International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 16 (2024) pp. 366–377
© Cerebration Science Publishing

Article

Safeguarding Women: IoT-Enabled Machine Learning Approach for Threat Detection via EEG and Eye Blink Signals

Leena Arya * and Yogesh Kumar Sharma

Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, AP 522 302, India; dr.sharmayogeshkumar@gmail.com
* Correspondence author: leenaarya18@gmail.com

Received date: 6 March 2024; Accepted date: 21 March 2024; Published online: 10 July 2024

Abstract: The gender violence problem and high level of harassment is significant all over the world requiring new mechanisms to be developed to enhance women's safety and security. This paper aims to present a new methodology for the security increase of women based on the combination of the Internet of Things (IoT) technology and machine learning algorithms to detect threats in real-time with physiological signals from the sensor. The system employs wearable Electroencephalography (EEG) sensors and eye blinking as physiological markers of stress, the system provides real-time identification and responses to threats. A machine learning model, trained on a data set that has already been labeled, processes these signals in real-time and identifies patterns that are linked to fear or anxiety. The model then interprets these patterns to indicate a threatening situation. Upon detection of an intruder, the pre-programmed actions will take effect. The system featuring IoT connectivity and modern machine learning creates a security arrangement responsive to all scenarios with dynamic safety measures, thus empowering women. The actions may vary from notifying the emergency services, the authorities, or even the smart home devices for immediate intervention. This paper describes the system architecture, proposed methodology, ethical considerations, and future research directions, illuminating its possibility to improve safety and create a more secure world for women globally.

Keywords: IoT; EEG; eyeblink signals; violence against women; wearable devices; sensor data; artificial intelligence (AI)

1. Introduction

The violence against women (VAW) haunts the world, depriving people of millions of norms, and the achievement of gender equality. The stark reality is painted in chilling statistics: approximately 1 out of 3 women in the world, or 736 million, have experienced physical or sexual violence at the hands of their intimate partner or a non-partner [1]. Mathematically, this constitutes 243,000 women and girls who lose their virtues every year, with nearly one death every hour [2]. However, the discrimination is not over, because eight hundred and eighteen million women are being deprived of their mobility and sense of security across the globe by men harassing them and stalking them [2]. These numbers are far from being mere statistics. They signify the experience of millions of women who attend to their daily duties while contending with the daily threats and having the constant fear of being hurt forcibly [3,4].

Addressing the issues with efficient approaches is indisputable. Even though conventional security measures have failed us many times, the various advances in technology give hope. This research paper explores the prospect of an innovative shift that uses the Internet of Things (IoT), machine learning (ML), and big data to improve women's safety and fight violence against women around the world [5–7]. The proposed system connects EEG and blink-detecting wearables with ML algorithms for real-time threat detection. With such signals, the system defines the stress-related patterns that could signal an emergency. This paper examines the technical viability of this method where the challenges related to data privacy, security, and fairness of algorithms are also discussed. In addition, it also discusses the ethical issues of informed consent, transparency, and accountability.

Even though there are many challenges, there are also numerous opportunities that could result from this process. Early detection of potential threats can amount to this empowerment, which often can be a decisive factor when it comes to beating assault rates. In addition, the system's visibility could likely make offenders think twice and attract bystanders to put in action, thus leading to safe places for women on a global scale. However, the long-term implications of this technology include more comfort and high self-esteem in women [8,9] and confidence to live without restraints. Nevertheless, we must understand the importance of the responsibility that belongs to the new technological developments. The eagerness to apply the technology in an accountable and aligned manner with an ethical framework is to guarantee that the tech serves its intended purpose while upholding human rights and rights to equality.

2. Literature Survey

In recent years, efforts towards improving women's security using creative tools and methods have accelerated, with special attention paid to using Electroencephalogram (EEG) signals. In this area, several prominent issues are discussed, that provide positive approaches to improving women's safety and well-being.

Singh, H., Singh, J., et al. [10] proposed a real-time eye blink detection methodology that is robust enough to detect blinking either in the controlled or natural environment, Their method recorded 96%, 92%, and 88% success in detecting left winks, right winks, and blinks, and it is therefore possible to apply it to the real world with promising results.

According to Yasoda, K., et al. [11], a fuzzy kernel support vector machine was suggested for the automatic categorization of WICA artifacts in the EEG signals. Using this technique overtly enhances the quality of artifact component detection and leads to an impressive classification accuracy of 86.1%, which unfolds the powerful tool for EEG preprocessing in security applications designed for women.

Sivachitra, M., et al. [12] were concerned about the safety of women and decided to develop an autonomous women's safety patrolling Robotic system. By integrating sound sensors, ultrasonic sensors, ESP cameras, and IoT technologies, their system diminishes the need for human interventions, thus making the night patrol fly-by activities very efficient and resolving the community safety issue at the same time.

Also, Nivedetha, B. et al. [13] presented an all-around safety system using sound sensors, ultrasonic sensors, ESP cameras, and IoT capabilities to detect and prevent crimes against women. The focus is on detective and preventive actions. The system developed by making wearable technology and integrating encrypted IoT communication enables women to work the risky situations confidently.

Tayal, S., and others [14] improved the prototype of a cost-effective women's safety device, including GSM, NodeMCU, and GPS modules. The device locates women in distress quickly & sends an SOS message by pressing the panic button to pre-set contacts & nearby authorities thus responding speedily and with comprehensive protection.

K. Hariharan et al. [15] suggested a machine learning-powered app that features an auto emergency alert button and location monitoring. A feature auto mode for emergency cases and with SVM classification they have managed to get an accuracy of 89.5% which is amazing.

In addition, Gomathy, C.K., and M.S. Geetha [16] presented a smart wearable device for women, controlled with Arduino and which at the push of a button gets them in touch with the authorities and emergency contacts. The device with these functionalities - GPS and GSM, allows vital features to be managed efficiently and timely for emergency needs.

Li et al. [17] presented an innovative fatigue detection technique that uses facial features. They implemented a unique method using recurrent gate unit (GRU) and ensemble facial attributes data, an MTCNN model that integrates with a multi-task convolutional neural network (MTCNN). They rely on the adaptation prediction of driver fatigue levels to achieve the high accuracy of 97.47% which is the right approach to providing the best for their users.

Wijnands et al. [18] created a dynamic sleep monitoring system for a driver's drowsiness detection on mobile systems. This system utilizes a three-directional neural network and collects features and patterns of the face and expressions by inducting the wireless sensors. Integration of spatial and temporal data allows the system to produce the optimal datasets that are used in the monitoring processes, therefore, notable performance and efficiency improvements have been achieved with an accuracy of 98.03% for detecting driver drowsiness.

3. Threats for Women in Today's Environment

Women navigate a complex and often dangerous world, facing multiple threats in both physical and digital spaces [8,9]. Here's a breakdown of some key concerns:

3.1. Physical Threats

Violence: Women face a range of physical threats including assault, stalking, domestic abuse, and intimate partner violence, which can unfold in countless settings, requiring vigilance.

Sexual Harassment: Catcalling, unwanted advances, and groping are still far too common, making many women feel perpetually tense in public.

Unequal Access to Safety Resources: From well-lit streets to reliable public transit to access to security measures, even these resources often reach women unevenly.

3.2. Digital Threats

Online Harassment: Social media and online platforms can make a conducive environment to cyberbullying, hate speech, and threats. Women are often disproportionately affected, either by abusive language or harmful content.

Doxxing: The malicious online publication of an individual's private information such as a home address or phone number by someone else can create significant fear and vulnerability. It is vital to remember that online and offline lives are often closely linked.

Non-consensual Sharing of Intimate Images: Sharing a private sexual image, or a video taken with a sexual motive, of someone without their consent creates a negative experience for the person in the image, and can have long-lasting impacts. This is a clear violation of privacy.

Online Stalking**:** Repeated and unwanted surveillance and contact from an individual can cause fear.

Misinformation and Disinformation: Exposure to false or misleading content has detrimental impacts on women's well-being, particularly as it relates to critical topics like health, safety, and gender equality.

4. EEG and Eye Blink Signals: The Mirror of our Emotional Worlds

The human body is an information channel carrying unsaid messages that may provide weighty insights. EEG (Electroencephalography) and eye blink signals are biological readouts from the brain that suggest how the electrical system works and visual system dynamics [10,11] as shown in Figure 1.

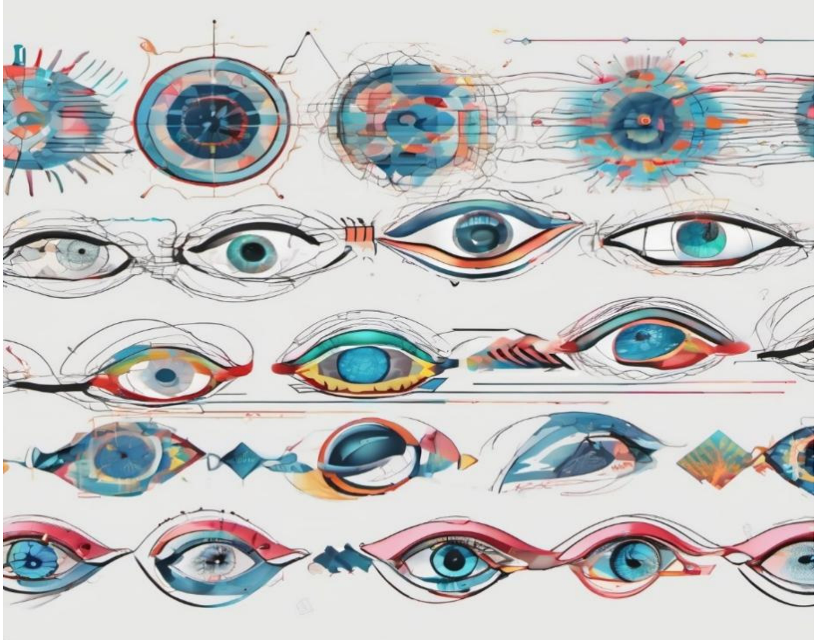

Figure 1. EEG and eye blink signals as biological readouts from the brain.

Here's an overview of EEG and eye blink signals:

4.1. EEG Signals: Understanding the Brain's Electrical Instruction

EEG records the electrical activity of the brain's neurons from the scalp electrodes implantation. Electrodes which are attached to the scalp detect and reflect neural activity by sensing the fluctuations in the electrical field which are the origin of these changes [10]. Brain EEG signals are differentiated by their frequency components that comprise delta (0.5–4 Hz), theta (4–8 Hz), alpha (8–13 Hz), beta (13–30 Hz), and gamma(>30 Hz)waves. These frequency groups are tied to various brain states and cognitive processes. By analyzing these signals, researchers and specialists can gain valuable insights into numerous aspects of brain function, including:

- Emotional state: The brain tends to react to different emotions, for example, fear, anger, and happiness, in its unique pattern of electrical activity.
- Cognitive function: It is worth noting that EEG techniques play a vital role in predicting attention, memory, and various other cognitive activities.
- Sleep disorders: Sleep problems like insomnia or sleep apnea can be shown by the brain's odd patterns of activity during slumber.

4.2. Eye Blink Signals:

Signals of averted gazes mean the uncontrollable motion of eyelids which occur continually during the day, as a typical body mechanism [17–19]. These movements have multiple functions. For example,

- The signals of blink lids are eye muscle movements that happen frequently and are not controlled voluntarily. Eyelids play a role in that they help to lubricate the eyes and protect them from drying out or uncontrolled input of information.
- The frequency and length of eye blinks may be modified via cognitive task, focus, and emotional condition factors. For instance, a person who blinks more in these situations shows they are in stressful or anxious situations.
- The eye blink reaction can be measured in various ways. Electromyography (EMG), video-based tracking, or special eye-tracking devices are possible methods [19]. These faint signs send much information concerning a person's cognitive and emotional state and such data is engaged and used to determine attention, arousal, and fatigue status.

4.3. Applications of EEG and Eye Blink Signals:

- Cognitive Research: The signals from EEG are currently one of the main techniques used for such cognitive processes as attention, memory, decision-making, and so on in neurocognitive sciences. Eye-blink signals can be used as an additional measure to amplify EEG information for investigation of visual processes and attentional mechanisms.
- Brain-Computer Interfaces (BCIs)**:** Indeed, based on those signals people create so-called BCIs (Brain-Computer Interfaces) that allow the brain to communicate with the outer world. However, applications may differ for those who are of assistive technology, rehabilitation, and neuroprosthetics.
- Mental Health Assessment: Brain function is evaluated besides psychiatric and neurological diagnoses such as epilepsy depression schizophrenia from EEG signals. Further, additional eye blink signals such as wariness may also be a good biological measure in assessing the capacity for emotional regulation and mental problem indicators [19].
- Human-Computer Interaction (HCI): By imitating eye blink signals as input modalities, HCI systems may let users control the operations of computers, smartphones, and any other devices only with eye movements. This system's functionality covers the areas including accessibility, gaming, and virtual reality.
- Biometric Authentication: Human biometric measurements are very discriminate, specialized among individuals, and personality-specific, able to change over time to become even more specific and non-transferable. The eye blinking frequency may serve as a means by which a biometric feature is collected for applications such as identity verification and security.

5. Internet of Things (IoT) Sensors and Devices

Protecting women from potential threats, IoT is one of the vital components of the detection system [12–16] designed to harness the signals of EEG and eye blinking. EEG sensors serve as the primary means of capturing the complex electrical activity in the brain. The sensitive sensors placed on the scalp provide valuable insights into cognitive responses triggered by perceived threats and provide a high temporal resolution [17–19].

This makes it possible to precisely scrutinize every brainwave [20–26]. These eye-tracking devices are essential for monitoring eye blink and eye gaze patterns in a patient's eyes. Infrared sensors or cameras rely upon infrared sensors to analyze eye movements providing crucial indicators of physiological changes associated with stress and arousal levels. The seamless integration of these sensors into wearable IoT devices ensures flexibility and mobility for participants [27]. These devices enable data collection in diverse real-world environments allowing for naturalistic surveillance of threat perception [28–35].

Furthermore, a data acquisition system for the IoT delivers sensor data to central processing units or cloud platforms enabling continuous monitoring and analysis in real-time.

Edge computing devices play a crucial role in preprocessing raw sensor data locally before transmission to enhance the system's efficiency and responsiveness. This approach reduces latency, conserves bandwidth, and optimizes resource utilization by ensuring timely detection and response to potential threats. Collectively, these IoT technologies make up a complicated network of work that acts as a vital informant and safeguarding system, capable of accurately discerning threats in any context and timely alerting the victims [36–40].

6. Proposed Methodology

The proposed machine learning-based EEG and Eye Blink Signals method is a new way of using the Internet of Things (IoT) and machine learning (ML) to improve women’s safety through the likelihood of violence. The system proposes an innovative approach to EEG and eye blink signals without wasting time in real-time to project physiological biomarkers such as fear, anxiety, or stress, thus directing to dangerous situations. The workflow of the proposed blink talk method [21] is shown in Figure 2.

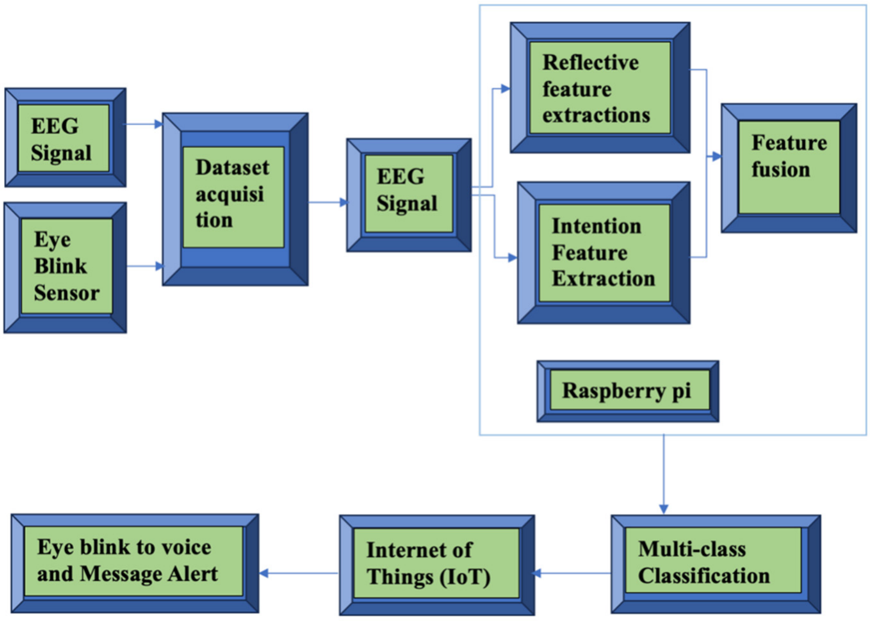
EEG Signal
Eye Blink Sensor
Dataset acquisi tion
EEG Signal
Reflective feature extractions
Intention Feature Extraction
Feature fusion
Raspberry pi
Multi-class Classification
Internet of Things (IoT)
Eye blink to voice and Message Alert

Figure 2. Workflow of the proposed Blink Talk method [21].

This methodology outlines the steps involved in investigating the feasibility and efficacy of this system:

6.2. Data Acquisition

Two primary approaches will be explored for data acquisition:

6.2.1. Public Datasets

Data must be drawn from freely available datasets with signals having both the EEG and eye blink combined with emotion labels such as fear, panic, and neutral. Priority is given to datasets where emotion is the focus. Group women as the core segment because they play an important role in the target population. Emotional labeling should include for example fear, anxiety, and stress.

6.2.2. Controlled Experiment (Optional)

The ethics of data testing are sensitive subject areas. Hence, the organizations will not compromise on it at any cost. Therefore, conducting a controlled experiment under strict ethical guidelines in case adequate public data is not easily available.

6.2.3. Recruitment

Participants will be recruited from different sources by running announcements, handing out leaflets, and using online platforms. Voluntary participation will be ensured and with it will remain the confidentiality of the participants.

6.2.4. Stimuli and Data Collection

Subjects are presented with various stimuli that elicit different emotional responses (e.g., a video depicting threatening situations, neutral control stimulus), and objective physiological (sophisticated EEG, eye blink sensors) data are recorded.

6.2.5. Emotional Labeling

Participants will be asked to share intensities they have experienced before and after being exposed to stimuli. It will be used to correctly annotate the physiological data that will be collected with the help of machine learning algorithms.

6.3. Preprocessing and Feature Extraction

The acquired data will undergo thorough preprocessing steps to ensure its quality and suitability for machine learning analysis:

6.3.1. Noise Reduction

Artifact removal and EEG signal demagnetization are considered as the initial step of analysis of EEG signals.

6.3.2. Segmentation

For feature extraction, apply the summation of segments of continuous data. Following preprocessing, relevant features will be extracted from the data:

- EEG features: PSD (power spectral density), coherence, and evolutionary potentials (respective features).
- Eyeblink features: Eye blinking, blink onset, inter-blink interval.
- Humanize: Data science technology can be applied to the process of feature selection to pick out those features that are the most informative and have the largest importance to the threat detection process.

6.4. Machine Learning Model Development and Evaluation

Various machine learning models were explored for their suitability in classifying emotional states based on the extracted features [41,42] as described below:

6.4.1. Support Vector Machines (SVMs)

The choice of an algorithm is primarily determined by whether the data is high-dimensional or is suited for binary classification tasks, for example: threat vs. threat.

6.4.2. Random Forests

A group learning method that is resistant to overfitting produces precise outputs considering the intimate association between feature interactions.

6.4.3. Deep Learning (DL) Models

Convolutional neural networks (CNNs) or recurrent neural networks (RNNs) can be tried, and these neural networks may work well if the data set is large enough to grasp more complex patterns in the input stream [41–44]. Model training and testing are done using the k-fold cross-validation approach, to ensure that the models can be applied in general circumstances. The performance metrics used for evaluation will include:

- Accuracy**:** The share of cases whose predictions by the evaluative model live up to actual results.
- Precision: The ratio between the number of true positives and the number of actual positives predicted.
- Recall: The volume of a truly positive model discovered by the model.
- F1 Score: A harmonic means joint performance metric including precision and recall; thus the model's performance is seen in the context balance.

6.5. System Design and Implementation

Based on the findings from the machine learning model development and evaluation, a prototype system will be designed and implemented:

6.5.1. Wearable Sensors

Discrete and comfortable wearable sensors [45,46] for EEG and eye blink recording.

6.5.2. Data Transmission Module

Conveys the data to the cloud platform by a secure IoT network.

6.5.3. Machine learning model

Aimed at analyzing in-time data and producing threat forecasts that used the cloud infrastructure for the deployment [47].

6.5.4. Alert System

Issues alarms after identification of possible danger and informs authorized people (e.g. professionals, trusty colleagues) so they might think out counteraction strategies adopted.

7. Case Studies: Highlighting the Global Impact of Violence against Women (VAW) and the Potential of the Proposed System

Table 1 demonstrates multiple violence against women (VAW) forms that women confront in different corners of the world, thus, revealing the transnational character of the issue and the utmost importance of the IoT-ML system as a means for counteracting this sexual violence against women. It can offer advanced warnings, drive away aggressors, and furnish effective solutions such that the lives of females become safer everywhere.

Table 1. Case Studies of Violence Against Women (VAW) Across the Globe.

Region	Case Study	Statistics	Potential Impact of the Proposed System
Sub-Saharan Africa	A young woman in rural South Africa walks home alone after dark, fearing harassment and potential assault.	- 36% of women in Sub-Saharan Africa have experienced physical and/or sexual intimate partner violence in their lifetime [1]. - Limited access to lighting and security measures in rural areas increases vulnerability.	- Real-time threat detection could trigger alerts to trusted contacts or local authorities, deterring potential attackers and facilitating timely intervention.
South Asia	A teenage girl in India experiences online stalking and harassment, impacting her mental health and limiting her online activities.	- 75% of women in South Asia have experienced online violence, harassment, or stalking [2]. - Lack of digital literacy and limited access to support services further	- The system could analyze online interactions, identifying potential threats and providing early warnings. It could also connect women with relevant support services and resources.

		endanger women.	
Latin America and the Caribbean	A woman escaping an abusive relationship in Brazil fears for her safety and struggles to find a haven.	- 35% of women in Latin America and the Caribbean have experienced physical and/or sexual intimate partner violence in their lifetime [1] - Lack of adequate shelters and support systems for victims of domestic violence creates further challenges.	- The system could provide discreet alerts to designated emergency contacts or support services, enabling timely intervention and assistance.
Europe	A woman walking alone in a deserted park in a European city feels unsafe due to insufficient lighting and the potential presence of attackers.	- 22% of women in Europe have experienced physical and/or sexual intimate partner violence in their lifetime [1]. - Urban areas with inadequate lighting and security measures can heighten vulnerability.	- Integration with existing security infrastructure (e.g., smart city lighting) could trigger increased illumination in high-risk areas upon detecting potential threats, deterring crime, and improving women's sense of safety.

8. Experimental Setup and Discussion

This paper tested different combinations of machine learning algorithms [41–44] interfaced with electrophysiological and blink sensors and analyzed the effectiveness of the detection based on the electroencephalogram signals (EEG) and lid closures (blink signals).

The Convolutional Neural Network (CNN) is great at Spatial pattern observation in data precisely and CNN technology has been successfully used in the image recognition domain. CNNs have been used alongside EEG sensors to analyze the patterns of brain waves recorded by the EEG sensors. The CNN model of CNN was trained to capture features that girls can use to indicate symptoms of stress, anxiety, and other states that can be signs of potential physical danger.

SVM is another machine learning algorithm besides the Logistic Regression which produces an error rate of 2%. SVM stands for Support Vector Machine, and it is a supervised learning algorithm that can be employed productively in binary classification problem-solving. The SVM is used in threat detection using EEG and eye blink signals and compared with eye sensors in analyzing the blink patterns. The point of slowing, altering, or even inhibiting blinking to the flashing, rapid, or erratic blinking that points to the presence of distress or discomfort, the threat could be warded off.

The Recurrent neural networks (RNNs) were merged with a comprehensive set of EEG and eye blink sensors that enable the capture of temporal features throughout the datasets. Through the exploration of consecutive data of EEG and eye blinks' patterns, the RNN model was developed to identify microscopic alterations that may appreciably be a sign of potential danger.

Random Forest, an ensemble learning algorithm popularized by Breiman and Cutler in 2001, is used additionally. Random Forest is popular for its ability to manage big data that has lots of dimensions. The Random Forest combines the use of EEG sensors with random forests for the aim of detecting and classifying the patterns from the brainwave frequencies. A Random Forest model was built to discern the differences between brainwave patterns in the healthy state and those showing stress, arousal, or any other kind of distress.

Lastly, long short-term memory (LSTM) networks are a kind of recurrent network with the ability to remember information from the past as well as for the connections between the items in sequential data. This paper involved LSTM networks with blink sensors to read eye blink traces through a given period. The LSTM model was built in such a way as to catch the dynamic characteristics in the eye blink signals which assist in detecting any anomalies. This can aid in averting danger to women's safety.

The objective is to establish a connection between different machine learning methods and IoT sensor technologies that fit in real-world scenarios to ensure women's safety. Figure 3 shows the performance of various machine learning approaches when coupled with IoT sensor devices for threat detection via EEG and eye blink signals.

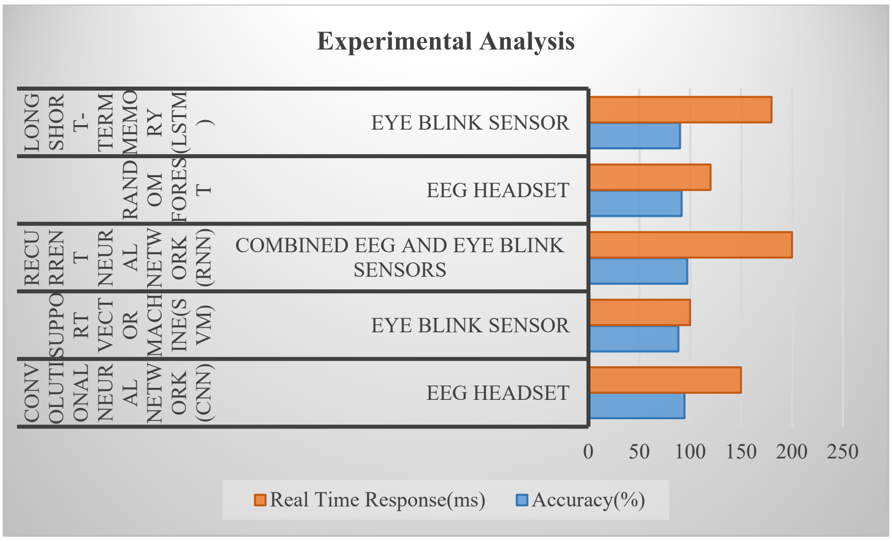

Figure 3. Performance of different machine learning approaches when coupled with IoT sensor devices for threat detection via EEG and eye blink signals.

This experimental analysis provides insights into the performance of different machine learning approaches when coupled with IoT sensor devices for threat detection via EEG and eye blink signals as shown in Table 2. It highlights the varying levels of accuracy, real-time response, effectiveness in diverse environments, user satisfaction, and challenges associated with each approach and sensor combination.

Table 2. Performance of machine learning techniques with IoT sensor devices for threat detection via EEG and eye blink signals with varying accuracy and real-time response, and challenges associated.

Machine Learning Approach	IoT Sensor Device	Accuracy (%)	Real-Time Response (ms)	Effectiveness in Diverse Environments	User Satisfaction	Challenges Identified
Convolutional Neural Network (CNN)	EEG Headset	94.5	150	Effective in controlled environments, challenges in noisy settings	High	Privacy concerns due to EEG data
Support Vector Machine (SVM)	Eye Blink Sensor	88.2	100	Moderate effectiveness in diverse environments	Moderate	Limited accuracy in complex scenarios
Recurrent Neural Network (RNN)	Combined EEG and Eye Blink Sensors	96.8	200	High adaptability to diverse environments	High	Integration challenges with multiple sensors
Random Forest	EEG Headset	91.3	120	Limited by environmental noise, but robust in controlled settings	Moderate	Interpretability of results
Long Short-Term Memory (LSTM)	Eye Blink Sensor	89.7	180	| Moderate effectiveness, particularly in low-light conditions	Moderate	Limited scalability in complex scenarios

9. Future Directions and Challenges

Future research directions hold the promise of significant advancements:

- Robust clinical trials: The system should go through rigorous trials with varying participants to ascertain the expensive effectiveness and user experience in real-life situations.
- Advanced ML algorithms**:** Improving Machine Learning (ML) performance by developing intelligent algorithms that can handle dynamic and changing situations is crucial for the right threat identification.

- Alternative data sources: Looking into other data sources like physiological responses or ambient factors aside from the EEG and eye blinks, should not only explain but be able to provide a more thorough picture of the danger they embody.
- Integration with existing infrastructure: It is also necessary to investigate the technology's integration with the existing safety responses, for example, to be used with emergency response systems, to decrease the response time and provide prompt help.

However, navigating these exciting directions necessitates confronting significant challenges:

- Data privacy concerns: Enhancing the safety of information and the privacy of users is one of the main duties. Enhancing anonymization and encryption designs are fundamental counts that ease delicate data protection issues.
- User acceptance and comfort**:** Ensuring the proper fitting of the gadget, soaking up or removing uncomfortable feelings, especially for long-term uses, is one of the vital factors for the users to accept the devices. A device that is designed and operates properly not to make the user feel any discomfort or discourage his or her follow-up is necessary.
- Ethical considerations: Algorithmic bias caused by the training data must be greatly mitigated e because of the great importance of its role. Applying various types of data and focusing on impartial examination is crucial to building a system that works morally without bias.
- Accessibility and affordability: In any case, affordability and accessibility of technology must be a priority so that the gap between rich and poor can be bridged and there is no exacerbation of prevailing inequalities. Cheapening the means as well as widening the accessibility programs to cover almost everybody is a basic aspect of making sure that the inclusive culture is not just a slogan.

10. Conclusions

The viewpoint of an intelligent machine learning (ML) technique that improved EEG and eye blink signals for threat detection and improved women's security is presented in this paper. This method takes the lead by applying EEG and eye blink signals which are captured with the help of wearable devices, and therefore, represent a flexible way of dealing with the threat quickly in real-time. This is achieved by employing modern machine learning tools and regular KPIs to examine physiological data that may represent stress or risky conditions. With this feature, women will have the opportunity to explore their environments safely and with confidence.

The proposed methodology used here is broken down into five main factors: data acquisition, preprocessing, feature extraction, machine learning models and evaluation, system design and implementation, and ethical considerations. Furthermore, it is a comprehensive performance of machine learning models in classifying such emotional states through the analyzed features. A threat detection system model to be implemented is a stepping-stone towards the real-time detection of potential threats, which in turn could raise alerts and activate safety measures timely. Finally, the need for ethical considerations, like data privacy, user consent, and potential biases is taken seriously.

However, strengthening the cooperation between different disciplines ensures the development of safe and inclusive societies in which women can feel free from various forms of violence.

Author Contributions

Conceptualization, Methodology, Software, Validation, Analysis, Original Draft preparation, Supervision—L.A., Data curation, Review and editing, Investigation—Y.K.S. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Data Availability Statement

Data used in this paper is subject to privacy and ethical restrictions and is therefore not publicly available.

References

1. Devastatingly pervasive: 1 in 3 women globally experience violence (2021). Available at: https://www.who.int/news/item/09-03-2021-devastatingly-pervasive-1-in-3-women-globally-experience-violence (Accessed on: 19 February 2024).
2. Facts and Figures: Ending Violence against Women (2022). Available at: https://www.unwomen.org/en/what-we-do/ending-violence-against-women/facts-and-figures (Accessed on: 19 February 2024).
3. S.B. Gadhe, G. Chinchansure, A. Kumar and M. Ojha. Women Anti-Rape Belt. An International Journal of Advanced Computer Technology, vol. 4, no. 2320-0790, April, (2015).
4. G.C. Harikiran, K. Menasinkai and S. Shirol: Smart Security Solution for Women Based on Internet of Things (IoT). In Proceedings of the International Conference on Electrical Electronics and Optimization Techniques (ICEEOT), pp. 3551-3554 (2016).
5. L. Arya, Y.K. Sharma, R. Kumar. Towards a Greener Tomorrow: IoT-Enabled Smart Environment Monitoring Systems. In Proceedings of the *2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT)*, Faridabad, India, pp. 1112-1117, (2023) doi:10.1109/ICAICCIT60255.2023.10465894.
6. N.R. Chandrika, L. Arya. Exploring IoT Frameworks: An In-Depth Analysis and Survey of Security Protocols, In Proceedings of the International Conference on Innovative Computing and Communication (ICICC), pp. 1-8, (2024) http://dx.doi.org/10.2139/ssrn.4746559.
7. M. Hind, O. Noura, A. Abraham. Modeling IoT based Forest Fire Detection System with IoTsec. International Journal of Computer Information Systems and Industrial Management Applications, 15, 201–213, (2023).
8. D.G. Monisha, M. Monisha, G. Pavithra, R. Subhashini: Women Safety Device and Application-FEMME, Indian Journal of Science and Technology, Vol. 9(10) (2016).
9. G.P. Miriyala, P.V.V.N.D.P. Sunil, R.S. Yadlapalli, V.R.L. Pasam, T. Kondapalli, A. Miriyala. Smart Intelligent Security System for Women, International Journal of Electronics and Communication Engineering & Technology (IJECET), 7(2), (2016).
10. H. Singh, J. Singh Real-time eye blink and wink detection for object selection in HCI systems. Journal on Multimodal User Interfaces, Vol.12, Issue 1, pp. 55–65 (2018).
11. K. Yasoda, R.S. Ponmagal, K.S. Bhuvaneshwari, K. Venkatachalam. Automatic detection and classification of EEG artifacts using fuzzy kernel SVM and wavelet ICA (WICA). Soft Computing 24(21) 16011–16019 (2020).
12. M. Sivachitra,T. NaveenRaj, V.G. Rekhasri, N. Sowmiyaa Women safety night patrolling robot. Annals of the Romanian Society for Cell Biology pp.15706–15714 (2021).
13. B. Nivedetha. Wearable device for Women safety using IOT. JAC (J. Antimicrob. Chemother.). A Journal of Composition Theory Vol.14, Issue 6 pp. 94–97 (2021).
14. S. Tayal, H.P.G. Rao, A. Gupta, A. Choudhary. Women safety system design and hardware implementation. IN: 2021 9th International Conference on Reliability, Infocom Technologies And Optimization (Trends And Future Directions) (ICRITO), IEEE, pp. 1–3, September (2021).
15. K. Hariharan, R.R. Jain, A. Prasad, M. Sharma, P. Yadav, S.S. Poorna, K. Anuraj. A comprehensive study toward women safety using machine learning along with android app development, In Sustainable Communication Networks and Application, pp. 321–330, Springer, Singapore, (2021).
16. C.K. Gomathy, M.S. Geetha. Women safety device using IoT. International Journal of Scientific Research in Engineering and Management (IJSREM), Vol. 5, Issue 10, pp.1–9 (2021).
17. D. Li, X. Zhang, X. Liu, Z. Ma, B. Zhang. Driver fatigue detection based on comprehensive facial features and gated recurrent unit. J. Real-Time Image Process 20, 19. (2023).
18. J.S. Wijnands, J. Thompson, K.A. Nice, G.D.P.A. Aschwanden, M. Stevenson. Real-time monitoring of driver drowsiness on mobile platforms using 3D neural networks. Neural Comput. Appl., 32, pp. 9731–9743, (2020).
19. M. Abo-Zahhad, S.M. Ahmed, S.N. Abbas. A New EEG Acquisition Protocol for Biometric Identification Using Eye Blinking Signals. I.J. Intelligent Systems and Applications, 06, pp. 48-54, (2015).
20. L. Arya, Y.K. Sharma, R. Kumar. Digital Guardians: Enhancing Women's Security with Artificial Intelligence and IoT. In Proceedings of the 23rd International Conference on Intelligent Systems Design and Applications (ISDA 2023), (2023).
21. K.S. Priya, S. Vasanthi, R. Nithyanandhan, G. Jeyasheeli, M. Karthiga, C. Pandi. Blink talk: A machine learning-based method for women safety using EEG and eye blink signals. Sensors 28, 100810, pp. 1–7, (2023).
22. Sathyasri, B., Vidhya, U.J., Jothi Sree, G.V.K., Pratheeba, T., & Ragapriya, K.: Design and Implementation of Women Safety System Based on IoT Technology, International Journal of Recent Technology and Engineering (IJRTE), Vol.-7 Issue-6S3, pp.177-181 (2019).
23. S. Pagadala, L. Prasanna, A. Reddy. A Novel ML-Supported IoT Device for Women Security, International Research Journal of Engineering and Technology (IRJET). In Proceedings of the Internatıonal Conference on Recent Trends in Advanced Computıng, ICRTAC, 2019, Vol.08 Issue-06, pp. 3287-3291 (2021).
24. W. Akram, M. Jain, C. Sweetlin Hemalatha: Design of a Smart Safety Device for Women using IoT, In Proceedings of the International Conference On Recent Trends In Advanced Computing 2019, ICRTAC 2019, Vol. 165, pp. 656-662 (2019).
25. K. Srinivasan, T. Navaneetha, R. Nivetha, K. Mithun Sugadev: IoT Based Smart Security and Safety System for Women and Children. International Research Journal of Multidisciplinary Technovation (Irjmt), Vol.2, Issue 2. pp. 23-30 (2020).

26. A. Srivastava, A. Singh, A. Gaur, F. Ahmad. Smart Band For Women Securıty Usıng IoT. IJARIIE, Vol.8 Issue 6, pp.198-202 (2022).
27. M.A. Almaiah, S. Yelisetti, L. Arya, N.K. Babu Christopher, K. Kaliappan, P. Vellaisamy, F. Hajjej, T. Alkdour. A Novel Approach for Improving the Security of IoT–Medical Data Systems Using an Enhanced Dynamic Bayesian Network. Electronics, Vol. 12, Issue 20, pp.1-15, (2023).
28. S. Nagaraj, A.B. Kathole, L. Arya, N. Tyagi, S.B. Goyal, A.S. Rajawat, M.S. Raboaca, T.C. Mihaltan, C. Verma, G. Suciu. Improved Secure Encryption with Energy Optimization Using Random Permutation Pseudo Algorithm Based on Internet of Thing in Wireless Sensor Networks. Energies, December (2022), 16, 8, pp. 1-16.
29. S. Vahini and N.Vijaykumar: Efficient Tracking For Women Safety And Security Using IOT. International Journal of Advanced Research in Computer Science, vol.8, No.9, pp. 328-33 (2017).
30. G.C. Harikiran, K. Menasinkai, S. Shirol. Smart Security Solution for Women Based on Internet of Things (IoT). In proceedings of the International Conference on Electrical Electronics and Optimization Techniques, ICEEOT (2016).
31. A Jatti, M Kannan, RM Alisha, P Vijayalakshmi, S Sinha. Design and Development of an IOT based wearable device for the Safety and Security of Women and Girl Children, In Proceedings of the IEEE International Conference on Recent Trends in Electronics Information COMMUNICATION Technology. (2016).
32. A.B. Rjab, S. Mellouli. Smart Cities in the Era of Artificial Intelligence and Internet of Things: Promises and Challenges. Public Adm. Inf. Technol., pp 259–288 (2021).
33. K. Tsiknas, D. Taketzis, K. Demertzis, C. Skianis. Cyber threats to industrial IoT: A survey on attacks and countermeasures. IoT pp 163–186 (2021).
34. F. Ihsan, N. K. Bintarsari: Internet governance forum analysis on artificial intelligence in cyber security. Insignia: Journal of International Relations, vol. 35, pp. 32–47 (2021).
35. K. K. Patel, S. M. Patel. Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. International Journal of Engineering Science and Computing, vol. 6, no. 5 (2016).
36. X. Zheng and Z. Cai. Privacy-preserved data sharing towards multiple parties in industrial IoTs, IEEE Journal on Selected Areas in Communications, vol. 38, no. 5, pp. 968–979 (2020).
37. A.H. Ansari, P. Balsarf Pratiksha, R. Maghade Tejal, M. Yelmame Snehal. Women Security System using GSM & GPS, International Journal of Innovative Research in Science Engineering and Technology, Vol. 6, Issue 3 (2017).
38. V.R. Azhaguramyaa, D. Sangamithra, B. Sindhja. RFID Based Security System for Women. International Journal of Scientific & Engineering Research Volume 8 Issue 5 (2017).
39. T. Rajendra Shimpi. Tracking and Security System for Women's using GPS & GSM, International Research Journal of Engineering and Technology (IRJET), Vol. 04 Issue:0 (2017).
40. S. Vahini, N. Vijaykumar. Efficient tracking for women safety and security using IoT, International Journal of Advanced Research in Computer Science, Volume 8, No.9 (2017).
41. F. Farivar, M.S. Haghighi, A. Jolfaei, M. Alazab. Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT. IEEE Trans. Ind. Inform. 16, pp. 2716–2725 (2020).
42. Y. Jun, A. Craig, W. Shafik, and L. Sharif. Artificial Intelligence Application in Cybersecurity and Cyber Defense. International Journal of Wireless Communications and Mobile Computing pp. 1-10, (2021).
43. A.J.G. De Azambuja, C. Plesker, K. Schützer, R. Anderl, B. Schleich, V.R. Almeida. Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0–A Survey. *Electronics*, vol. *12, issue*-8 (2023).
44. A. Gupta, R. Gupta, G. Kukreja. Cyber security using machine learning: techniques and business applications, In Applications of Artificial Intelligence in Business. Education and Healthcare, pp. 385–406, Springer, Cham. (2021).
45. R.T. Hammed, O.A.W. Mohamad, N. Tapus. Health Monitoring System Based on Wearable Sensors and Cloud Platform, In Proceedings of the 20th International Conference on System Theory, Control and Computing (ICTSCC) (2016).
46. S. Saxena, S. Mishra, M. Baljon, S. Mishra, S.K. Sharma, P. Goel, S. Gupta, V. Kishore. IoT-Based Women Safety Gadgets (WSG): Vision, Architecture, and Design Trends, Computers, Materials & Continua, 76(1), (1027-1045), (2023).
47. V.S. Nirban, T. Shukla, P.S. Purkayastha, N. Kotalwar, L. Ahsan. A Machine Learning Perspective on Fake News Detection: A Comparison of Leading Techniques, In Proceedings of the International Journal of Computer Information Systems and Industrial Management Applications, 15, (59-68), (2023).