Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Next-Gen Exam Paper Protection: IoT Smart Lock with GPS, Biometrics & Anti-Tampering

Mohiyuddin Khan[1] and Ankur Khare[2*]

[1]*Research Scholar, Computer Science and Information Technology Department, Rabindranath Tagore University Raisen, Madhya Pradesh 464993, India*
Email ID: mkctakhan@gmail.com

[2]*Assistant Professor, Computer Science & Information Technology Department, Rabindranath Tagore University, Raisen, Madhya Pradesh 464993, India*
**Corresponding Author Email: khareankur94@gmail.com*

ARTICLE INFO

Received: 26 Dec 2024

Revised: 14 Feb 2025

Accepted: 22 Feb 2025

ABSTRACT

The examination is a crucial part of the education system for determining students' abilities and could be the main focus of the overall structure. Every year, we heard of exam cancellations or postponements caused by paper leaks. To accomplish a compact and manageable result, we have decided to develop and implement a "transported printed question paper in a secured way." This is to avoid leakages and protect the question box during the transportation. This will be a very secure system that uses tamper-detection module, GPS tracking, biometric authentication, and central server-based fraud detection. The paper presents a robust Internet of Things-based solution that integrates modern technology to ensure that only authorized individuals (Exam Coordinator and Exam Incharge) can access the question papers box on the designated exam day. One such feature is biometric verification, and real-time location monitoring can be achieved with GPS tracking, and tamper-detection module can identify physical tampering or unwanted access while in transit. IoT device data is processed by a central server, which then creates alerts for quick action in the event of abnormalities like route deviations, tampering attempts, or unauthorized access. The system's design ensures the confidentiality and reliability of information by securely transmitting encrypted data. By integrating these features, the proposed approach offers an extensive approach for protecting the handling and transportation of printed questions, reducing risks, and ensuring a secure and efficient examination process.

Keywords: GPS tracking, Biometric verification, Tamper-detection module, Central server-based fraud detection

INTRODUCTION

Security is the continuous process of protecting an organization, which could be a person, a business, or property. In society, education will be the vital role. Examinations are essential for evaluating and verifying academic success since education is the foundation of growth for individuals as well as society. Exams may be given on paper, and maintaining printed question papers safe during transportation is essential for protecting the reliability and validity of assessment systems worldwide.

Fundamental problems for students, however, include "exam paper leakage," which results from exam cancellations or postponements. Every year, we compile information about things like exams that have been postponed or canceled due to paper leaks in the daily paper or on television [6]. The majority of paper leak cases are found to occur during the transit of papers, and the individuals involved in the distribution and transportation of papers are typically the perpetrators. Therefore, the present offline system is no longer reliable, and it is essential to improve paper security both during transportation and during storage before the start of the exam [7]. In this paper, we proposed and developed a smart question paper box so that question papers can be handled and transported safely while maintaining their security and legitimacy. Traditionally, manual procedures and basic security measures like sealed envelopes and reliance on human inspection have been used to secure question papers [8]. However, these traditional approaches do have problems, particularly in large-scale examination circumstances when logistical complexity increases significantly. Unauthorized access, manipulation, or misplacement during transportation could be the result of deliberate fraud or human error.

The advent of modern technologies such as biometric identification, real-time data analysis, and the Internet of Things (IoT) presents opportunities to mitigate these risks and modernize existing systems to ensure the safe transmission of questions and boxes. The system architecture (Fig. 1) ensures the seamless integration of IoT-based technologies and security measures to maintain the integrity, reliability, and trustworthiness of the examination process.

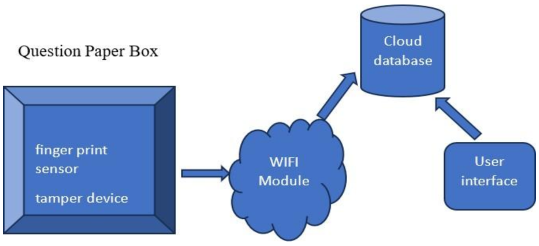

Figure 1: System Architecture

IoT technologies offer a revolutionary solution by enabling intelligent automation and real- time monitoring. Connect devices like GPS trackers, biometric systems, and tamper-detection methods to create a safe and efficient transportation network [9]. GPS tracking, which ensures continuous position monitoring of the transportation, allows authorities to trace the movement of question papers and respond to any deviations from the intended route. Additionally, by ensuring that only authorized personnel can access the question papers during critical periods, such as dispatch and delivery, biometric authentication removes the possibility of unauthorized access. The tamper-detection module plays a crucial role in protecting question papers while they are in transit. Abnormal physical damage to the box can be quickly identified and flagged, as can tampering attempts, by using advanced packaging materials and sensors that detect physical changes. A central server-based monitoring system in conjunction with these systems enables real-time fraud identification. In the event that an unauthorized access attempt is detected or the device deviates from the intended path, for instance, notifications can be given to enable examination authorities [10]. This paper proposes a sophisticated Internet of Things- based structure that integrates biometric identity, GPS tracking, a tamper-detection module, and fraud detection to provide a reliable framework for the secure handling and transit of question paper boxes. By addressing the drawbacks of traditional methods and using modern technology, the proposed approach ensures the integrity, traceability, and security of question papers throughout the transit process. This paper aims to assist in the development of a reliable examination environment and increase public confidence in examination systems. This system's implementation can serve as a model for educational institutions worldwide by ensuring fair and trustworthy examination processes.

Objective of this Paper

The main objective of this paper is to develop and design an Internet of Things-based framework that will enhance the integrity and security of printed question paper boxes during transportation and handling. The following are the basic objectives:

- To enable continuous tracking of the question paper box's location throughout transit, use GPS tracking devices.

- To ensure that only those with the appropriate authorization may access the question papers, fingerprint devices & tamper detection modules will be interfaced with location tracking in such a way that opening the box should be done in specific location and time, in which creating and include biometric authentication technologies will be an added benefactor for our product.

- Add tamper-detection module with sensors to detect and alert to relevant authorities for any physical changes, that can compromise the security of the question papers.

- Establish a centralized server-based monitoring system that can immediately create notifications to the relevant stakeholders in the case of a security abnormality, such as route deviations, tampering events, or unauthorized access attempts.

- By providing a dependable, safe, and traceable solution that prevents paper leaks and ensures unbiased and trustworthy evaluation processes, this can promote confidence in exam systems.

Problem Statement

Transporting and handling question papers in a box safely is essential to maintaining the validity, reliability, and integrity of examination systems. However, traditional methods that rely on manual processes, human oversight, and basic security measures like sealed envelopes are more vulnerable to security breaches. Problems including unauthorized access, manipulation, misplacement, and paper leaks during transit not only disrupt exams but also damage public confidence in the educational system.

Key challenges associated with the current approach include:

- Human Error and Malpractice: When transporting the question papers box, there is a higher likelihood of intentional fraud or accidental misuse. Numerous cases of paper breaches have been connected to workers involved in the transportation process.

- Lack of Real-Time Monitoring: It may be difficult to spot delays, illegal behavior, or route deviations while traveling because traditional forms of transportation lack real-time surveillance or monitoring.

- Tampering and Security: Traditional sealed packaging is insufficient to prevent tampering. Often, attempts to physically alter the contents or access them are ignored until it is too late.

- Absence of Automated Fraud Detection: Existing systems lack intelligent methods to identify and respond to fraud such as tampering, route deviations, or unauthorized access attempts.

- Impact on Examination Systems: Paper leaks and other security problems cause exams to be canceled or postponed, which stresses students, costs educational institutions money, and damages the reputation of testing boards.

Given these challenges, a modern, technologically advanced solution to protect the question papers box while in transit is essential. By integrating modern technologies like biometric authentication, GPS monitoring, tamper-detection module, and centralized fraud detection, the suggested IoT-based architecture reduces these weaknesses and ensures a safe, reliable, and verifiable system for question paper transportation.

LITERATURE SURVEY

According to research by Deebak, B. D., & Hwang, S. O. (2023), tamper detection is another crucial element of safe package transportation. Tamper-detection module has been the subject of several studies as a means of detecting inappropriate handling or access. Sensors integrated within the packaging materials allow for real-time tracking of the integrity of shipments throughout transit. According to a study published in Sensors, data in Internet of Things systems is secured using lightweight authentication frameworks. It is possible to adapt these systems to monitor the condition of packages, ensuring that any attempts at tampering will instantly trigger an alarm [1]. Secure data transfer is essential for preventing unwanted access to private information while packages are being transported, claims researcher Aljumah, A. (2024). End-to-end encryption methods like TLS and AES-256 are the main focus of Sensors and PMC research in order to facilitate safe communication between IoT devices and central servers. To prevent sensitive data tampering and illegal eavesdropping, these protocols are essential for sending biometric information, real-time location data, and tamper alerts[2]. Real- time breach and cyberattack detection is a state-of-the-art method of cybersecurity in Internet of Things systems, claim Alsheikh, M. A., and Khoa, T. V. (2024).

Federated learning for cyberattack detection in blockchain-based data-sharing networks is examined in a study, which also offers insights into how these models might be applied to protect package delivery. By using machine learning algorithms to find patterns suggestive of attacks, this research helps create secure and reliable IoT-based package transport systems. Real-time package tracking using GPS technology has become the industry standard to avoid theft and loss of critical items [3], in accordance with Ozdemir, Z., & Tugrul, B. (2019) [4]. The importance of GPS tracking in giving constant visibility of objects in transit has been emphasized, which enhances the capacity to monitor and react to any security risks. By establishing virtual boundaries around transit routes, geofencing technologies have also shown promise in alerting stakeholders when a product veers off course. Combining GPS monitoring with geofencing improves security by sending out real-time alerts when packages enter regions that are forbidden or disapproved.

According to research by Haque, S., Zeba, S., and Haque, M. A. (2021), exam fraud is a problem in Indian institutions that threatens the integrity of academic assessments and the educational system. This paper addresses this issue. It proposes an Internet of Things-based approach to detect and prevent exam misbehavior by using sensors to identify illegal metallic objects or items outside the usual range of infrared proximity sensors. The book provides detailed instructions for implementing this paradigm, together with a block diagram and circuit architecture. By enhancing exam security and fairness, the proposed approach aims to maintain the integrity of academic assessments and promote trust in the educational system.

METHODOLOGY

System Implementation

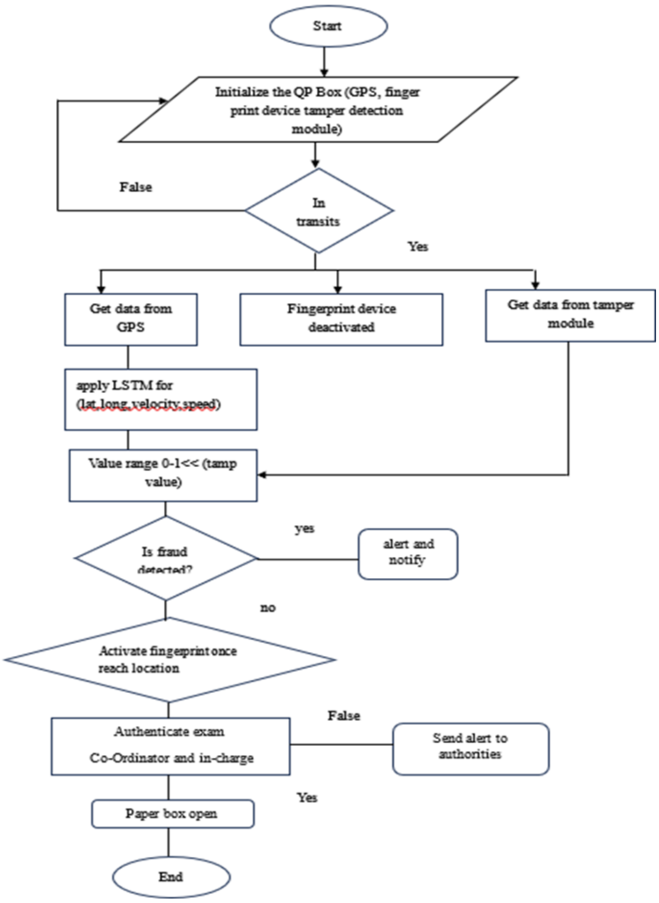
Start
Initialize the QP Box (GPS, finger print device tamper detection module)
False
In transits
Yes
Get data from GPS
Fingerprint device deactivated
Get data from tamper module
apply LSTM for (lat,long,velocity,speed)
Value range 0-1<< (tamp value)
yes
Is fraud detected?
alert and notify
no
Activate fingeprint once reach location
False
Authenticate exam Co-Ordinator and in-charge
Send alert to authorities
Yes
Paper box open
End

Figure 2: The flowchart represents the working of the system

This section presents an overview of the system implementation (Fig. 2) and a detailed description of the proposed IoT-based question paper transportation system. the system include location monitoring, strong sensors for detecting tampering, and fingerprint recognition. It monitors the box's integrity to ensure that it cannot be opened without authority. It also keeps track of the question paper box's present location using a GPS tracker. All of this data is sent to the cloud server. The real-time updates through approved web and smartphone logins allow all stakeholders to receive notifications about any significant events that take place as well as every predefined condition of the process in order to preserve the integrity of the question paper transportation.

GPS Tracking for Real-Time Location Monitoring

The GPS tracking technology ensures real-time location monitoring of the question paper box during transportation by integrating a GPS module within the packaging. This module continuously captures and transmits location data to a cloud server over Wi-Fi or cellular networks, allowing authorities to track the box's movement in real time. To increase security, geofencing technology establishes virtual boundaries along the transit path. In the case that the box deviates from the intended path or reaches restricted regions, an instant alert is sent out, allowing for immediate action. Additionally, the system includes offline capabilities, where the GPS module stores position data locally during network failures and uploads it to the cloud once connectivity is restored. This continuous tracking technology ensures secure and efficient transit while reducing the possibility of tampering or unauthorized access [11].

Tamper-detection module

Tamper-detection module ensures the integrity and safety of the question paper box during transportation by utilizing advanced tamper-detection module. These sensors can identify physical damage, vibrations, unusual temperature fluctuations, and unauthorized access. If the technology detects any effort at tampering, it immediately notifies the central server. Simultaneously, the relevant authorities receive real-time notifications, enabling timely action to prevent potential fraud activities. This robust solution reinforces the reliability of the transit operation while reducing the likelihood of question paper leaks or unauthorized handling.

Biometric Authentication Process

The biometric authentication method uses fingerprint recognition technology (Figure 1) to give authorized people safe access to the printed question papers box. The exam coordinator and exam in charge must register their biometric data, including fingerprints, which are safely kept in the system, before the exam day. An optical fingerprint reader built within the question paper box on the examination day confirms both the identities of individuals. They have to use the device to scan their fingerprints for authentication. the system verifies the input against the pre-registered biometric data and checks the location. The technology automatically opens the box and makes the question papers available for distribution after the authenticate people have been successfully verified. By preventing unwanted access, this dual-authentication system improves the security and integrity of the examination procedure.

User Interface

To ensure the secure and transparent handling of printed question papers, the proposed system makes use of robust data security measures and real-time monitoring. A mobile or web-based application that provides real-time information on the transportation and unlocking process allows stakeholders to track the location of the question paper box on a map in real time [12]. The system also immediately alerts users in the event of significant factors, such as tampering, unauthorized access attempts, or deviations from the intended path, to ensure prompt action. To protect data security and confidentiality, all information transmitted from IoT devices— such as GPS trackers, tamper-detection module, and biometric scanners—to the central cloud server is encrypted via TLS.

Structured Security Framework for Question Paper Box

The question paper box is structured into three parts, including the transport phase, the exam day phase, and the monitoring and Fraud detection phases, to ensure security, integrity, and efficacy:

A. Transport Phase: During this stage, the question paper box is securely transported to the designated examination location. The box is equipped with GPS tracking and tamper-detection module to ensure its integrity while in transit. GPS tracking allows for real-time location monitoring, and tamper-detection module can identify physical damage or unauthorized entrance. Importantly, there is no requirement for biometric authentication during transportation, allowing for seamless mobility while maintaining excellent security.

B. Exam Day Phase: On the day of the examination, the exam coordinator and exam in charge must physically appear at the examination location. Both Exam Coordinator and Exam In-charge must authenticate themselves using their already registered biometric data, such as fingerprints, via biometric scanners integrated into the question paper box. The system verifies their identities using stored data. Once both individuals have properly authenticated, the system opens the box, allowing the printed question papers to be safely delivered.

C. Monitoring and Fraud detection: Fraud detected, such as tampering attempts or deviations from the predefined transit path, immediately causes alerts to be produced via LSTM module. The real-time transmission of these signals to the relevant authorities ensures the prompt response. In the above stages, the system makes use of continuous monitoring supported by a central server-based analysis.

Central Server-Based Fraud Detection (CSFD)

The central server serves as the main hub for processing and analyzing data from Internet of Things devices, such as GPS trackers, biometric scanners, and tamper-detection module. It uses fraud detection to aggregate this data in real-time to identify anomalies, such as route deviations or attempts at manipulation. When the server notices any suspicious activity, it notifies the relevant authorities right away and sends out alerts. To ensure secure data storage and transfer, the system makes use of robust encryption techniques. Private information, such as biometric data and tamper alerts, is protected from unauthorized access by the encrypted data exchanged between IoT devices and the central server. Data in transit is protected by transport layer protection (TLS), which provides an additional layer of protection during communication. The security and integrity of critical data throughout the system are ensured by these protections.

Using the LSTM model for fraud detection in question paper transportation involves a, number of several steps, which are described below.

A. LSTM Architecture

LSTM is a special kind of RNN that can retain a lot of information over a long period of time. It was developed to handle sequential data and effectively address the problem of vanishing gradients that traditional RNNs face. First introduced by Hochreiter and Schmidhuber in 1997, LSTMs are particularly helpful for applications requiring long-term dependencies, such as time series forecasting, speech recognition, and natural language processing (NLP).

Figure 3 illustrates the LSTM network, which is made up of a memory cell that holds data that is updated by three unique gates: the input gate, the forget gate, and the output gate. The three gates control the information flow into and out of the cell, and the cell retains values for arbitrary periods of time.

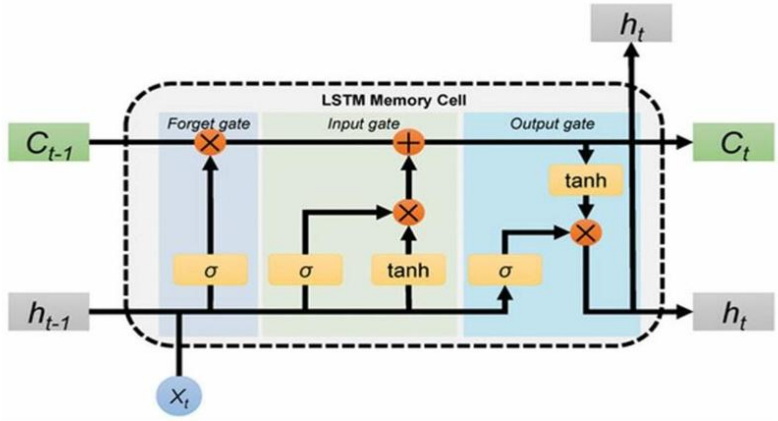

Figure 3: LSTM architecture

The structure of the LSTM network is made up of memory blocks, or cells, with numerous states. The cell state is the primary information flow chain. It allows information to flow forward unchanged. The forget gate (f_t) determines what information should be kept or erased. The sigmoid function receives data from the previous hidden state (h_{t-1}) and data from the current input (x_t). The sigmoid function (σ) determines values between 0 and 1; forgetting is indicated by a value nearer 0 and keeping is indicated by a value nearer 1. Furthermore, the cell state vector C_{t-1} controls the elements that will be forgotten.

The following are the steps for detecting fraud using the LSTM method:

1. Input Data Representation

At each time step t, the input to the LSTM model consists of the following features:

- Location (latitude and longitude)
- Velocity (speed or distance between consecutive locations)
- Frequency (transaction frequency or intervals) Thus, the input vector represents as:

x= [lat,lon,velocity,frequency]

2. LSTM Recurrence Equations

1. **Forget Gate:** it decides which historical facts should be forgotten. The equation1 explain how forget gate is calculated

$$f_t = \sigma(W_f.[h_{t-1},x_t]+b_f) \quad (1)$$

Where, W_f= Weight matrix for the forget gate

b_f= Bias term

σ= Sigmoid activation function

2. **Input Gate:** The equation2 determines which part of the current input to store in the cell state.

$$i_t=\sigma(W_i. [h_{t-1},x_t]+b_i) \quad (2)$$

3. Candidate Cell State: The equation3 represents the calculated new potential values added to the cell state.

$$\tilde{C}_t=\tanh(W_C. [h_{t-1},x_t]+b_c) \quad (3)$$

Where, W_i, W_C = Weight matrices

b_i, b_c = Bias terms

h_{t-1} =The previous time step's hidden state, which contains short-term memory.

$\tilde{C}_t$ =This is the candidate cell state at time step t. It includes fresh data that was obtained from the previous hidden state and the current input.

tanh =The hyperbolic tangent activation function ensures that $\tilde{C}_t$ values range within the range of -1 to 1. This stabilizes learning and manages gradient flow.

4. **Cell State Update:** Equation 4 represents combining the new candidate with the previous memory.

$C_t=f_t. C_{t-1}+i_t. \tilde{C}_t$ (4) Where, C_t= Updated memory cell state

5. **Output Gate:** the output gate O_t determines It decides which cell state component is transferred to the hidden state h_t through the output of the sigmoid gate and with new values generated by tanh from cell state as in equation 5-6.

$$O_t= \sigma(W_O.[h_{t-1},x_t]+b_O) \quad (5)$$

$h_t = O_t.\tanh(C_t)$ (6) Where, h_t=Updated hidden state

3. Output Layer for Fraud Detection

After the LSTM network's processing of the location data, the final hidden state h_t is sent to a fully connected layer for classification. The output layer determines the probability of fraud at time step t as in equation7.

The output is $\hat{y}_t = \sigma(W_y.h_t + b_y) << T_i$ (7) Where, $\hat{y}_t$= the predicted fraud probability.

W_y =the weight matrix for the output layer.

b_y=the bias for the output layer.

T_i= Tamper detection module

σ= The probability of fraud is represented by the sigmoid activation function, which yields a value between 0 and 1.

These equations enable LSTMs to detect long-term correlations, which makes them useful for detecting fraud in systems that rely on geolocation.

Finger print module

The system will track location and identify fraud detection after proceeding with fingerprint authentication for access control. Once these checks are completed, the fingerprint (FP) module will be activated based on predefined source and destination parameters, considering both location and real-time constraints. Every fingerprint template has a unique ID that will be acquired during the authentication process. When a user places their finger on the sensor, the system will compare the captured fingerprint with the current database. If a match is detected, the matching ID will be returned; if not, -1 will be returned. Our proposed method verifies the exam coordinator and exam in-charge using biometrics. Until they have successfully authenticated with the relevant IDs, the question box will not be enabled.

Graph Representation

The graph presents Fraud Detection by displaying both predicted and actual fraud probabilities over various time steps.

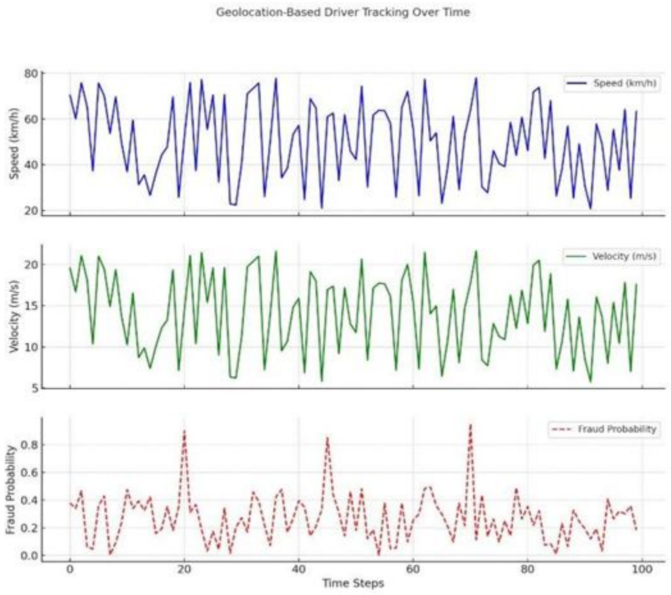

Figure 4 (a): Geolocation-Based Driver Tracking

The three line graphs in the figure4 (a) "Geolocation-Based Driver Tracking" set that are presented show different metrics that have been tracked over a hundred-time steps, providing information about driver behavior and possible fraud detection. In the first graph, which is displayed in blue and displays speed in kilometers per hour (km/h), the driver's speed fluctuates between around 30 and 70 km/h, with frequent peaks and troughs signifying changes in driving habits. The second graph, which is drawn in green and shows velocity in meters per second (m/s), shows that the driver's velocity fluctuated significantly between around 7 and 20 m/s. Finally, the third graph, which is titled "Fraud Probability" and shows the likelihood of fraud by bouncing between 0 and 0.8, is shown with a red dashed line.

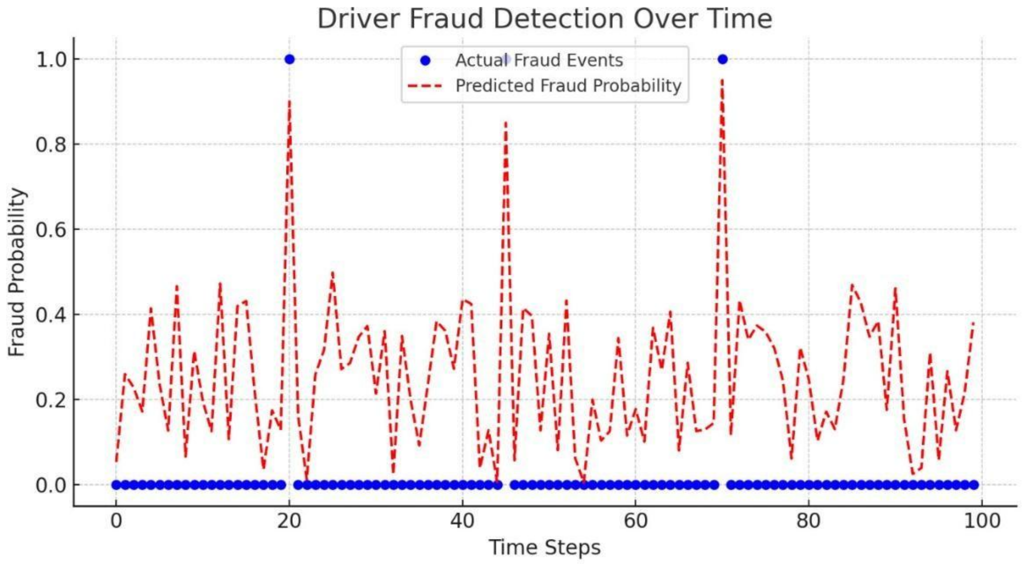

Figure 4(b): Driver Fraud Detection

The "Driver Fraud Detection " graph figure 4(b) shows the actual fraud incidents and the anticipated fraud probability across a number of time steps. Time steps are shown on the x- axis, and the fraud probability, which ranges from 0 to 1, is shown on the y-axis. A number of 1 denotes proven fraud, while a value of 0 indicates no fraud. The blue dots show genuine fraud events. The shown fraud probability produced by the fraud detection model is shown by the red dashed line. The fraud probabilities in the model fluctuate, with multiple sharp peaks indicating possible fraudulent activity. Some of these peaks seem to be false positives, where the model predicts fraud but no event actually happens, while others correspond with real fraud instances. On the other hand, false negatives occur when there is genuine fraud but the probabilities of it is still minimal. These differences point to possible ways to increase the model's accuracy, such adjusting detection thresholds, improving feature selection, or adding more training data. All things considered, the graph provides a spotlight on the model's effectiveness, highlighting its benefits as well as limitations in spotting fraudulent activity.

CONCLUSION

Using an Internet of Things-based security system is a reliable and effective way to protect printed exam papers during transportation. By integrating features like tamper-detection module, GPS tracking, biometric authentication, and central server-based fraud detection, the system ensures that only authorized personnel can access the question papers on exam day. Through proactive danger identification and real-time monitoring, it safeguards the confidentiality and integrity of the testing process. Its scalability and flexibility allow it to adapt to emerging security issues, making it a comprehensive and future-ready solution for educational institutions. This approach provides a significant improvement in preventing paper leaks and ensuring a safe examination process.

REFERENCES

[1]. Deebak, B. D., & Hwang, S. O. (2023). Federated Learning-Based Lightweight Two-Factor Authentication Framework with Privacy Preservation for Mobile Sink in the Social IoMT. Electronics, 12(5), 1250. https://doi.org/10.3390/electronics12051250.

[2]. Aljumah, A. (2024). UAV-Based Secure Data Communication: Multilevel Authentication perspective. Sensors, 24(3), 996.https://doi.org/10.3390/s24030996.

[3]. Khoa, T. V., Alsheikh, M. A., Alem, Y., & Hoang, D. T. (2024). Balancing Security and Accuracy: A novel federated learning approach for cyberattack detection in blockchain networks. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2409.04972.

[4]. Ozdemir, Z., & Tugrul, B. (2019). Geofencing on the Real-Time GPS Tracking System and Improving GPS Accuracy with Moving Average, Kalman Filter and Logistic Regression Analysis. 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 1–6. https://doi.org/10.1109/ismsit.2019.8932766.

[5]. Haque, S., Zeba, S., Haque, M. A., Kumar, K., & Basha, M. P. A. (2021). An IoT model for securing examinations from malpractices. Materials Today Proceedings, 81, 371–376. https://doi.org/10.1016/j.matpr.2021.03.413.

[6]. Mishra, V., & Yadav, M. K. (2022). IoT based Smart Transportation System: Implementation and Security Challenges. International Journal of Vehicle Structures and Systems, 14(5). https://doi.org/10.4273/ijvss.14.5.03.

[7]. Jaiman, A., Sharma, A., Jaiman, V., & Porwal, N. (2023). Secured transportation and distribution of examination papers using IOT and AI. Research Square (Research Square). https://doi.org/10.21203/rs.3.rs-2682795/v1.

[8]. Oladimeji, D., Gupta, K., Kose, N. A., Gundogan, K., Ge, L., & Liang, F. (2023). Smart Transportation: An Overview of technologies and applications. Sensors, 23(8), 3880. https://doi.org/10.3390/s23083880.

[9]. Haque, S., Zeba, S., Haque, M. A., Kumar, K., & Basha, M. P. A. (2021b). An IoT model for securing examinations from malpractices. Materials Today Proceedings, 81, 371–376. https://doi.org/10.1016/j.matpr.2021.03.413.

[10]. Roseela, J. A., & Godhavari, T. (2020). Biometric and RFID based authentication system for exam paper leakages detection using IoT technology. Indonesian Journal of Electrical Engineering and Computer Science, 20(3), 1271. https://doi.org/10.11591/ijeecs.v20.i3.pp1271-1277.

[11]. Wankhade, Pravada P., and S. O. Dahad. "Real time vehicle locking and tracking system using GSM and GPS technology-an anti-theft system." International Journal of Technology And Engineering System (IJTES) 2.3 2011.

[12]. Godavarthi, Bhavana, Paparao Nalajala, and L. R. Teja. "Wireless sensors based data acquisition system using smart mobile application." Internet of things,"International Journal of Advanced Trends in Computer Science and Engineering 5.1): 25-29. 2016

[13]. T. Petrov, M. Dado and K.E. Ambrosch. 2017. Computer modelling of cooperative intelligent transportation systems, Proc. Engg., 192, 683-688. http://dx.doi.org/10.1016/j.proeng.2017.06.118.

[14]. Y. Agarwal, K. Jain and O. Karabasoglu. 2018. Smart vehicle monitoring and assistance using cloud computing in vehicular Ad Hoc networks, Int. J. Transp. Sci. Tech., 7, 60-73. https://doi.org/10.1016/j.ijtst.2017.12.001.

[15]. M. Babar and F. Arif. 2019. Real-time data processing scheme using big data analytics in IoT based smart transportation environment, J. Ambient Intelligence and Humanized Computing, 10, 4167-4177. https://doi.org/10. 1007/s12652-018-0820-5.