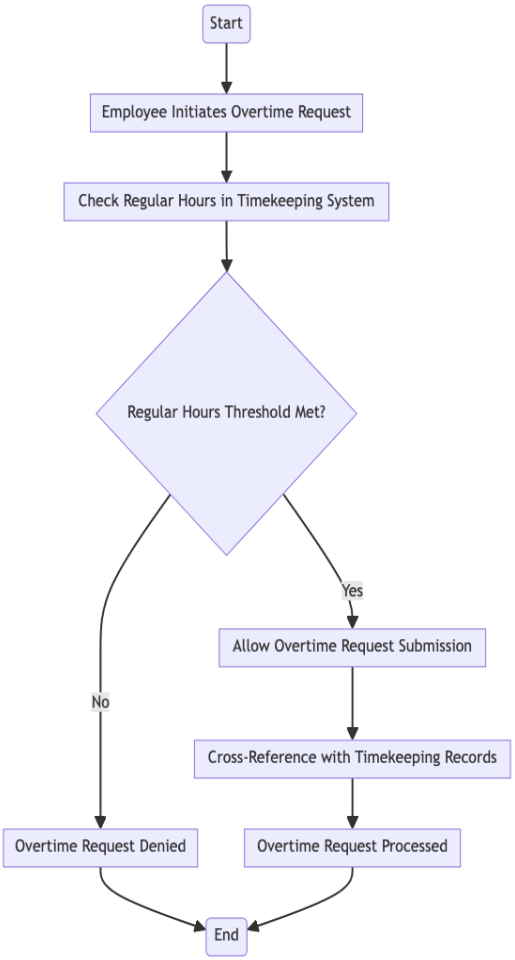
In some cases, unauthorized overtime can be a result of fraudulent activity. For example, three Department of Defense employees defrauded the federal government of more than $35,000 each for overtime that was falsely claimed.

In another case, employees providing logistics support at a South West Asia location were claiming excessive amounts of overtime compensation.

a city employee in New Haven was accused of collecting over $11,000 in overtime hours that weren't worked, which was more than half of the department's overtime budget.

In a specific case, the U.S. Postal Service reported that in FY 2019, 263,694 of their 633,108 career and non-career employees (42 percent) had unauthorized overtime. This led to significant costs, with penalty overtime costs ranging from $69.2 million to
$228.5 million in different fiscal years.
Unauthorized overtime can also strain both company resources and employee well- being. It can lead to higher costs, lower worker morale and productivity, and higher turnover.
The existing Time and attendance system does not have option
To prevent unauthorized overtime, To address this issue, we can consider a multi- faceted approach involving both system-level checks and ML/AI solutions system-level validation, ML-based anomaly detection, automated alert system, audit trails and reporting, predictive analysis, and role-based access control.

System-Level Validation
To ensure that overtime requests are legitimate and based on actual regular hours worked, we should implement system checks within the UI or provide self-reporting options that validate regular hours worked before allowing an overtime request. This proactive method could involve cross-referencing with timekeeping records or setting up rules that only enable overtime requests after a certain threshold of regular hours is recorded.



User Interface: The user interface for employee overtime requests should be designed to be clear and user-friendly. It should prominently display the number of regular hours worked in the current period.
Feedback Mechanism: If a request is denied or flagged, the system should immediately provide clear feedback to the user, explaining the reason (e.g., "Insufficient regular hours worked").
Dynamic Rules Adaptation: The system should be flexible enough to adapt to different employment contracts or departments within the organization, as overtime rules may vary. Since each employee group has its own overtime rules, the UI should provide suggestions based on individual employee pay contracts.

Data Synchronization: we should ensure that the timekeeping data is updated in real- time or near-real-time to avoid delays or discrepancies in processing overtime requests.

Processing Speed: The system should be capable of processing requests quickly to avoid workflow disruptions, especially in fast-paced work environments.

ML-Based Anomaly Detection

The ML-Based Anomaly Detection approach is a powerful tool for identifying irregular patterns in overtime requests and approvals, which could indicate misuse or errors in the system. Let's discuss the specifics of how this can be implemented.

To detect anomalies or unusual patterns in overtime requests that deviate from established norms, potentially indicating unauthorized or fraudulent activities, the goal is to enhance overall system integrity, improve oversight, and reduce the risk of financial loss due to incorrect overtime payments.

Choice of Machine Learning Algorithm

Unsupervised learning is a machine learning technique that allows a model to discover patterns and information in unlabelled data, without the need for input-to-output mappings or a provided teacher.

Unsupervised learning models are commonly used for three main tasks: clustering, association, and dimensionality reduction. Some of the most common algorithms used in unsupervised learning include clustering, anomaly detection, and neural networks.

Clustering is used to group datasets with shared attributes in order to extrapolate algorithmic relationships, while association mining identifies sets of items that often occur together in a dataset.

Isolation Forest -Unsupervised

Isolation Forest is an unsupervised learning algorithm and anomaly detection algorithm that identifies anomalies in data by isolating them in a tree structure.

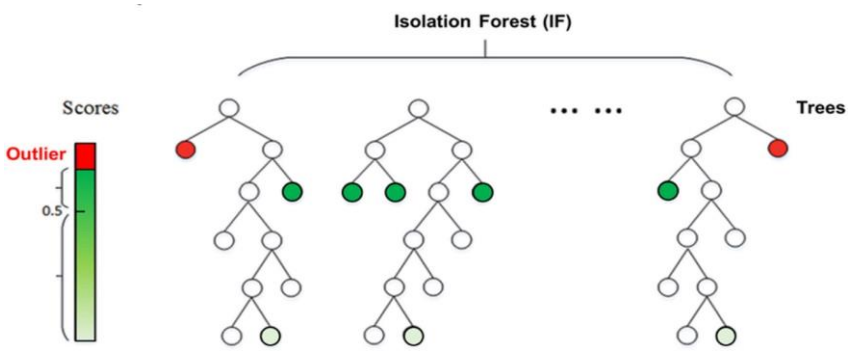
The algorithm is based on the principle that anomalies are few and different from the rest of the data, which makes them easier to identify.

Here's how the algorithm works: it randomly selects a feature and a split value, and then isolates the data points that fall below that value. This process is repeated recursively until the anomaly is isolated from the rest of the data. Isolation Forest is a tree-based algorithm that leverages the theory of decision trees and random forests. It is capable of detecting anomalies faster and with less memory compared to other algorithms.

Isolation Forest is implemented in an unsupervised manner, which means there is no actual "training" or input-to-output mappings to learn a mapping function. Instead, it identifies anomalies by isolating outliers in the data. Isolation Forest is widely used in various applications, including fraud detection, network intrusion detection, and preventative machine maintenance.

Tree Construction

The algorithm constructs multiple decision trees, known as an 'ensemble', wherein each tree isolates observations. The length of the path to isolate a point in the tree serves as a measure of its 'normality'. Shorter paths indicate anomalies.



Data Preparation: Collect relevant data for each overtime request, such as the number of regular hours worked, the department, the role of the employee, the time and frequency of overtime requests, and any previously identified anomalies.

Feature Selection: Choose features that indicate normal and anomalous behavior. For example, a high frequency of overtime requests, requests without corresponding regular hours, or irregular patterns in the timing of requests.

Training the Model: The Isolation Forest algorithm is applied to an overtime dataset. This algorithm creates decision trees, where each node splits the data based on selected features. Anomalies, which refer to unauthorized overtime requests, are isolated closer to the root of the tree, while normal points require more splits to be isolated.

Anomaly Score Calculation: Each overtime request gets an anomaly score. This score is based on the path length to isolate the point. Shorter paths result in higher scores, indicating a higher likelihood of being an anomaly.

We can set a threshold score that classifies a request as an anomaly. This threshold can be determined based on organization's specific context and tolerance for false positives.

Interpreting Results: Requests flagged as anomalies by the model should be further investigated. These may include cases where overtime was requested without sufficient regular hours or patterns that deviate significantly from the norm.

Continuous Improvement

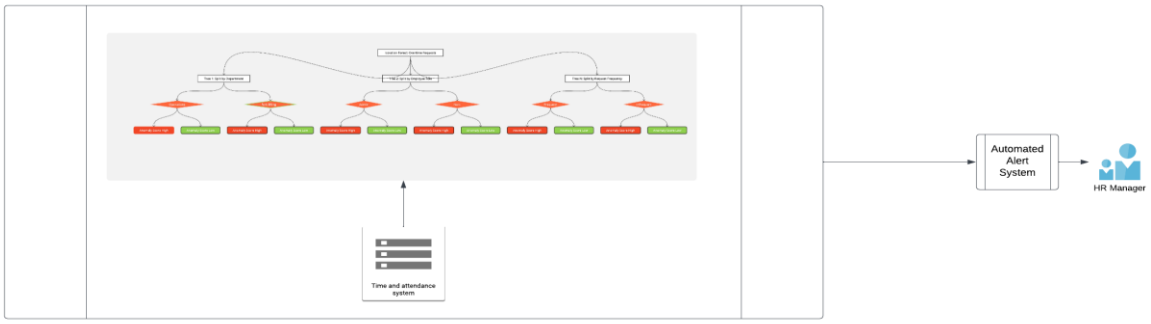
Regularly update the model with new data to capture evolving patterns in overtime requests.

Adjust the threshold and features as needed based on feedback from the investigations of flagged anomalies.

Advantages: Efficiency: The Isolation Forest algorithm is capable of efficiently processing large datasets, making it suitable for real-time or near-real-time anomaly detection.

Effectiveness: It is particularly effective in scenarios where anomalies are infrequent and not clearly defined, such as unauthorized overtime requests.

Scalability: The algorithm can handle an increasing number of features or growing data volumes without a significant impact on performance.



Automated Alert System:

To promptly inform supervisors or time admins about potential issues.

Create an automated system that sends alerts to relevant staff when an overtime request is submitted without corresponding regular hours. This system can be rule- based and integrated with the current timekeeping software.

Audit Trails and Reporting:

To maintain transparency and accountability in the overtime authorization process, it is important to log all overtime requests and authorizations with detailed audit trails.

Regular reports can then be generated and reviewed to identify any patterns of abuse or system loopholes.

Role-Based Access Control (RBAC):

To restrict the authorization of overtime and define the conditions under which it can be approved, we should implement Role-Based Access Control (RBAC) within Time and attendance system. This will ensure that only authorized personnel have the ability to approve overtime requests. Additionally, establish strict criteria for approval to further regulate the process.

II. Conclusion:

In conclusion, the unauthorized overtime issue presents a significant challenge that requires a sophisticated and integrated approach. The implementation of ML-based anomaly detection algorithms, such as the Isolation Forest, offers a promising solution to identify and prevent potential abuses in the system. The proposed automated alert system enhances the responsiveness of supervisors and administrators to anomalous events. Furthermore, system-level validation processes ensure compliance with labor laws and safeguard against financial losses. This comprehensive approach not only addresses the immediate concerns associated with unauthorized overtime but also sets a precedent for predictive and preventive measures in workforce

management systems.

Reference:

[1]. M. Alam, "Isolation Forest: A Tree-Based Algorithm for Anomaly Detection," Medium, Oct. 28, 2020. [Online]. Available: https://towardsdatascience.com/isolation-forest-a- tree-based-algorithm-for-anomaly-detection-4a1669f9b782.

[2]. "Anomaly Detection Using Isolation Forest in Python," Paperspace Blog, Mar. 2, 2020. [Online]. Available: https://blog.paperspace.com/anomaly-detection-isolation- forest/.

[3]. Office of Inspector General, "Assessment of Overtime Activity," 2020. [Online]. Available: https://www.uspsoig.gov/reports/audit-reports/assessment-overtime-activity.

[4]. A. Fortuna, "New Haven City Employee Receives Thousands in Fraudulent Overtime Payments: Warrant," NBC Connecticut, Apr. 14, 2023. [Online]. Available:

[5]. https://www.nbcconnecticut.com/news/local/new-haven-city-employee-receives- thousands-in-fraudulent-overtime-payments-warrant/3013834/.

[6]. S. Mazzanti, "'Isolation Forest': The Anomaly Detection Algorithm Any Data Scientist Should Know," Medium, Sept. 15, 2023. [Online]. Available: https://towardsdatascience.com/isolation-forest-the-anomaly-detection-algorithm-any- data-scientist-should-know-1a99622eec2d.

[7]. "Overtime," Worker.gov. [Online]. Available: https://www.worker.gov/pay-overtime/.

[8]. "Overtime Pay | U.S. Department of Labor," Dol.gov, 2019. [Online]. Available: https://www.dol.gov/general/topic/wages/overtimepay.

[9]. "Do You Have to Pay Employees for Unauthorized Overtime? - Quickbooks," Quickbooks.intuit.com. [Online]. Available: https://quickbooks.intuit.com/time- tracking/resources/overtime-laws-unauthorized-employee/.

[10]. K. H. Rhodes, "Managing Unauthorized Overtime: What Employers Can Do under the FLSA," Complete Payroll Solutions. [Online]. Available:

[11]. https://www.completepayrollsolutions.com/blog/unauthorized-overtime.

[12]. Homebase Team, "Unauthorized Overtime: What It's Costing You and How to Prevent It," Homebase, Jun. 28, 2023. [Online]. Available: https://joinhomebase.com/blog/unauthorized-overtime/.

[13]. "Unauthorized Overtime: Why It Happens and How to Prevent It - Shiftbase," Shiftbase.com. [Online]. Available: https://www.shiftbase.com/glossary/unauthorized- overtime.

[14]. "Unsupervised Fraud Detection: Isolation Forest," Kaggle.com. [Online]. Available: https://www.kaggle.com/code/rgaddati/unsupervised-fraud-detection-isolation-forest.

[15]. N. E. Kın, "What Are Isolation Forests?" Medium, Jun. 7, 2022. [Online]. Available: https://engineering.teknasyon.com/what-are-isolation-forests-151d8e98ef5f.

[16]. "How to Use the Isolation Forest Model for Outlier Detection," Practicaldatascience.co.uk, Mar. 14, 2021. [Online]. Available: https://practicaldatascience.co.uk/machine-learning/how-to-use-the-isolation-forest- model-for-outlier-detection. [Accessed: Day-Month-Year].

[17]. Liu, Fei Tony, et al. "Isolation Forest." 2008 Eighth IEEE International Conference on Data Mining, Dec. 2008, https://doi.org/10.1109/icdm.2008.17.