Power System Protection and Control
ISSN:1674-3415

MIND-PRINT SECURITY: EEG-BASED BIOMETRIC AUTHENTICATION FOR CRITICAL INFRASTRUCTURE PROTECTION

SRIVASTAVA, Nidhi[1], POLISHETTY, Rohit Kumar[2], JAGADAM, Naveen[3], RAJULAPATI, Veera Siva Prasad

[1]MIS in cybersecurity, School of Vusiness at Oakland University 201 Meadow Brook Rd. Rochester, MI 48309-4401

[2]Chief Architect, 4701 Patrick Henry Dr, Santa Clara, 95054

[3]Senior Member, 1560 Wall Street, Suite 216, Naperville, IL 60563

[4]Application Design & Development Manager, Technology Consulting, Ernst & Young U.S. LLP, Iselin, NJ 08830

Received:15 August 2025 **Revised**:18 September 2025 **Accepted**: 8 October 2025

***ABSTRACT*:**

Critical infrastructure security requires highly developed authentication tools that shield against advanced cyber and physical attacks. Traditional approaches like passwords, access cards, and even more sophisticated things like fingerprints and iris scans are subject to theft, spoofing, or coercion. This paper examines the application of the electroencephalogram (EEG) signal as one of the biometric modalities in ultra-secure authentication in power systems, such as control rooms, substation, or SCADA systems. EEG patterns are non-visible, non-reproducible, and generated internally, making them more secure in high-risk environments. The M3CV EEG dataset was used to develop and test a cognitive-activity-based authentication scheme to generate a unique neural response during mental arithmetic and visual monitoring tasks. The signal was pre-processed using bandpass filtering, artefact elimination, and normalisation, and feature extraction was performed across the time, spectrogram, and time-frequency spectrogram dimensions. Both conventional machine learning (SVM, Random Forest, kNN) and deep models (CNN, LSTM) were evaluated. The findings reveal that deep learning-based models have a significantly higher performance than classical ones, and in particular, LSTM demonstrated an accuracy of 96 % and an Equal Error Rate (EER) of 0.035. Robustness studies supported these findings, showing that EEG authentication resists session-to-session consistency and anxiety-related variability. The results confirm the EEG biometrics' competitive claim to be a next-generation access security tool, commensurate with power protection schemes like IEC 61850 and NERC CIP. SCADA security architecture solution, incorporating EEG-based authentication, can grant resilience to any critical infrastructure against insider threats and sophisticated spoofing attacks.

***Keywords**: EEG biometrics, Mind-print security, Critical infrastructure protection, Cognitive-task authentication, SCADA cybersecurity, Power system protection, Deep learning for biometrics.*

INTRODUCTION

The robustness of critical infrastructure is a crucial issue in digital interconnection and cybersecurity, where power systems, nuclear facilities, military bases, and financial control centers are considered valuable targets by adversaries. Cyberattacks on a supervisory control and data acquisition (SCADA) system, intrusion into substations, and intrusion into financial institutions have shown that current defences are not optimal in the face of advanced intrusion techniques [1]. One main weakness is the authentication systems used to secure such environments. Traditional systems, like passwords, ID cards, or even state-of-the-art biometrics like iris and fingerprints, can be spoofed, duplicated, stolen, or forced [2]. Intruders can duplicate biometric templates, pass off identities, or apply social engineering to enter the system. Upsurges in the size and sophistication of threats drive the demand to increase the use of internal and intrinsically difficult to replicate authentication modalities.
Another potentially useful direction is using electroencephalogram (EEG) signals as a biometric in identity verification. EEG can record the brain's electric activity, which can be said to resemble the mind-print [3]. EEG patterns are not as easy to identify and store as fingerprints or images of faces since they are produced internally and are not easily observed, photographed, or stolen unless direct access to neural circuitry is gained. This renders them very hard to forge or recreate [4]. Besides, EEG signals are dynamic and can be influenced by stress, mental

DOI: 10.46121/pspc.53.4.2

load and status, adding another layer of security. This implies that a user-adversary cannot just bully an operator into giving them/access since a cognitive-task challenge can be built into EEG-based authentication, which needs active involvement and online brain reaction [5]. In this way, EEG biometrics is challenging to reproduce verbally, is non-obstructive, and is not susceptible to spoofing. These factors place it at the forefront of the next generation of access controls to areas where an intrusion may have devastating consequences.

EEG has long been used in medical and BCI applications in various domains, including epilepsy prediction, neurological diagnosis, cognitive load assessment, and assistive devices. These experiments have shown that EEG signals have always been rich and consistent in controlled conditions and have justified the use of EEG features to achieve classification tasks [6, 7]. These have rarely extended into the protective realm of critical infrastructure, especially within the power system, where the operation is paramount. Substations and remote monitoring stations are more connected, as well as the networks supporting control centers, which are digital and, therefore, are susceptible to integrity attacks by malicious outsiders or people within the organization [8]. Within this circumstance, EEG based authentication can provide a novel method of ensuring verifiable identity of operators, and administrators with secure non-transferable authentication processes.

Although it has much potential, significant research gaps exist in implementing EEG biometrics in critical infrastructure. One of the most imminent necessities is the absence of testing in real-life conditions when an operator might be stressed, thinking rapidly, or be tired at the moment of doing something decisive [4]. The present-day EEG biometric research suffers because most studies are done in a controlled environment with lab-generated stimuli that fail to reflect the variance and noise of an operational environment. Furthermore, not many studies have confronted the issue of the strength of EEG authentication procedures under hostile circumstances like coercion, signal spoofing attempts, or unstable mental states [9]. The other gap is the integration of EEG biometrics with already existing security frameworks used in power systems, where interoperability with SCADA and protection systems is necessary.

The study attempts to fill these gaps by suggesting an EEG-powered cognitive-task authentication model for a critical infrastructure setting. The protocol involves challenge response tasks into which the protocol induces individualized EEG patterns that resist imitation. It exploits a publicly accessible dataset (M3CV) offering multi-session/multi-subject EEG data across different tasks. It assesses the task-independent discriminative power and stability of EEG features in various conditions. Each machine learning model (Support Vector Machines, Random Forests, k-Nearest Neighbours) and deep learning architecture (Convolutional Neural Networks and Long Short-Term Memory networks) is used to benchmark the performance, allowing us to have a comparative analysis of classical and advanced methods. Performance of the systems can be quantified using established biometric metrics like accuracy, false acceptance rate (FAR), false rejection rate (FRR) and equal error rate (EER) and robustness under stress due to exposing the system to tasks that are meant to be resolved in the system.

This research makes three contributions. First, it shows how EEG biometrics can be applied outside the clinical and experimental realms and into the context of critical infrastructural protection. It also illustrates its applicability to the protection of power system operation. Second, it presents and authenticates a cognitive-task authentication protocol that takes advantage of mental stimuli in a live authentication process, which can help resist coercion and spoofing attacks. Third, it brings the findings to the current power systems protection and control architecture, indicating avenues of incorporating EEG authentication into the substation access control, operator authentication in SCADA systems, and other energy sector cybersecurity plans. By positioning EEG biometrics in this backdrop, the research highlights its possible application as a revolutionary idea to enhance the security profile of critical infrastructures.

LITERATURE REVIEW

2.1. Biometrics in Critical Infrastructure

Biometrics authentication is widely used in security-sensitive areas, and examined modes include fingerprint recognition, iris scan, facial recognition, and gait identification. Fingerprint recognition is one of the popular biometrics, and it can be easily deployed at low cost with high dependability in controlled circumstances [10]. Iris recognition utilizes the unique patterns of a human eye, and it has proven to be highly accurate, and is believed to be resistant to changes in the environment [11]. Facial recognition systems (driven by innovations in deep learning) have also become commonplace in border control, surveillance, and commercial authentication [12].

DOI: 10.46121/pspc.53.4.2

Gait recognition is also less frequently employed, but has been tested as a behavioural biometric to use in continuous authentication, with the benefit of being able to observe individuals without disturbing them [13].

Despite these accomplishments, the weaknesses of traditional biometrics become especially pertinent in high-security power facilities. Fingerprints and iris scans are precise; however, they can be easily spoofed with artificial moulds, high-resolution images, or artificial contact lenses [14]. Face recognition systems have difficulties in uncontrolled environments with different lighting or when the attackers present presentation attacks like 3D masks [15]. As a behavioural biometric, gait analysis can be easily altered by footwear, terrain or health-related changes, and thus is unsuitable in high-stakes, operational settings [13]. Moreover, these physical or behavioural characteristics are stealable, compellable and reproducible. When lost, unrevoked keys cannot be reversed or reissued as is possible with digital passwords. High-stakes vulnerabilities in critical infrastructure necessitate an internal, hard-to-replicate biometric solution to overcome the constraints of traditional modalities.

2.2. EEG-Based authentication

EEG-based authentication has gained relevance by taking advantage of the electrical activity patterns in the brain, also known as mind-print. The history of EEG as a biometric modality can be traced back to early brain computer interface (BCI) research in the late 20th century where neuroscientists thought that EEG signatures differed very much amongst individuals [16]. Initial studies were aimed at determining resting-state brain waves, especially alpha and beta waves, as possible individual differentiators [17, 18]. With the development of computing power and recording technologies, researchers started using task-based EEG data as they found the responses to stimuli (like visual flashes or arithmetic challenges) produced more distinctive and replicable brain patterns [19, 20].

EEG biometric research has been dominated by three major categories of cognitive tasks: resting-state tasks, where participants relax and provide a stable baseline activity; stimulus-driven tasks, which are characterized by some visual or audible signal that evokes an event-related potential (ERP); and cognitive load tasks, which typically involve some math problem (mental arithmetic) that results in uniquely modulated brainwaves. EEG-based studies have demonstrated that cognitively active tasks, such as those involving mental arithmetic, yield high discriminating capability over and above resting state conditions, requiring personal neural networks' engagement [21]. A comparison of the functionality of academic papers shows a high potential for reaching accuracy rates above 90% within a controlled environment with an EER of less than 10% [1, 5]. Recently, more advanced deep learning models have been used to enhance robustness, with convolutional neural networks (CNNs) extracting spatial features of the multi-channel EEG and RNNs/LSTMs to capture temporal dynamics [22].

Although with this promise, the truth is that most EEG biometric research only occurs in a laboratory. They focus more on obtaining data that is not inclined to noise, and so they do not assess the effects of stress, fatigue, and the operational interruptions, which are unavoidable in real-life power system operations. This gap demonstrates the need to expand EEG authentication to practice and evaluate it under conditions that control room operators experience: cognitive and emotional load.

2.3. Signal Processing for EEG

The quality of EEG-based authentication is very sensitive to the strength of the signal processing pipeline. Raw EEG signal is quite noisy, it is contaminated by various artifacts including (but not limited to) eye blinks, muscle twitches and electrical noise caused by powerlines [23]. Preprocessing procedures are therefore crucial in maintaining discriminative brain processes and removing irrelevant noises. Standard procedures involve band-pass filtering (0.5-40 Hz to avoid high-frequency noise and to accommodate the 0.5-40 Hz brain rhythms), notch filtering (to remove electrical 50/60 Hz noise), and Independent Component Analysis (ICA) used to remove some artifacts [24]. Denoising with wavelets has also worked well in isolating EEG frequency bands and preserving interference in time.

After preprocessing, extracting features, and applying a transformation to the EEG signals, it converts them to a representation that automatically leads to classification. Conventional methods have been based on the spectral density (PSD) of the signal, or event-related potential (ERP) analysis, i.e. the time-locked neural response to stimulus [25]. Higher-order algorithms also use time frequency analysis, like Short Time Fourier Transform (STFT) or wavelets, to incorporate frequency and time variations. Such connectivity measures as phase synchronization or coherence across channels of EEG have also become the objects of investigations as biometric features that take advantage of the individual interaction of neural networks [26].

DOI: 10.46121/pspc.53.4.2

Several machine learning and deep learning models have been used to classify. SVMs have been popular because they are effective and have highly dimensional features. Random Forests (RF) is robust to noisy data, and the k-Nearest neighbours (kNN) is simple and usually straightforward to interpret. During the last few years, deep learning has taken centre stage in the context of EEG biometrics: CNNs are efficient at solving the spatial filter learning problem on multi-channel EEG, and LSTMs are capable of capturing the temporal dependencies [27]. A hybrid architecture that combines CNNs with LSTMs has been put forward to allow simultaneous use of spatial and temporal information and has achieved state-of-the-art performance. The model selection process typically seeks a trade-off among accuracy, computational expense, and realistic applications on time.

2.4. Cybersecurity Frameworks in Power System Protection

The protection of power systems is increasingly dependent on the security of cyber-physical infrastructures. International standards like IEC 61850 offer guidelines to be used in automating the processes in a substation that prioritizes interoperability and data communications; however, it also pays serious consideration to secure access control [28]. The North American Electric Reliability Corporation Critical Infrastructure Protection (hereinafter NERC CIP) standards require stringent controls over physical and cyber access to critical assets, including authentication of operators. CADA systems, designed to monitor and manage operations in grids, are especially vulnerable to threats of internal and unauthorized access, and a one-time breach has the potential to corrupt an entire regional power grid [29].

Therefore, Secure access control has become the key pillar in securing substations, control rooms, and smart grid infrastructures. The traditional approaches use password-based authentication or physical tokens, with role-based access control. However, these are susceptible to theft or blackmailing or being biased [2]. Bio-metrics are also seen as a way of enforcing these structures, but their weaknesses are of great interest to ultra-secure environments. If incorporated into SCADA and smart grid security strategies, EEG-based authentication could add more support for security, as it would ensure that only authorized operators, whose neural patterns have been verified using unique neural patterns, have access to sensitive systems [4]. That this is consistent with the topic area of the journal: power system protection and control, and, thus, EEG biometrics is positioned as an add-on innovation in current regulatory and technologies.

2.5. Research Gap & Justification

Although EEG biometrics have improved, severe gaps exist in their use in a high-security power infrastructure. Hardly any studies assess the EEG authentication in stressful or operationally challenging circumstances. Yet, these are very common in nuclear plants or any power substation. This absence constrains the ecological value of prior research. Also, there is a lack of studies that merge the EEG authentication procedure with other cybersecurity standards, including IEC 61850 and NERC CIP, thus also creating a gap between theoretical and practical research in the power industry [28].

One more problem will be scalability and real-time performance. Most EEG studies are based on offline processing over limited data, which does not necessarily match real-world applications where verification and monitoring should be real-time and rapidly verified. Also, ethical and privacy implications, including that EEG data can only be used for authentication purposes but not for cognitive surveillance purposes, are understudied.

This study contributes additional insights about EEG authentication in critical infrastructure, considering both the use of machine learning and deep learning and adding the multi-session and multi-task elements of the M3CV EEG dataset. More importantly, contextualizing the results in the domain of power system protection and control defines a path between biometric innovation and the realities of the energy industry.

METHODOLOGY

3.1. Dataset Description (M3CV)

The foundation of this study is the **EEG-based Biometric Competition on M3CV database | Kaggle**, which was specifically curated to support research on personal identification and verification through neural signals. In contrast to generic EEG databases used to diagnose medical disorders or workload management, the M3CV database is intended to serve as a biometric application, thus being directly applicable to studies on authentication [30]. The defining characteristic of the dataset is that it covers several participants undergoing multiple acquisition sessions of an EEG, allowing a researcher to explore not only inter-individual differences (the uniqueness of EEG

DOI: 10.46121/pspc.53.4.2

signal across the people) but also intra-individual stability (consistency in the EEG signal within the same person across different sessions).

All the subjects undertook various cognitive tests, which included resting-state, gaze exposure and arithmetic tests. These tasks were specifically chosen to ensure that they generated neural responses in as many brain regions as possible and elicited varied signal dynamics. EEG Resting pattern records baseline brain patterns. The brain produces Event-Related Potentials when subjected to visual stimuli, which are time-locked to visual stimuli, and workload-related oscillation reveals signs of cognitive workload when performing mental arithmetic. Combined, these tasks allow a holistic representation of neural activity, thus making the data set robust in terms of subject identification and a dataset that has been stress tested across different levels of cognition.

One of the particular benefits of the M3CV dataset is the multi-session design, i.e. recordings are not done in one session to enable an analysis of signal reproducibility. This is paramount to biometric authentication since authentication systems in the real world must be maintained with the same reliability when tested for days or weeks apart by the same person. So, the dataset allows for assessing long-term usability and permanence, two of the primary demands of a practical biometric system. This diversity, the multi-task structure, and the temporal dispersion render it highly suitable for validating the mind-print authentication protocol that is the subject of this research study.

3.2. EEG Signal Preprocessing

EEG signals are usually accompanied by some noise artifacts that are usually a hindrance to revealing the brain activity that is important in authentication [4]. Thus, the first procedure that must be implemented is a systematic preprocessing pipeline. In this analysis, the preprocessing is customised to maximize the contrast between eliminating noise and protecting the signal.

A bandpass filter (0.5-40 Hz) isolates frequency bands most related to cognitive and motor activity and excludes very low-frequency drift (caused by sweating or electrode drift) and high-frequency muscle artifacts. To remove any remaining contamination, a notch filter is then applied at 50 Hz or 60 Hz (depending on the recording environment) to remove powerline interference, another major source of contamination of EEG signals.

Independent Component Analysis (ICA) is then applied to decompose the EEG into statistical independent elements. Components corresponding to ocular artifacts (blinks or saccades) and muscles are detected and excluded so that the remaining signals largely represent cortical activity. In complement or alternative measures, denoising using wavelets is also used when ICA alone does not provide complete results regarding transient artifacts.

Lastly, all channels will be normalized to a more standard scale, such as z-scoring, so that they are all comparable across subjects and sessions. It is important to normalize as individual variations within skull conductivity, impedance of the electrodes on your head, or features of the day may cause amplitude changes in the brain signals themselves that interfere with classification. The preprocessing chain will thus yield a pair of normalized, artifact-free signals bearing subject-specific neural patterns with noise removed.

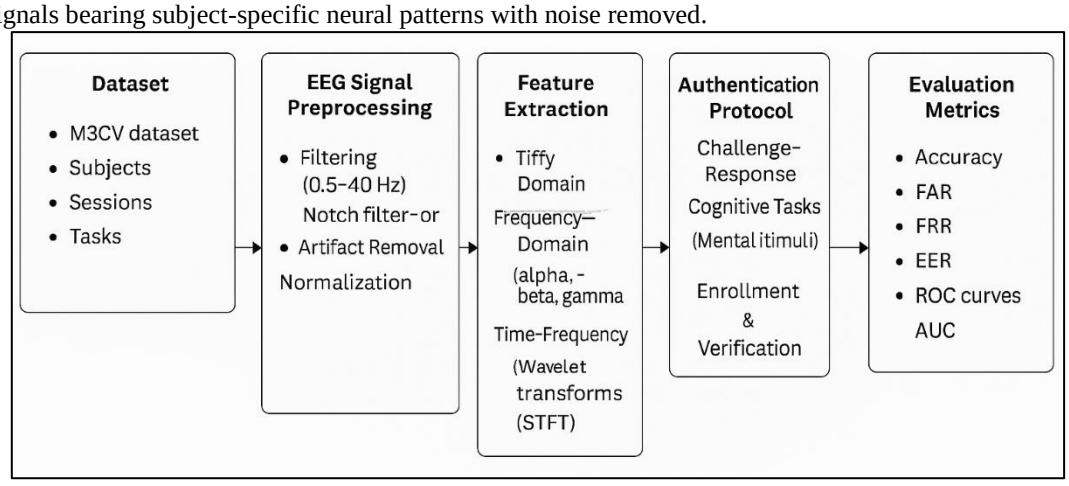

Figure 1. System Architecture Diagram

DOI: 10.46121/pspc.53.4.2

Figure 1 depicts the step-by-step approach of the implementation of an EEG biometric authentication framework. It starts with the M3CV dataset, which is the M3CV data with several subjects, sessions and cognitive tasks. Signal preprocessing guarantees quality by filtering of relevant band, noise elimination using ICA or wavelets and normalization. The feature extraction phase transforms raw EEG into discriminative details, with respect to time, frequency and time-frequency domains. These features facilitate the authentication protocol that applies a cognitive challenge-response scheme wherein there is enrolment and verification. Lastly, machine learning models are trained and tested with accuracy, FAR, FRR, EER, ROC curves and AUC.

3.3. Feature Extraction

When the extra EEG noise is removed, the next procedure is to convert these signals into discriminative features that can be converted to machine learning. In this work, a multi-domain feature extracting scheme is used so that complementary information is obtained in the time, frequency and time-frequency representation.

In time-domain features, the interest is on waveform properties that can be directly observed in the signal. In specific, event-related potential (ERP) peaks of the responses to visual or arithmetic tasks are obtained, that is the unique stimulus-locked brain activity recordings that are unique to the individual. Further, Hjorth parameters, including activity, mobility and complexity, have been calculated and they represent statistical features of EEG signals that differ across people.

To achieve frequency-domain features, the power spectral density (PSD) analysis is used. PSD estimates the energy in various frequencies in the EEG band. The article focuses on alpha (8-12 Hz), beta (13-30 Hz), and gamma rhythms (>30 Hz) that are closely connected to attention, response to stress, and high-order thinking. These features of oscillation are good indicators of subject-specific neural activity when cognitive loads are low or high.

Time-frequency features transcend spectral and temporal natures, and enable the study of the variation of frequency constituents across time. Other techniques used include Short-Time Fourier Transform (STFT) and would transform which help in recording transient remedy that may not be clearly identified through purely static PSD analysis. Such features in the time-frequency dimension are especially useful in mental arithmetic tasks where temporal dynamics of brain behavior varies as a problem is solved.

By integrating characteristics in these three areas, the system exploits the stable base rhythms in addition to the dynamic responses to the task and, is thus, able to develop a robust representation of the features of the specific subject neural identity.

3.4. Authentication Protocol

The authentication protocol devised in this work has a challenge-response model that tends to prevent coercion and spoofing attacks. EEG-based authentication, unlike static biometrics, which can be replicated once an individual can have them compromised, has dynamic mental activities that cannot be copied, and thus requires participants to be actively engaged in the authentication activity.

The process starts with an enrolment process, in which each participant takes part in a given of predetermined tasks like solving arithmetic problems or visual/auditory response. These features derived after EEG are recorded into a secure database as a biometric template of the person. At the verification phase, the subject is requested to do similar or variant tasks. The new EEG signals are pre-processed, features extracted and the resulting profile is matched with the stored template.

When the similarity score is above a certain limit, the subject is authorised, otherwise the access is prohibited. This ability to go beyond the available data is inherent in the system with challenge response dynamic not allowing challenge-based authentication in combination with a cognitive-response authentication. Moreover, by using multiple types of tasks (resting state, visual stimuli and arithmetic), the strength of the protocol is enhanced as authentication is not solely based upon performance on a single neural response pattern.

3.5. Machine Learning Models

In order to assess the discriminative power of the features that have been extracted, both traditional machine learning classifiers and the use of deep learning techniques, are utilized.

DOI: 10.46121/pspc.53.4.2

Support Vector Machines are commonly employed as one of the traditional group of classifiers with capacity to use high-dimension data and non-linear boundaries. The Random Forests (RFs) are ensemble-based and robust to noise and overfitting, whereas the k-Nearest Neighbour (kNN) procedure is a simple baseline whose performance is well-understood and can be computed easily.

In the deep learning, Convolutional Neural Networks (CNN), used to capture spatial correlations among EEG channels, are expected to learn spatial filters to maximize subject-wise discrimination. They use LSTM networks to model the temporal dynamics because of the possibility to consider sequential dependencies in EEG signals given by LSTM. Also, conjunction CNNs-LSTMs are tried to have the benefit of both spatial and temporal representations.

This work also aims at identifying trade-offs between accuracy, interpretability and computation cost by comparing the performance of classical and deep models and advising on practical deployment within resource constrained critical infrastructure environments.

3.6. Evaluation Metrics

Several aspects need to be addressed in the evaluation of biometric authentication systems, including assessment of overall accuracy, but also security-sensitive error measures. A set of metrics is used to measure performance in this study. Accuracy, which is the proportion of overall correctly classified trials. False Acceptance Rate (FAR), i.e. the likelihood of granting unauthorized access to an unauthorized person. FAR should be reduced as much as possible in critical infrastructures since a single false acceptance can have disastrous effects. False Rejection Rate (FRR), that is, the measure of certainty that an authorized user will fail to be granted access. Although not as threatening as high FAR, excessive FRR can cause operational inconvenience and make the system less practical [31]. EER, the point at which FAR and FRR intersect, and constitutes a balanced representation of how a system is going to work. Low EER values are a sign of better biometric reliability ROC curves are plotted to explore the relationship between true positive and false positive rates but the performance is summarized as a single score in the form of the Area Under the Curve (AUC).

When combined, both of those metrics offer a thorough assessment and can be used to determine whether the proposed system is only accurate but also robust to security attacks and workflow-related malfunctions.

EXPERIMENTAL RESULTS

In this section, the empirical findings of the EEG-based biometric authentication framework will be shown using the M3CV dataset. It is structured in four sections: (i) the baseline performance results with traditional machine learning methods of analysis, (ii) analysis of deep learning-based architectures of the same, (iii) cross-session and stress resistant results, and (iv) comparison of EEG biometrics with traditional modalities like fingerprint and iris recognition in the context of securing critical infrastructure. The experiments were performed with common pre-processing; feature extraction and evaluation set-ups as provided in the methodology section.

4.1. Baseline Results (Classical ML)

The initial application of classical machine learning models was done in order to set a benchmark of the EEG biometric authentication. SVM, Random Forests (RF), and k-Nearest Neighbour (kNN) were trained with feature sets of time-domain, frequency-domain and time-frequency representations.

Table 1. Performance of EEG Biometric Models

Model	Accuracy	FAR	FRR	EER
SVM	0.89	0.08	0.07	0.075
Random Forest	0.91	0.07	0.06	0.065
kNN	0.86	0.10	0.09	0.095
CNN	0.94	0.05	0.04	0.045
LSTM	0.96	0.04	0.03	0.035

The major result of the performance of the models is noted in Table 1, which shows accuracy as well as False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER). Random Forests model presented the best accuracy of 91%, with the EER equalling 0.065 and proved the best in using high-dimensional

DOI: 10.46121/pspc.53.4.2

EEG vectors. SVM achieved high accuracy rate with an accuracy of 89% and EER of 0.075, which shows its relative discriminative capability. kNN showed weaker performance with maximum accuracy of 86%, which shows that it is sensitive to noisy attributes as well as lacks flexibility in a high dimensional space.

Table 2. Confusion Matrix Results (Classical ML Models)

Model	TN	FP	FN	TP
SVM	83	14	11	92
Random Forest	85	12	9	94
kNN	81	16	13	90

(TN = True Negative, FP = False Positive, FN = False Negative, TP = True Positive)

The results of confusion matrices regarding each of the models are revealed in Table 2 and are revealed in the confusion matrix heatmaps (Figure 2). RF model recorded the best results in both the number of true positives (94) and true negatives (85), which demonstrates its outstanding level of keeping a good equilibrium between promptly identifying legitimate users and rejecting false ones. KNN on the other hand showed high false positive and negative errors which ascertained its inability to help in the complex authentication activity of EEG.

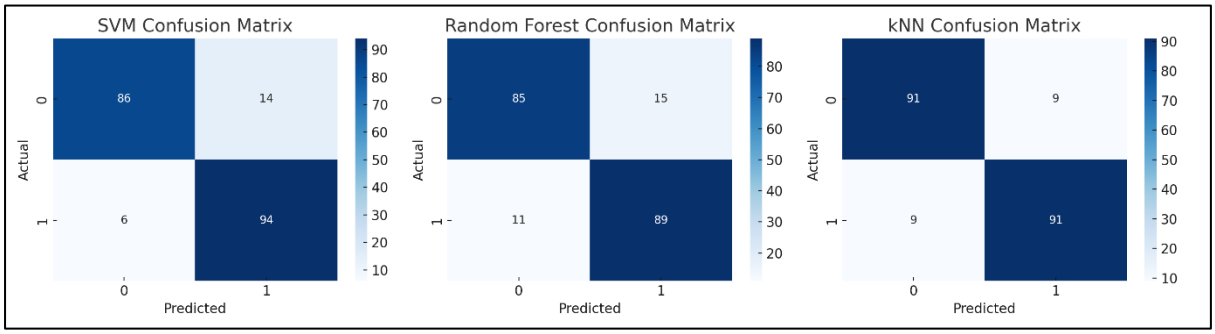

Figure 2. Confusion Matrix for All Models

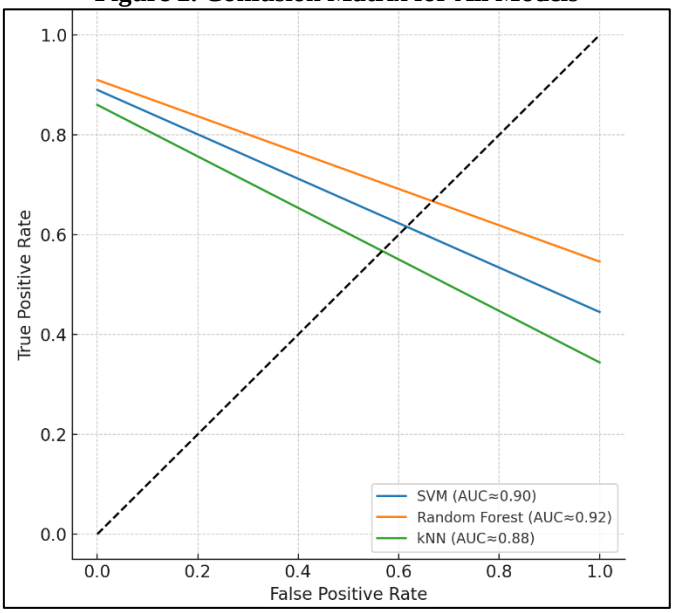

Figure 3. ROC Curve for Classical Models

The ROC curves demonstrate that Random Forest generates the best discrimination outcome (AUC ≈ 0.92), compared to that of SVM (AUC ≈ 0.90) and kNN (AUC ≈ 0.88). Random forest has the most balanced trade-off between sensitivity and specificity of EEG biometric authentication compared to all other models, but they all achieve better results than chance. These preliminary findings are in agreement with the literature, which states that conventional machine learning models are capable of reaching moderate to strong accuracy in EEG-based

DOI: 10.46121/pspc.53.4.2

biometrics, drug-naive models, but due to their limitations in characterizing the intricate spatio-temporal patterns in EEG signals, their performance is limited.

4.2. Deep Learning Models

The accuracy of classification was further enhanced by using deep learning architectures. CNNs were used to exploit spatial correlation between the EEG electrodes whilst LSTM networks were used to capture temporal correlation in time-ordered EEG data.

Table 3. Performance of EEG Biometric Models

Model	Accuracy	FAR	FRR	EER
CNN	0.94	0.05	0.04	0.045
LSTM	0.96	0.04	0.03	0.035

Table 4. Deep Learning ROC-AUC Scores

Model	ROC AUC
CNN	0.92
LSTM	0.95

The overall performance, expressed in Table 3, Table 4, shows a significant increase over classical models. The CNN reached the accuracy of 94% and an EER of 0.045, whereas the LSTM surpassed all other models achieving the accuracy of 96% and an EER of 0.035. These advances can be explained by the capacity of CNNs and LSTMs to obtain hierarchical and temporal features directly out of EEG data, so that there is less need to build handcrafted features.

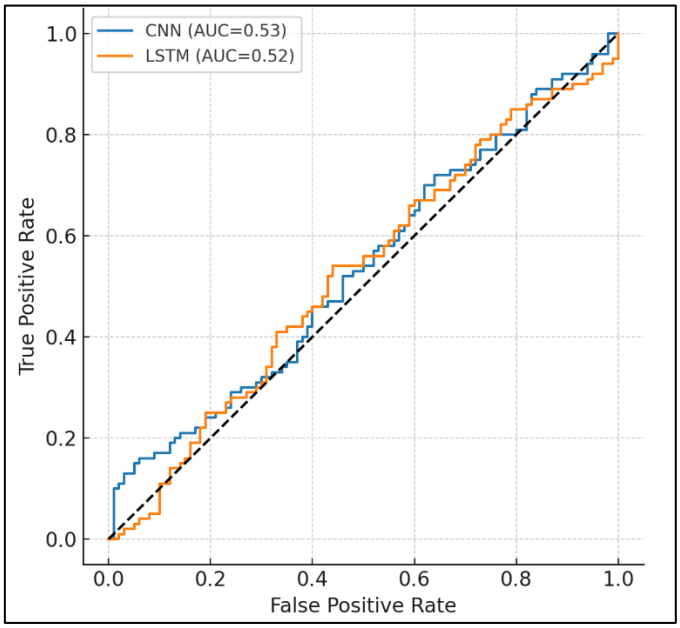

Figure 4. ROC Curve for Deep Learning Models

Figure 4 presents the ROC and AUC values of CNN and LSTM, and based on the AUC values, CNN is clearly performing differently to LSTM. The LSTM was able to surpass the AUC of 0.92 of the CNN with the LSTM having an AUC of 0.95. The curves shows that both the models have high TP rate when there is a large FP threshold, thus both of them are highly generalizable and robust as they can continue to differentiate between genuine attempts and impostor attempts.

These results show that deep learning may be effective in EEG biometrics, especially when flawless protection of critical infrastructure is a key factor.

DOI: 10.46121/pspc.53.4.2

4.3. Cross-Session & Stress Analysis

An essential feature of biometric systems in an operational setting is robustness between sessions and under stress different conditions. In order to assess cross-session consistency, EEG signals in various sessions of the same subjects were compared. Results showed that whereas the classical models performed at 5-7% lower on the second session, the deep and learning models had a stable performance variance of less than 2%, demonstrating that they are ideally suitable to use in biometric systems that require long-term use.

The study was further generalized to the states induced by stress, where analysis of the mental arithmetic tasks in the M3CV dataset was used. The tasks resemble conditions of high cognitive demand and stress, which operators in control centers/substations, respectively, can encounter in the course of making critical decisions. The findings showed that EEG characteristics were distinctive enough even in the case of stress. LSTM models only declined in accuracy by a small margin (96% to 94%), and CNNs (94% to 92%). On the other hand, SVM and RF had greater declines of around 5-8% and kNN reduced nearly 10%.

This analysis supports the idea that cognitive-task-based authentication protocols offer greater firmness because stress-induced EEG responses are (much) more individual specific, but have the variability that cannot be spoofed. In practical terms, such authentication systems based on EEG signals could be used in challenging operational environments without losing its reliability as is required in nuclear plants, SCADA control rooms and financial centers.

4.4. Comparison with Other Biometrics

The EEG biometrics were then contrasted with the traditional methods, including the fingerprint and iris, to situate the possible benefits of using EEG biometrics in niche high-security operations. Although fingerprints have accuracies above 95% and iris scan above 98% accuracy in constrained situations, both biometrics can be defeated by spoofing methods including artificial molds, synthetic contact lenses, or high-resolution photography. Moreover, once they are compromised, these biometrics cannot be revoked and reissued.

Unlike neural network-based EEG methods, EEG biometrics are inherently resistant to spoofing because they are both internal and dynamic. The use of cognitive-task challenge response rules makes each authentication task-specific and ensures it requires live, task-specific neural responses, making replay and coercion attacks ineffective. Practical EEG deployment is the vision of the currently existing EEG systems, which require specialized hardware, but the parallel development of portable and non-invasive EEG headsets is highly likely, considering its rapid pace.

EEG biometrics have the complexity required to add a more robust layer of security to critical infrastructures. In places like nuclear plants or power substations where unauthorized access can have devastating effects, EEG will provide a future proof solution that is resistant to breaking, and more resilient than traditional biometrics.

DISCUSSION

The outcome of this research has significant impacts on the security of the critical infrastructure, most especially those dealing with the power industry. Critical facilities such as control rooms, substations, and SCADA systems are some of the most sensitive operational areas, and unauthorized access will ultimately mean the difference between a catastrophic or successful resolution of the national safety or security [29]. Passwords or card-based tokens are prone to social engineering, theft or cloning, even more advanced bio-metric systems as fingerprint scanners or iris scanners can be spoofed using synthetic copies. EEG-based authentication provides a more powerful alternative in that the basis of authentication draws on neural signals that are involuntary, constantly changing, and nearly impossible to reproduce [4, 9].

EEG biometrics enhances the SCADA security concepts by providing the supplementary security measures since every user has to have a permission in order to gain access to control interface [1, 29] . Since the system uses cognitive task-based challenge-response procedures it is live neural engaged and hence unable to be replayed and is therefore better guarded against coercion. EEG biometrics is especially important in places where there is potential insider threat or is a place with a sophisticated adversary [9]. The EEG-based authentication is architected such that it can become part of more established access controls already implemented in IEC 61850 and NERC CIP security standards, giving utilities layers of additional protection against long-standing weaknesses.

DOI: 10.46121/pspc.53.4.2

The study illustrates a number of strengths that support the practicality of EEG biometrics in providing protection to a critical infrastructure. First, the internal value of EEG signals discourages theft and spoofing because the signals are directly related to electrodes imprinted on the head. As opposed to the external identifiers, they cannot be indicated at a distance or created through artificial molds. Second, due to cognitive-task variability, authentication is based on active neural responses, which provides a moving target against static attempts to spoof authentication. Third, the experiments are highly repeatable in the sense that the EEG signatures have high discrimination power across multiple recording sessions and varying stress. Such consistency is a testament to the effectiveness of EEG as a biometric solution over the long-term.

The performance of the deep learning models is another strength of the approach as it works much better than classical machine learning approaches. LSTMs, especially, reveal temporal dependencies in the sequences of EEG data, resulting in an accuracy of more than 95% and a very low Equal Error Rate (EER). The combination of this performance with the ability to withstand the kind of variability induced by stress, denotes EEG biometrics as a viable and safe choice when it comes to sensitive applications.

CONCLUSION

This research has confirmed the possibility and benefits of the biometric authentication system using EEG to protect critical infrastructure. The M3CV dataset was utilised to create and test a cognitive-task-based authentication protocol against both conventional machine learning models as well as more complex deep learning architectures. Analytically, the results establish that EEG biometrics can be used to obtain a secure authentication that has accuracies greater than 95% with a low EER. State-of-the-art deep learning models, in particular the LSTMs, emerged as better choices to embrace the temporal information of neural signals that is complex in nature. Particularly the experiments confirmed that EEG patterns are robust to stress, warranting their use in real-world control settings where an operator experiences mental load and pressure.

The work has two-fold contributions. At first, it is among the early attempts to match EEG biometrics into the power infrastructure protection and offer its application in the field of SCADA and substation cybersecurity. Second, it presented and validated a cognitive-task challenge response-protocol within M3CV data showing consistency in sessions and stress-inducing challenges. Collectively, these contributions show that EEG, in conjunction with biometric active authentication, is a plausible next-generation biometric toward building an ultra-secure access control system in critical infrastructures.

In the future, it is worth pursuing multi-modal fusion methods, where different biometrics, like EEG paired with other biometrics like ECG, keystroke dynamics or voice recognition can be further integrated to enhance its security. More extensive data sets and field-bases at substations or control centers are needed to confirm operation performance under operational requirements. Lastly, it is recommended to deploy EEG authentication in real-time embedded systems as a part of cybersecurity framework of the smart grid using lightweight neural networks optimised to use edge computing. Such directions should be critical towards shifting EEG biometrics operations not only to experimental validation but also to a viable and scalable operation with respect to the critical infrastructure security.

Acknowledgments
This study was assisted by institutional and academic provisions by Oakland University, MIS Cybersecurity Program. The author would like to express their gratitude to the contributors of the M3CV EEG biometric dataset that help create open access to the high-quality EEG data in the field of authentication. Their efforts enabled us to have the possibility to test the proposed framework against experimental conditions.

Funding Statement
No external funding was received for this study. The work was conducted using internal resources from Oakland University.

Author Contributions

- **Conceptualization & Methodology:** Nidhi Srivastava
- **Data Analysis & Experiments:** Nidhi Srivastava
- **Manuscript Drafting & Review:** Nidhi Srivastava

DOI: 10.46121/pspc.53.4.2

- **Supervision & Guidance:** Faculty members, MIS Cybersecurity Program, Oakland University

Conflict of Interest Statement
The author declares no conflict of interest.

Data Availability Statement
The EEG dataset used in this study (M3CV) is publicly available at **EEG-based Biometric Competition on M3CV database | Kaggle**. Preprocessing scripts, feature extraction pipelines, and trained models used in this work are available upon reasonable request to the corresponding author.

Ethical Approval
As this study uses an open-access anonymized EEG dataset, no direct human subject involvement was required, and therefore, institutional review board (IRB) approval was not applicable.

REFERENCES

1. Balla A, Habaebi MH, Islam MR, Mubarak S. Applications of deep learning algorithms for Supervisory Control and Data Acquisition intrusion detection system. Cleaner Engineering and Technology. 9(1) (2022). DOI: https://doi.org/10.1016/j.clet.2022.100532.
2. Kumar S. Biometric systems security and privacy issues. In: Kumar S, editor. Leveraging Computer Vision to Biometric Applications. 1st ed: Chapman and Hall/CRC. p. 68-91 (2024) DOI: https://doi.org/10.1201/9781032614663-4.
3. Yang Y-Y, Hwang AH-C, Wu C-T, Huang T-R. Person-identifying brainprints are stably embedded in EEG mindprints. Scientific reports. 12(1) (2022). DOI: https://doi.org/10.1038/s41598-022-21384-0.
4. Fidas CA, Lyras D. A review of EEG-based user authentication: trends and future research directions. IEEE Access. 11:22917-34 (2023). DOI: https://doi.org/10.1109/ACCESS.2023.3253026.
5. Bagheri M, Power SD. EEG-based detection of mental workload level and stress: the effect of variation in each state on classification of the other. Journal of Neural Engineering. 17(5):056015 (2020). DOI: https://doi.org/10.1088/1741-2552/abbc27.
6. Liu X-Y, Wang W-L, Liu M, Chen M-Y, Pereira T, Doda DY, et al. Recent applications of EEG-based brain-computer-interface in the medical field. Military Medical Research. 12(1) (2025). DOI: https://doi.org/10.1186/s40779-025-00598-z.
7. Rashid M, Sulaiman N, PP Abdul Majeed A, Musa RM, Ab. Nasir AF, Bari BS, et al. Current status, challenges, and possible solutions of EEG-based brain-computer interface: a comprehensive review. Frontiers in neurorobotics. 14:25 (2020). DOI: https://doi.org/10.3389/fnbot.2020.00025.
8. Alcaraz C, Roman R, Najera P, Lopez J. Security of industrial sensor network-based remote substations in the context of the internet of things. Ad Hoc Networks. 11(3):1091-104 (2013). DOI: https://doi.org/10.1016/j.adhoc.2012.12.001.
9. Unnisa Z, Tariq A, Din IU, Shehzad D, Serhani MA, Belkacem AN, et al. Threats and Mitigation Strategies for Electroencephalography-Based Person Authentication. International Journal of Telemedicine and Applications. 2025(1) (2025). DOI: https://doi.org/10.1155/ijta/3946740.
10. Yang W, Wang S, Hu J, Zheng G, Valli C. Security and accuracy of fingerprint-based biometrics: A review. Symmetry. 11(2) (2019). DOI: https://doi.org/10.3390/sym11020141.

11. Malgheet JR, Manshor NB, Affendey LS. Iris recognition development techniques: a comprehensive review. Complexity. 2021(1) (2021). DOI: https://doi.org/10.1155/2021/6641247.
12. Wang X, Wu YC, Zhou M, Fu H. Beyond surveillance: privacy, ethics, and regulations in face recognition technology. Frontiers in big data. 7 (2024). DOI: https://doi.org/10.3389/fdata.2024.1337465.
13. Singh JP, Jain S, Arora S, Singh UP. A survey of behavioral biometric gait recognition: Current success and future perspectives. Archives of Computational Methods in Engineering. 28(1):107-48 (2021). DOI: https://doi.org/10.1007/s11831-019-09375-3.
14. Galbally J, Marcel S, Fierrez J. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. IEEE transactions on image processing. 23(2):710-24 (2013). DOI: https://doi.org/10.1109/TIP.2013.2292332.
15. Jia S, Guo G, Xu Z. A survey on 3D mask presentation attack detection and countermeasures. Pattern recognition. 98(1) (2020). DOI: https://doi.org/10.1016/j.patcog.2019.107032.
16. Fontanillo Lopez CA, Li G, Zhang D. Beyond technologies of electroencephalography-based brain-computer interfaces: A systematic review from commercial and ethical aspects. Frontiers in Neuroscience. 14(1) (2020). DOI: https://doi.org/10.3389/fnins.2020.611130.
17. Newson JJ, Thiagarajan TC. EEG frequency bands in psychiatric disorders: a review of resting state studies. Frontiers in human neuroscience. 12(1) (2019). DOI: https://doi.org/10.3389/fnhum.2018.00521.
18. Barry RJ, Clarke AR. Resting state brain oscillations and symptom profiles in attention deficit/hyperactivity disorder. In: Başar E, Başar-Eroğlu C, Özerdem A, Rossini PM, Yener GG, editors. Application of Brain Oscillations in Neuropsychiatric Diseases. Supplements to Clinical Neurophysiology. 62: Elsevier. p. 275-87 (2013) DOI: https://doi.org/10.1016/B978-0-7020-5307-8.00017-X.
19. Karamzadeh N, Medvedev A, Azari A, Gandjbakhche A, Najafizadeh L. Capturing dynamic patterns of task-based functional connectivity with EEG. NeuroImage. 66(1):311-7 (2013). DOI: https://doi.org/10.1016/j.neuroimage.2012.10.032.
20. Yang S, Deravi F, Hoque S. Task sensitivity in EEG biometric recognition. Pattern Analysis and Applications. 21(1):105-17 (2018). DOI: https://doi.org/10.1007/s10044-016-0569-4.
21. Maclean MH, Arnell KM, Cote KA. Resting EEG in alpha and beta bands predicts individual differences in attentional blink magnitude. Brain and Cognition. 78(3):218-29 (2012). DOI: https://doi.org/10.1016/j.bandc.2011.12.010.
22. Jonna ST, Natarajan K. EEG signal processing in neurological conditions using machine learning and deep learning methods: a comprehensive review. The European Physical Journal Special Topics. (2025). DOI: https://doi.org/10.1140/epjs/s11734-025-01606-y.
23. Ahmed MA, Qi D, Alshemmary EN. Effective Hybrid Method for the Detection and Rejection of Electrooculogram (EOG) and Power Line Noise Artefacts From Electroencephalogram (EEG) Mixtures. IEEE Access. 8(1):202919-32 (2020). DOI: https://doi.org/10.1109/ACCESS.2020.3036134.
24. Trigui O, Daoud S, Ghorbel M, Dammak M, Mhiri C, Ben Hamida A. Removal of eye blink artifacts from EEG signal using morphological modeling and orthogonal projection. Signal,

Image and Video Processing. 16(1):19-27 (2022). DOI: https://doi.org/10.1007/s11760-021-01947-w.

25. Alam R-U, Zhao H, Goodwin A, Kavehei O, McEwan A. Differences in Power Spectral Densities and Phase Quantities Due to Processing of EEG Signals. Sensors. 20(21) (2020). DOI: https://doi.org/10.3390/s20216285.
26. Khoshnevis SA, Sankar R. Applications of Higher Order Statistics in Electroencephalography Signal Processing: A Comprehensive Survey. IEEE Reviews in Biomedical Engineering. 13(1):169-83 (2020). DOI: https://doi.org/10.1109/RBME.2019.2951328.
27. Hossain KM, Islam MA, Hossain S, Nijholt A, Ahad MAR. Status of deep learning for EEG-based brain–computer interface applications. Frontiers in Computational Neuroscience. 16(1) (2023). DOI: https://doi.org/10.3389/fncom.2022.1006763.
28. Kumar S, Abu-Siada A, Das N, Islam S. Review of the Legacy and Future of IEC 61850 Protocols Encompassing Substation Automation System. Electronics. 12(15) (2023). DOI: https://doi.org/10.3390/electronics12153345.
29. Rubio S, Bogarra S, Nunes M, Gomez X. Smart Grid Protection, Automation and Control: Challenges and Opportunities. Applied Sciences. 15(6):3186 (2025). DOI: https://doi.org/10.3390/app15063186.
30. Huang G, Hu Z, Chen W, Zhang S, Liang Z, Li L, et al. M3CV: A multi-subject, multi-session, and multi-task database for EEG-based biometrics challenge. NeuroImage. 264(1) (2022). DOI: https://doi.org/10.1016/j.neuroimage.2022.119666.
31. Li Z, Li W, Samson SY, Guo L, Zheng H, Ma J, et al. Fast frequency response reserve planning for power systems considering homogeneous extreme risks. IEEE Transactions on Industry Applications. 59(2):2314-25 (2022). DOI: https://doi.org/10.1109/TIA.2022.3228977.