EEG ANALYTICS MODELS USING AWS

A Project

Presented to the

Faculty of

California State Polytechnic University, Pomona

In Partial Fulfillment

Of the Requirements for the Degree

Master of Science

In

Computer Science

By

Mason Godfrey

2022

SIGNATURE PAGE

PROJECT : EEG ANALYTICS MODELS USING AWS

AUTHOR: Mason Godfrey

DATE SUBMITTED: Fall 2022

Department of Computer Science

Dr. Mohammad Husain
Project Committee Chair
Computer Science _____

Dr. Markus Eger
Computer Science _____

ABSTRACT

A wide variety of tasks are performed with password protected accounts. Passwords are often thought to be insufficient on their own, causing 2-Factor Authentication (2FA) to become significantly more common. However, many current 2FA methods can be easily compromised. This project examines electroencephalogram (EEG) readings as a potential authentication method. EEG readings had been used as a method of detecting emotions in a plethora of environments, but less research has been performed surrounding the uniqueness of EEG readings.

In this project, cloud resources are used in the development of a platform for accepting and storing EEG readings to be compared against machine learning models. When users attempt to log in to a website, their EEG readings are automatically stored. A virtual machine then retrieves the EEG readings and automatically checks if any individual's EEG readings are incorrectly classified as another individual's EEG readings and logs all cases where a user would incorrectly be given access to another user's account.

The cloud-based platform was developed with security as a priority, and was extensively tested to prevent unauthorized access. As such, access to every resource is restricted such that specific conditions must be met for a connection to be allowed. Though the frontend components of the website are easily accessible, the backend is hidden from website users.

Through preliminary testing, we found that the EEG readings are insufficient as a 2FA method when using our initial ML models. While we had a limited pool of participants, our initial ML models were insufficient in their ability to discern between individuals. At times, the model was over thirty percent confident that an invalid user should be granted access into a system. While this could indicate that EEG readings are not unique, we believe that our ML models are insufficient to prove that EEG readings can not be used as a unique identifier for individuals.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1:

INTRODUCTION

As technology continues to becomes increasingly integrated with daily life, it is becoming significantly more common to use password protected accounts to perform a wide variety of tasks. Passwords are used for services that store personal information, allow for the purchase of consumer goods, authorize transferring funds between bank accounts, and more. As time progresses, it is becoming more and more clear that passwords are insufficient to safeguard against account compromises on their own, leading to 2-Factor Authentication (2FA) as a method of providing additional security. While 2FA certainly helps decrease the ability for password-protected accounts to be hijacked, the devices used as the second factor (including phones, fingerprint readers, and face-scanning technology) can easily be lost, stolen, or mimicked making these devices similarly insufficient. A more personalized method of determining the identity of an individual without being susceptible to these shortcomings is required in order to ensure sufficient security.

This project examines electroencephalography (EEG) signal collection as an authentication method to be used within a 2FA system or to replace a 2FA system entirely. The project explores whether EEG signals have similar caveats to other user authentication methods. The hope is that the EEG signal authentication method will only grant account access to the authorized user that the EEG readings belonged to, and that authorization classifications are consistent through multiple attempts under the same environmental conditions.

Another reason that EEG signal collection is so appealing as a 2FA method is that it could be impossible for a third party to coerce the EEG signals from an authorized user. One of the alternate objectives of this research is to determine if the EEG signals taken during times of stress or other environmental factors will be found to result in readings different from those taken under expected conditions.

The approach taken by this research project involves the usage of a cloud-based platform to ensure that authorized users are granted access when (and only when) ac-

cess should be granted. The approach also looks to ensure that EEG readings will never grant access when compared against incorrect EEG models, as this would compromise the account of authorized users and indicate that EEG readings are not unique to individuals. Since current research findings support the notion that EEG readings are personally identifiable, findings to the contrary may lead to significant changes in future research and advancements in the understanding of EEG.

This project successfully implements rapid, cloud-based authentication using EEG readings and converges onto an authentication decision in less than a second. The program performs parallelized EEG analysis against ML models in order to test EEG uniqueness among individuals, though additional ML approaches should be performed through future work to account for the tested ML models' limitations. The research project is ongoing, and future iterations of the project may use improved ML models or implement additional authentication methods.

CHAPTER 2:

LITERATURE SURVEY

History of EEG

The first EEG device, which was developed to read brain electrical activity, was successfully developed by Hans Berger in 1929. The readings of the device consisted of oscillations and waves, which represented the intensities of the readings. Future EEG devices improved based on the available technology, allowing them to be both cheaper to produce and easier to use. The format of the data, oscillation and wave frequencies, has remained consistent despite the technological advances. EEG readings are classified into sub-bands based on the associated frequencies. The Delta sub-band contains the frequencies less than 4 Hz, and are most commonly generated in the frontal area of the cortex. These sub-bands are common during sleep, similar to the Theta sub-band (4 Hz to 7 Hz). However, the Theta sub-band generally occurs in different places throughout the brain. The Alpha sub-band (8 Hz to 13 Hz) is often seen in the occipital portion of the cortex, especially during resting periods. These bands are often associated with calmness and lack of stress. The Beta sub-band (14 Hz to 30 Hz) occurs in both the central and frontal portions of the brain, and are often present during active work or thought. The Gamma sub-band (31 Hz to 100 Hz) is generally observed during anxiety, processing senses, and emotional distress. Higher frequencies have yet to be universally classified into sub-bands. EEG frequencies have a large variety of applications. One traditional application is to determine emotions, including arousal, sleepiness, pleasantness, and unpleasantness. Other emotions may also be retrievable, including happiness, sadness, fear, disgust, anger, and surprise, as well as the emotions derived from each. It is believed that current EEG technology allows for the accurate determination of emotions once enough readings have been collected. Current research papers imply that EEG readings are also unique to individuals, which could allow them to replace passwords entirely.

Machine Learning Applications

Cloud computing is beneficial to the usability of a wide variety of machine learning applications. The usage of cloud computing platforms for neural network applications is especially promising due to the significant computing power of the platforms. This increased performance provides the neural networks with the ability to quickly and efficiently load, test, and evaluate models. In [1], a Brain-Computer interface was developed in order to predict seizures. Epilepsy is a chronic disorder that affects nearly one in a hundred people, and is believed to be caused by electrical stimuli within the brain. The research encountered several challenges, especially since both normal and abnormal readings can vary across patients. Another issue surrounds the project's usage of only intracranial EEG, which collects data at an extremely rapid pace. This problem was partially resolved by performing dimensionality reduction, allowing for the training dataset to be trimmed down to only the most significant components. The cloud component of the project made use of high performance computing, which allowed for significant quantities of data to be trained at a rapid pace. The researchers made use of Elastic Compute Cloud (EC2) in order to train their models, which were over 90% accurate in their classifications based on the authors' proposed algorithm. A variety of other models were also tested including random forest, linear State Vector Machines (SVM), Non-linear SVMs, and a Multilayer Perceptron (MLP) neural network. Accuracies of these other models ranged from less than 70% to 75%. From these findings it is clear that much care must be taken in determining both which features to look at and which models to run the data against. The issue is remarkably similar to the process that will go into the development of this project, even though this project does not delve into seizure prediction. The key differences is that individuals will be identified rather than an individual's condition, and that many models will be trained outside of the cloud platform as opposed to a single model being trained within AWS using high performance computing.

Detecting Emotions

Another application of EEG readings with machine learning is to determine emotional distress. In [3], the objective was to use the binary-tree fusion architecture to determine the emotional state of individuals. The researchers developed and provided helmets that, in addition to providing protection, were capable of collecting EEG information to miners that worked in extreme conditions, such as deep-sea miners and coal miners. The idea was that these miners, who are exposed to stressful situations on a nearly daily basis, would have a high level of anxiety. The authors categorized the emotional distress as being part of either the discrete space (containing emotions such as fear, contempt, disgust, surprise, happiness, and sadness) or the continuous space, which is built based on the dimensional emotion model. In the discrete space, emotions are stored as a vector in multidimensional space; the data has been stored numerically. This emotional data was collected by the EEG safety helmets for parsing on the cloud using the International Affective Picture System (IAPS) library, which can be used to group images and determine emotions. The researchers also attempted to represent anxiety levels felt by miners using quantitative means. As alluded to earlier, the researchers used a binary-tree fusion architecture to retrieve the alpha, beta, and theta rhythms of the miners. While the data collected by the researchers differs from the data to be collected in the proposed project, the research can still be used as a source of inspiration. The binary-tree fusion architecture used by the paper may be useful as a method to verify that users are not under distress. The researchers found that the theta and beta rhythms were related to distress in miners. One of the objectives of the current research project is to ensure that EEG readings are accepted in a consistent environment. This may allow the binary-tree fusion architecture to be used in addition to the verification model to ensure that readings are taken under a stress-free environment, or replace the proposed model entirely. With such a preprocessing method, it would be much more difficult to retrieve readings from a user that is under stress, and thus the resulting classification system, which either accepts or denies that readings are taken from the correct user under the correct conditions, may perform significantly better when determining if

conditions are correct.

Cloud-based Applications

Other research projects also looked at using the cloud to determine the stress levels of individuals, such as [2]. While the objective of determining emotional states of individuals was the same, the methods of doing so and the underlying reasons for the research were vastly different between the two research papers. Brain EEG analysis has the potential to save the lives of patients with brain diseases and disorders, as they can now be remotely monitored to determine their current health conditions at a (relatively) insignificant cost. Brain illnesses can take on a wide variety of forms, such as epilepsy, autism, major depression disorder, and more, each with the potential to generate different EEG readings. In order to ensure accurate predictions, the researchers were forced to perform preprocessing before extracting features from patients. Within their feature extraction, the researchers also reduced the dimensionality of readings, which removes unnecessary rotational information. The project used a Convolutional Neural Network (CNN) due to their ability to classify data with a large amount of noise, making them ideal for usage with EEG data. Again, the objective of the research paper does not parallel this project's objective. However, the usage of a CNN should be considered due to its ability to outperform standard neural networks. However, the performance may not be worth the increased time required to train the model. The addition of convolutional layers may drastically increase the time required to train the model, and since this project proposes using several trained models, this may cause a significant issue pertaining to the time taken, especially if models need to be added or retrained. Still, CNNs should be considered as a possibility.

EEG Deep Learning tools have been developed in order to train models based on EEG data. The company Tremend developed one such deep learning tool and made use of the toolkit provided by scikit-learn to work with csv files containing EEG information to predict monitoring results. While this tool is no longer available on the AWS marketplace, it classified data using both Linear Discriminant Analysis (LDA) and MLP before normalizing EEG data and placing them into either a csv or json file. Despite its

newfound absence on the AWS marketplace, the tool provides additional evidence that cloud platforms are beneficial for their ability to read testing data from the user before training the data against machine learning models. Ideally, however, a csv file would not be required to read input data from a user. In many cases, such as those where live readings are to be taken, csv files generate a security concern since their contents need not be generated live. Therefore, it would be possible for the same csv file to be used for successive login attempts and, if the file becomes compromised, for others to gain indefinite access to the associated account. As such, it would be much more beneficial to collect live readings, which are more difficult to reproduce (although they are notably more difficult to obtain).

CHAPTER 3:

RESEARCH GOAL

The project has multiple goals, each looking to determine the viability of EEG signals as a replacement for 2FA methods. While an additional objective is to determine if the EEG signals accepted while the user is under stress are sufficiently different from EEG signals accepted in other environments, this is not directly tested in the cloud-computing portion of the project. Instead, related testing will be performed by other researchers working on the same project. The goal of the cloud-based component of the project is to create an authorization platform and to determine whether EEG readings are unique on an individual basis. If not, EEG readings collected from two individuals could be incorrectly classified as readings from the same individual causing a major security concern. Each goal can be met using the cloud computing framework.

Authorization Framework

There are two expected outcomes of the creation of a cloud-based authorization system. The first expected outcome is a framework to allow for authorization to be verified using EEG readings with an AWS implementation, including the usage of cloud-based tools. While this project makes use of models implemented by its members, and the models consist of members who are working on the project, the framework does not exclude other model variations that may be included in future research. That is, the framework has been specifically designed to accept and use models regardless of their type, and the framework has been designed to generate as little coupling as possible. Future projects, research or otherwise, may use the framework to improve upon it for usage in real world applications. It is very likely that the most common initial real world applications will require very high security due to current limitations in EEG availability and ease-of-use, but the applications that use EEG readings may expand as EEG collection methods become easier to use and cost decreases.

EEG Uniqueness

The second expected outcome is a better understanding of the relationship between data entries taken by multiple individuals. While it is suspected that EEG readings

are unique to individuals by current research projects, this project is expected to either reinforce or disprove that claim. Readings collected by individuals are tested against every stored model. If the incorrect model determines that access should be granted to the individual providing the readings, this heavily indicates that either the model is insufficient and should be further trained or that EEG readings are not necessarily unique to an individual. Such a conclusion carries heavy weight, and has the potential to drastically change the course of EEG related research. As such, this relationship data will need to be heavily scrutinized to determine its meaning and validity before the findings of this project are made publicly available. If the project finds and publishes that EEG readings are not unique on an individual basis, the paper will undoubtedly be the source of many future research projects.

CHAPTER 4:

METHODOLOGY

First and foremost, this project tests whether Machine Learning algorithms can be used to determine whether EEG signals act as unique identifiers for individuals. More specifically, this project integrates a preliminary eXtreme Gradient Boosting (XGB) classifier module developed as a separate project component to accept EEG readings as input, determine how similar the readings are to other readings from the individual under normal conditions, and output how confident the XGB classifier is that the readings belong to the individual. While the project had been designed for Neural Networks to determine how to classify the readings, the cloud-based implementation's low coupling allows for easy integration with the XGB model. The model works through the usage of decision trees as opposed to the logistic regression often used by Neural Networks. Such functions include linear and logistic regression. An activation function may be used in order to ensure that the output is the XGB classifier's certainty that the EEG signal is associated with the individual during ideal conditions. Afterwards, the finalized model can be derived based on the data. Testing is performed using the following AWS cloud resources:

- Elastic Beanstalk (EB)
- Elastic Compute Cloud (EC2)
- Simple Storage Service (S3)
- Relational Database Service (RDS)

Cloud Resources

My unique focus surrounding the project involves the development of an RDS instance which stores data pertaining to Machine Learning models after their initial creation and training in a notebook tool. The notebook tool used to train and develop the ML model is Jupyter Notebook. After the creation of the RDS instance, I continued on to the development of an EB instance to create an interface between a website's html and css frontend displayed to the user and the website's python-based backend program

that is hidden from the user. The EB instance communicates directly with the RDS instance and, when provided with an identifier for individuals that have a model, performs verification of the readings against the model so long as the model exists. These calculations occur using Python within the EB instance, and is entirely inaccessible to users of the site. Within the Python program, readings are run against the model and an output (in the form of a confidence) is achieved. The algorithm then provides its confidence that the readings taken from the user indicate the user as the model's owner. The confidence is expected to change if the readings are taken under differing environmental conditions. The confidence output is always expected to be a float with a value between 0 and 1, inclusively. Regardless of the final model type, if the model is confident that the readings from the user are definitively similar to those of the authorized user, the EB instance signifies that access should be granted into the system; otherwise, the EC2 instance signifies that access should not be granted. In both cases, the numerical values for the confidence would remain hidden to the user in the real world scenario. The less information provided to the user, the more secure the system would be. However, since this project has a research focus, the confidence of the model is provided to the user for testing and development purposes. Additionally, other models can be easily tested against the initial data to see if any false positives occur. If so, EEG readings are insufficient as a method of uniquely identifying individuals or the models being used to classify individuals is insufficient. This process is done by recording EEG readings accepted by the EB instance into the RDS instance and passing them into an EC2 instance at a later time. The EC2 instance then runs every ML model against every user's EEG readings to find false positives and log them in the EEG database. Figure 1 provides the layout of the cloud-based implementation (note that an S3 bucket is used to store and retrieve the files referenced in the RDS database).

Elastic Beanstalk

The EB instance can be thought of as a cloud storage container that also functions as a website and virtual machine. The EB instance contains an S3 bucket in order to store backup files and folders. S3 buckets have a similar hierarchy to most modern operating

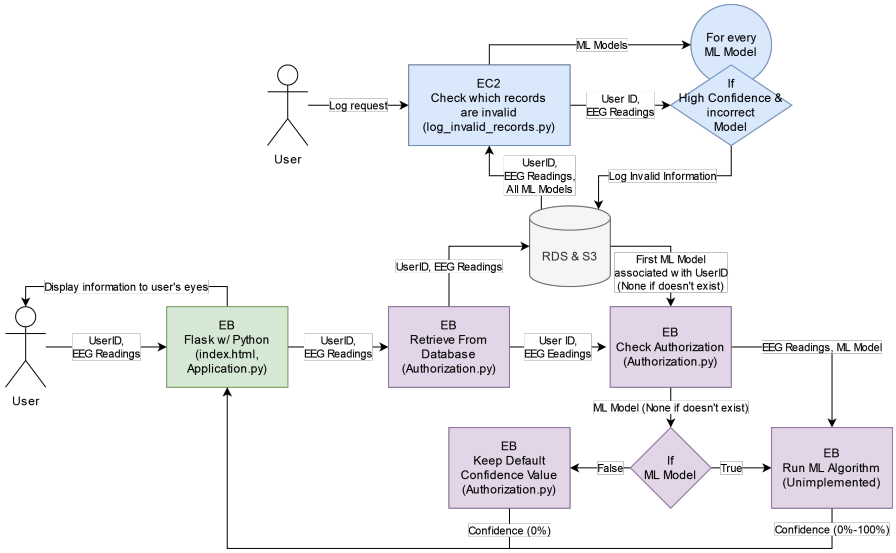

Figure 1 : Proposed EEG Analytics Models using AWS

systems. Generally, buckets do not restrict the extensions of files stored within them, meaning that practically any file extension can be given to files within an bucket. This naturally allows for html files to be stored within buckets and, since S3 buckets are accessible from any location with an Internet connection, can be used to host websites. Static website hosting, however, is not sufficient to run the back-end Python program used by this project. The back-end for the instance works as a Virtual Machine, and allows for the usage of Python alongside Flask without needlessly exposing back-end operations to website users. The website consists of a single web page that accepts the ID and EEG readings of a user and outputs the confidence that the user's readings fit against the model with the user ID key in the RDS instance. When the readings are passed into the system, the user ID and EEG readings are also logged to the database. The first iteration of the website will use a file containing the EEG readings but, if possible, this will be modified to instead accept live readings from a user. Changing from file-based readings to input-based readings may be exceptionally difficult due to the research and experimentation required to implement a method of accepting the live readings.

Relational Database Service

Only a single RDS database is required to store every EEG model. The RDS database is useful since data is not redundant and, importantly, isn't hosted in either the EB instance or the EC2 instance. This ensures an additional layer of security as the user has no possibility of retrieving models directly from the EB instance and ensures that the EC2 instance isn't unnecessarily holding EEG model information. In general, it is bad practice to store temporary files on an EB instance. Finally, an encryption algorithm is used to protect the data being stored within the RDS database as the models being stored inside contain extremely sensitive information. Assuming brainwaves are indeed unique on an individual basis, a malicious party gaining access to an individual's unencrypted brainwave information is similar to stealing their social security number. The information within the database that is the most vital to encrypt is the Machine Learning model and user EEG readings. A user's Machine Learning Model can be thought of as a client's lock as opposed to their key, while the keys are the EEG readings retrieved from the EB instance. The EEG model lock is passed into the EC2 instance where it is compared against the EEG reading to determine if a login attempt should be successful. The implementation also required the correct username, as access should not be granted unless the user the readings belongs to is the user that is attempting to log in.

Elastic Compute Cloud

The EC2 instance, which can be thought of as a virtual machine being hosted in the cloud, distributes the input data from the RDS instance using parallelization techniques and the MPI4Py Python module. The EC2 instance then performs simultaneous calculations on the data using virtual processing. The EEG readings accepted in the EB instance is run against every model in the RDS database simply by executing a command remotely. This process automatically ensures that every model is distributed into the virtual processors of the EC2 instance (with as even a distribution as possible) and that all models (other than the model associated with the correct ID) indicate false positive decisions only to the database through the generation of a new table entry. An even

distribution is preferred as each processor in the virtual machine should take roughly the same time to perform all necessary computations. By performing these calculations outside of the EB instance, the instance evades the downside of forcing other users to wait for the EC2 machines to be available before they are allowed to log, and assures that availability does not depend on how long it takes the final machine to create its findings. Instead, the EC2 instance performs these calculations separately using the same data. This allows users to attempt to login to the system while the EC2 instance is running. While both communicate with the database, their communications may be done simultaneously without generating a conflict within the SQL database or files stored within the S3 bucket.

Machine Learning Approaches

Neural Networks and XGB classifiers are not the only machine learning methods being considered during the development of this project. The XGB classifier is being used preliminarily as research into other promising machine learning approaches is being actively performed. A variety of other potential methods may prove useful, and are thus being continually considered. The project is continually updated and developed by other researchers to create stronger, more useful machine learning models. Part of the ongoing project involves researching the benefits and drawbacks of alternate Machine Learning methods to determine which are the most promising. The usage of more advanced Neural Networks (such as CNNs) is being considered due to their ability to generate accurate predictions for data with a large amount of noise.

While not a replacement for neural networks, the binary-tree fusion architecture is also being considered during preprocessing to ensure that data being passed into models is from an the expected environment (the individual has the expected level of stress or the expected lack of stress). In other research, the binary-tree fusion architecture demonstrated its usefulness in determining the stress level of individuals during preprocessing and demonstrated that it can be used to either prevent passing readings if they are from an unexpected environment or be used to indicate the environment the readings were taken from. Other preprocessing methods, such as reducing the dimensionality of

input data, are under consideration due to their potential to both decrease the training time requirements without severely affecting the accuracy of the model.

Regardless of which model type is used, all future models are expected to be created using Python along with the PyTorch library. In the current implementation, the EEG readings used as input are first parsed to remove noise created through blinking, wind, head movements, and other factors. This practice is expected to continue as models are developed. The dimensionality of these parsed readings is then determined in order to reduce the number of columns required for the program's output. By removing columns that don't provide much information, the speed at which testing can be performed is increased along with the efficiency. Analysis is also being performed to determine how much reading data is required to generate an accurate model that is capable of accurately determining whether a user should be authorized. The final model will have only the most significant features and require a length of input data that allows for accurate decisions about whether the individual providing the readings is indeed the authorized user.

Once the most significant features are determined, work on the finalized model may begin. While the current preliminary model is in the form of a XGB classifier, solutions that only require a single machine learning model to be trained regardless of the number of participants should not be discredited for the reasons discussed previously. K-means clustering may prove to be effective due to its ability to include several data points from several users simultaneously. K-means clustering may be able to determine the identity of the individual providing the readings, regardless of who they're attempting to be logged in as. As such, the data received in the previous step will be crucial in determining how the new model should be built and which Machine Learning algorithms it should make use of. The current implementation of this project was developed using the preliminary XGB classifier discussed previously.

After the XGB models had their initial training, they have been placed in an S3 bucket and linked to by the cloud-based implementation using an RDS instance by storing the names of the model files, the associated usernames, and the associated IDs. EB

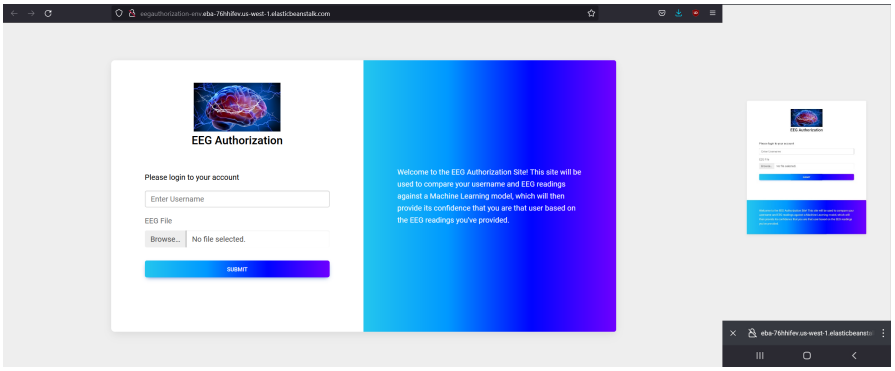

Figure 2 : EB website accessed from PC, mobile web browsers

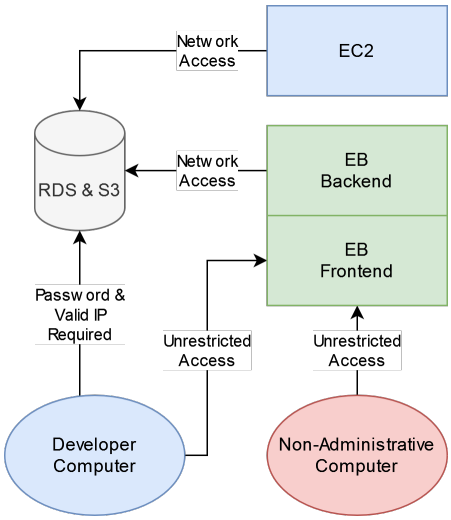

Figure 3 : Valid communication paths under current IP restrictions

using Python and Flask is used to host a website that accepts EEG readings from users and perform computations on the data against the associated XGB models. Finally, an EC2 instance is being used to take data present in the RDS database instances and determine whether the user is authorized to access the system. If the instance determines access should be granted under the incorrect model, this result is automatically logged in the database.

To increase security, measures which restrict access to those who should be authorized to access the system have been added to the cloud-based resources. More specifically, invalid IP addresses are prevented from accessing the database even if they have access to the database password. This is possible because AWS allows for restricting access based on IP addresses, valid ports, and even to machines on a private virtual network (such as other AWS resources). Due to the nature of the data being stored by

the RDS instance, such security measures are vital. Even a single leaked EEG reading can prove devastating and may result in serious lawsuits, especially since research into the significance of EEG readings is still ongoing.

CHAPTER 5:

EVALUATION

Since the proposed project encompasses several areas, great care is being taken to ensure that no individual component has an error that tampers with the results. As such, in addition to a final evaluation, individual components of the project are constantly undergoing evaluation by all project members. Since each project member focuses on a different component of the project, the cloud-based implementation makes use of a small portion of the project's deliverables, namely the EEG models developed by other members of the group.

Scalability of Resources

While other methods of hosting an EEG authentication system are viable, the cloud computing architecture has been selected due to its superior scalability. While locally hosted servers would similarly allow users to authenticate into a system, such an approach would not be easily expandable to encompass multiple networks. One approach of doing so would be to host several authentication servers, but doing so would cause increased server running costs and have the potential for instances to have inconsistent versions or mismatched data. The website, database, files, and even virtual machine instances in one network would be inconsistent with other networks. While such an issue can be minimized by communicating with other networks, hosting the website using a cloud platform alleviates inconsistencies entirely. By using a cloud-based authentication platform, there will be no need to add additional servers, guarantee data consistency, or add additional resources. The proposed system allows many users to authenticate through the system simultaneously, and users may attempt to authenticate so long as they have an internet connection.

RDS and S3 were used to store information for several reasons. While the information could have instead been stored within both the EC2 instance and EB instance, this would cause data to be stored in two separate locations and could lead to inconsistent data storage. The EC2 instance and EB instance also have limited data storage and, while this would cause no issues for small amounts of data, available storage space

would run out quickly if a large amount of access attempts are made. RDS also allows for querying to augment data. Queries have the potential to combine information related to multiple tables, allowing for analyses containing information pertaining to multiple data entries to be displayed using the same interface.

Attack Surfaces

While cloud resources are useful for their scalability, they also generate large attack surfaces. By being accessible through an internet connection, the resources expose themselves to an extremely wide variety of devices and users, many of which may have malicious intentions. Since this system is meant to be used for environments where heightened security is required, the system should be as secure as possible.

Attackers looking to gain access to a user's account are likely to target the machine learning model associated with that user. One method of doing so is by determining how the ML model is trained and creating a file to compromise the system. However, a malicious party may also obtain or intercept EEG readings that would grant access to the system and use the readings in a replay attack. It is impossible to determine whether the EEG readings have just been taken, whether the correct user is sending them, and whether the readings had been modified. As such, this form of attack may be devastating if performed. This form of attack could easily be mitigated by pairing the ML model with an additional 2FA method, such as a password or SMS requirement. If the EEG readings were paired with a password, an attacker would need to know the password before an attack would succeed. Requiring usage of an SMS code is more secure as the attacker would need the would-be victim's phone. While neither case makes a replay attack impossible, they significantly strengthen the system and drastically reduce the viability of authentication-based attacks. Given the high security applications this system will likely be used for, as well as the amount of time required for EEG collection, adding an additional authentication factor will make little difference in the amount of time required for a successful authentication to occur.

Attackers looking to gain access to the data being used by the program, which consists of machine learning models and EEG readings, are likely to attack the S3 bucket

and RDS instance which store the associated records. While attack surface has been reduced through the usage of IP access restrictions and the requirement of a password, it is entirely possible for an attacker to spoof an IP address and predict the password required to access the system. As such, additional restrictions can be placed on the affected resources. For example, certain IP addresses are allowed to access the system, but the IP addresses that are allowed to connect can be limited to only the machines within the virtual network the S3, RDS, EC2, and EB resources share. This would mean that only the resources that are vital to the network can communicate with each other, preventing a direct attack through the internet. The downside to this approach is that developers must be connected to the EC2 instance to see changes in the network, so developers may want to develop a test network for development purposes.

Project Development Procedure

While insignificant relative to the project as a whole, EEG models have the potential to drastically change the findings of the project. As such, the models are only accepted into the S3 bucket and referenced in the RDS instance once they are trained sufficiently. The models must be trained against sufficient data, the data itself must be trained against a sufficient number of other users, and all data for a particular individual must be taken under the same environmental conditions. While the data used to train the model against is certainly important, many more considerations must be made to ensure the integrity of the model or models. The model's final loss must be sufficiently small, and any model should be trained for the same number of epochs, with the same learning rate, with the same loss criterion, using the same layers and the same batch size. If the model or models are trained insufficiently, they will be rejected. However, if any model is trained more or with different data than other models, they must be heavily considered before they are accepted into the S3 instance and referenced from the RDS instance.

Project Evaluation Procedure

Each component of the cloud-based architecture undergoes constant evaluation. The EB instance is tested by attempting to access any other files that are physically present in EB back-end. One method of doing such testing is through attempting to access their

links directly, but additional checks against the EB instance allow it to deny access if users should be unable to access a page under normal circumstances. The components of the website are constantly scrutinized to determine whether it is possible to breach the RDS database or the EC2 instance from within the EB instance, though the ability to gain such access is unexpected. Gaining access to any information on the EC2 instance, or even gaining knowledge of the existence of the EC2 instance, can have devastating effects on the security of the system by exposing an additional attack surface. If any issues are discovered, any components involved with the vulnerability will be modified in order to remove the vulnerability.

The RDS database should be limited in the operations it can perform. Communication with the EC2 instance should be limited to providing the associated model, EEG readings, and ID information to the EC2 instance or adding an additional entry from the EC2 instance if a false positive occurs involving authorizing an individual where access should not be granted. The RDS database should have limited communication with the EB instance as well. It should be able to accept a User's ID and EEG readings and return the first ML model associated with the user. As such, security-related testing includes simulated breach attempts will be performed to see if it is possible to generate commands externally, and to determine if these commands can affect the database in any way. If any additional commands can be made, or if it is possible to create or retrieve database records externally, then the database will be modified to remove the vulnerability as best as possible.

The final evaluation of the cloud-based implementation is based on whether the program accurately identifies whether EEG readings belong to a user, and how many times it logs a false success. While accuracy is certainly important, it relies on how confident the ML model is that a user should be granted access, and it is more preferable to deny access to an authorized user than to grant access to an unauthorized user. However, if the program logs successes where failures should be generated, then either the model used to identify individuals is incorrect or EEG readings are not unique per individual. Unfortunately, determining whether the model is sufficient to prove or disprove EEG

uniqueness may prove to be exceptionally difficult. If model indicates that EEG readings are not individually unique, all project members will be made aware and each will perform an analysis to determine how the discrepancy may have been caused. Depending on the findings of the project, the project researchers will discuss findings with their committee members to determine how to proceed in case of a possible error in data interpretation.

Findings

Through the development of this project, it was found that the models provided for usage in EB authentication and EC2 analysis were insufficient to prove or disprove the uniqueness of EEG readings. While they are able to distinguish between individuals when using provided csv files containing EEG readings from users, the XGB models had multiple weaknesses related to overfitting and malicious input. Since the same files are used for training, testing, and evaluation, there is no way to guarantee that data has not been used during other parts of the development process. For example, if a set of readings were used during the training process, there is no way to guarantee that the same data won't be used during the evaluation process using the current implementation. It has also been discovered that data is being shuffled before the training process is allowed to begin, meaning the model is unable to learn based on sequential EEG reading patterns. This may significantly reduce the ability of the ML model to recognize patterns in EEG readings and result in a much weaker model.

Testing has also been performed to test the ease at which malicious input is generated. Since the website uses EEG files as opposed to accepting live readings, files that would not normally allow access into the system may be modified to instead grant access. In the current ML implementation, the model predicts whether readings belong to a user every few rows of input. These predictions are binary, meaning they always result in either a 'true' or 'false' value, where true indicates that access should be granted to the system and where false indicates that access should be denied. The results of all predictions are then combined and averaged out to generate a final confidence score. This allows for both data repetition and data length attacks. In a data repetition attack,

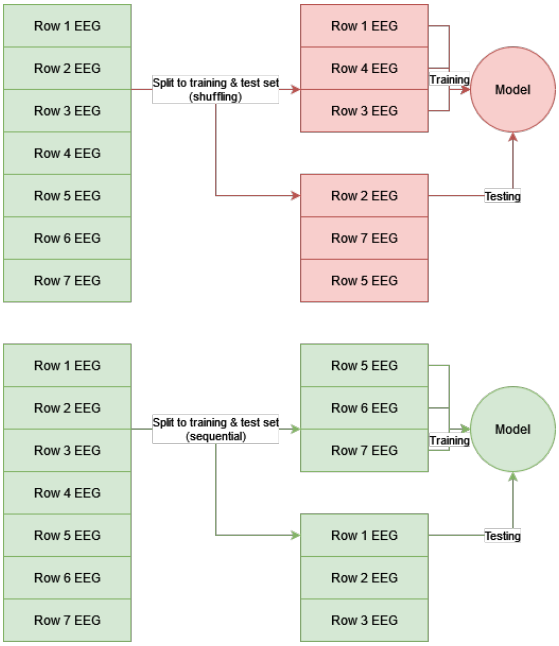

Figure 4 : Possible training and test set splits with and without shuffling

confidence will always increase if rows that generated a 'true' decision are repeated. Since data is stored within a CSV file, one must simply find the rows that generate a positive decision and repeat those rows to ensure access will be granted to the system. In a data length attack, an attacker may simply reduce the size of the CSV file to contain less data. If rows that would generate a 'false' decision are removed from input to the model, the confidence of validity will drastically increase. This attack is partially mitigated by the website's implementation, which checks the length of the input file before allowing access to the system. However, such an attack should be instead mitigated during the model's training process.

CHAPTER 6:

FUTURE WORK

Multiple components of the project should be taken into account both by developers looking to continue implementation using this project and by researchers looking to create similar cloud-based architectures. The EB website is limited to using csv files which contain EEG readings as input. However, there are no implemented methods to guarantee when the EEG readings were taken. Readings may have also originated from another source, and are susceptible to malicious input. Rather than accepting csv files containing EEG readings, the website should be able to accept live readings. If implemented properly, this would guarantee that all readings were created at the time of usage by the EB instance, as well as ensuring that EEG readings originated from a headset. Live readings are very difficult to spoof. In real-world applications, confidence should never be displayed to the user. The malicious attack discussed during the evaluation section would have been far more difficult had confidence been kept hidden from the user, or if the user was allowed limited login attempts.

Live EEG Authentication

Future research projects should consider the usage of headsets for live EEG reading collection and authentication as the csv files used for the current implementation are susceptible to malicious input. If an attacker can submit a file for authorization, it is difficult to verify that the file's contents haven't been used before, and an attacker may modify the file to grant a heightened confidence rating. While live EEG readings from a headset are more secure, they are significantly more difficult to prepare. The acceptance of live readings requires that all preprocessing must occur on the website, which will increase the time required for an authentication decision and require that larger files be uploaded to AWS. EB has restrictions on the amount of data that can be uploaded at a time, and unprocessed EEG data is notably large. The system is expected to handle only seconds of EEG data at a time, meaning the readings received must be near perfect. Another issue involves the fact that EEG readings change based on environmental factors. A user may be denied access since they recently had a caffeinated beverage, are

afflicted with a cold, or even if they are in a bad mood. Users may also be attempting to access the system from a location where they are unable to provide EEG readings. Given the security requirements and expectations of a particular system, such access attempts may be denied automatically. However, certain projects may wish to allow the user to login to the system without EEG readings. This could be done through the usage of traditional 2FA methods, such as a password and SMS pair, but should only be pursued as a fallback authentication method.

Machine Learning Limitations

The preliminary XGB ML model was also found to be weak, and incapable of preventing malicious modifications to input data. Decisions should be made with awareness to data length, as well as data repetition. The strength of the model should also be increased by ensuring the usage of separate training, testing, and evaluation sets. Data should be fed to the ML model sequentially, such that no shuffling occurs with input data. Other approaches should also be considered, such as a template-based approach where input EEG readings is compared against stored EEG readings provided by the same user. This would allow a single ML model to perform all decisions. Other types of ML model, such as classifiers or neural networks, may also prove more effective than those used during the development of this project.

REFERENCES

[1] Mohammad-Parsa Hosseini et al. “Cloud-based deep learning of big EEG data for epileptic seizure prediction”. In: *2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*. Dec. 2016, pp. 1151–1155. DOI: 10.1109/GlobalSIP.2016.7906022.

[2] Hengjin Ke et al. “Cloud-aided online EEG classification system for brain healthcare: A case study of depression evaluation with a lightweight CNN”. In: *Software: Practice and Experience* 50.5 (2020), pp. 596–610. DOI: https://doi.org/10.1002/spe.2668. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/spe.2668. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/spe.2668.

[3] Md. Mustafizur Rahman et al. “Recognition of human emotions using EEG signals: A review”. In: *Computers in Biology and Medicine* 136 (2021), p. 104696. ISSN: 0010-4825. DOI: https://doi.org/10.1016/j.compbiomed.2021.104696. URL: https://www.sciencedirect.com/science/article/pii/S001048252100490X.