Project Synopsis

on

**Elemental Index Finder**

Submitted as a part of course curriculum for

**Bachelor of Technology**

in

**Computer Science**



**Submitted by**

Manan Garg

1900290120059

Manav Verma

1900290120061

Ashish Kumar

1900290120027

**Under the Supervision of**

Mr. Gaurav Singh Rawat

Assistant Professor, CS

**KIET Group of Institutions, Ghaziabad**

**Department of Computer Science**

**Dr. A.P.J. Abdul Kalam Technical University**

**2022-2023**

**DECLARATION**

We hereby declare that this submission is our work and that, to the best of our knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgement has been made in the text.

Signature of Student

Name: Manan Garg

Roll No.: 1900290120059

Date: August 30,2022

Signature of Student

Name: Manav Verma

Roll No.: 1900290120061

Date: August 30,2022

Signature of Student

Name: Ashish Kumar

Roll No.: 1900290120027

Date: August 30,2022

**CERTIFICATE**

This is to certify that Project Report entitled “Elemental Index Finder” which is submitted by **Manan Garg, Manav Verma and Ashish Kumar** in partial fulfilment of the requirement for the award of degree B. Tech. in Department of Computer Science of Dr A.P.J. Abdul Kalam Technical University, Lucknow is a record of the candidates own work carried out by them under my supervision. The matter embodied in this report is original and has not been submitted for the award of any other degree.

**Date: August 30,2022 Supervisor Signature**

Mr. Gaurav Singh Rawat

Assistant Professor, CS

**ACKNOWLEDGEMENT**

It gives us a great sense of pleasure to present the synopsis of the B. Tech Mini Project undertaken during B.Tech. Third Year. We owe a special debt of gratitude to Mr. Gaurav Singh Rawat, Assistant Professor, Department of Computer Science, KIET Group of Institutions, Delhi- NCR, Ghaziabad, for his constant support and guidance throughout the course of our work. His sincerity, thoroughness and perseverance have been a constant source of inspiration for us. It is only his cognizant efforts that our endeavours have seen the light of the day.

We also take the opportunity to acknowledge the contribution of Dr P. K. Singh, Head of the Department of Computer Science, KIET Group of Institutions, Delhi- NCR, Ghaziabad, for his full support and assistance during the development of the project. We also do not like to miss the opportunity to acknowledge the contribution of all the faculty members of the department for their kind assistance and cooperation during the development of our project.

Date: August 30,2022

Signature:

Name: Manan Garg

Roll No.: 1900290120059

Signature:

Name: Manav Verma

Roll No.: 1900290120061

Signature:

Name: Ashish Kumar

Roll No.: 1900290120027

**ABSTRACT**

We will make a website to categorize the environmental characteristics of an area with the Map of that area. We will display the AQI of the air, water quality based on the dissolved Oxygen, pH level of the water and other things to check if the water is suitable for drinking or not. Also, the level of water level beneath the ground level is very important because if the water level is too low, the water pressure will be very less. Our website will target the people who shift from one place to another or who change homes frequently. We will try to make them informed about the natural characteristics of that area and help them decide if living in a particular area is safe for them or not. We will also try to calculate the probability of the degradation of the natural sources around an area with the help of the data from the past 5 years. We will predict the quality of the sources in the next 5 years. We will be using Machine Learning for prediction of data.

**LIST OF FIGURES**

1. Flowchart of the Model …………………………………………………...24
2. Flowchart of Website...…………………………………………………....25
3. DFD of Project ……………………...…………………………………….26

**TABLE OF CONTENT**

DECLARATION ………………………………………………………………... 2

CERTIFICATE …………………………………………………………………. 3

ACKNOWLEDGEMENT ………………………………………………………. 4

ABSTRACT ……………………………………………………………………... 5

LIST OF FIGURES …………………………………………………………....... 6

CHAPTER - 1 INTRODUCTION …………………………………………….... 8

* 1. INTRODUCTION …….……………………………………………. 8
  2. PROBLEM STATEMENT ………………….…………................... 8
  3. OBJECTIVE ….………………………………….…………………. 8

CHAPTER – 2 LITERATURE REVIEW …………………………………… 9-22

CHAPTER – 3 METHODOLODY ………………………………………… 23-26

3.1 METHODOLOGY …………………………………………………………23

3.2 TECHNOLOGY USED ……………………………………………………23

3.3 FLOWCHART ………………………………………………………….24-25

3.4 DFD …………....……………………………………………………………26

CHAPTER – 4 MODULES ……………………………………………………..27

4.1 FEATURES ………………………………………………………....27

CONCLUSION ………….……………………………...………………………28

FUTURE SCOPE ……………………………………………………………….29

REFERENCES ………………………………………….…………………. 30-31

**CHAPTER – 1**

**INTRODUCTION**

**1.1 INTRODUCTION**

The focus of the project is to help individuals gain the most necessary information of current times regarding the pollution levels and the conditions in which a minimum increase can become a major factor in determining the life or death of a person. Our project focusses on keeping a person informed about the quality of natural resources i.e., soil, water, and air. We will try to keep the people informed about the natural resources. Our website will make a prediction about the level of these resources in the next five years with the help of Machine learning using the dataset of past five years. It will help an individual in choosing a correct locality or place to live.

* 1. **PROBLEM STATEMENT**
* Nowadays a major determining factor while residing in an area is the conditions of the area that is the quality of air, water, and soil.
* The quality of these three determine the life expectancy of a person as well
* The structure standing in the area.
* The increase in the current pollution level is the cause of various diseases and then eventually lead to death.

**1.3 OBJECTIVE**

To make a website to give the quality of the air, water and soil including ground water level etc. of an area through a map and give a rating of the area on the data as well as give the suggestion and prediction of the conditions in the future.

**CHAPTER – 2**

**LITERATURE REVIEW**

**2.1 Detecting Malicious Behaviors in JavaScript Applications**

Detecting Malicious Behaviors in JavaScript Applications JavaScript applications are widely used in a range of scenarios, including Web applications, mobile applications, and server-side applications. On the other hand, the flexibility of the JavaScript language makes such applications prone to attacks that inject malicious behaviors. We prototyped our solution on the popular JavaScript engine V8 and used it to detect attacks on the android system. Our evaluation shows the effectiveness of our approach in detecting injection attacks to JavaScript applications [1]. In fact, the flexibility of the JavaScript language makes such applications even more prone to attacks that inject malicious behaviors. In JavaScript applications, the anomalous behaviors by injected code break the execution integrity of the victim app, resulting in different behaviors from benign ones in the way they are activated. For hybrid Android apps, we observed that the caller-callee relationship of JavaScript functions can provide information to distinguish benign and malicious calls to these APIs. Our approach is based on function activation information of the apps and system events. In this section, we introduce the runtime environment of JavaScript Apps. Based on that, we use a motivating example to demonstrate how the function-activation relationship is effective in differentiating anomalous behaviors. A. It also offers a way to deal with the requirement of systems that contain the JavaScript engine in a sandbox. The static layouts and dynamic behaviors of these hybrid apps are implemented in Web languages, e.g., HTML, CSS and JavaScript. Intercepting Function Activation We leverage the mechanism of the exception handling in V8 to extract function-activation information. We intercept and rewrite the JavaScript code of the apps, such that it throws an exception in every function. In this way, we get the function call stack during the execution of the rewritten code. Specifically, for every JavaScript function of a given app, the dynamic rewriter inserts code to get the JavaScript call stack at the beginning of the function and log the entering event of the function and log the exit event at the end of the function. In the source code of Android, the function evaluate() (which is in the source file Webcor/bindings/v8/V8Proxy.cpp) is where WebView starts to execute JavaScript code. We modify this function to intercept and rewrite JavaScript code before passing the instrumented code to V8.B. In the WebKit component of the Android system, we instrument hooks to extract the function information. More specifically, for the app's local behaviors triggered by calling certain PhoneGap APIs, we modify the function npObjectInvokeImpl() in the source file WebCore/binding/v8/V8NPObject.cpp to extract the API calls made by PhoneGap, as well as the corresponding system resources that the app requests. For the app's network behaviors, we modify the function createRequest() in the source file WebCore/xml/XMLHttpRequest.cpp where the XML HTTP requests are generated, to extract the information about Ajax requests.[2] Evaluation In this section, we evaluate the effectiveness and performance of our solution. A. Effectiveness In order to evaluate the effectiveness of our solution, we deploy our approach to model the behaviors of real-world popular hybrid Android apps and demonstrate its capabilities in anomalous behavior detection with simulated code injection attacks on those apps. The original behavior model for Rewarding Yourself is shown in Figure 6, where nodes are states represented by related information of JavaScript functions in the app, and the arrow from a state to another denotes the transition between these two states. Discussion of Limitation The detection in our approach is based on function call relationship and triggering events. Despite the effectiveness shown by the case studies, it is possible for attackers to inject the code and active it under the same condition as in the original app. In such cases, our approach may miss the injection within a target function [3]. Using JavaScript-based technologies to build mobile apps is a popular technique in the web and social network infrastructure. However, the flexibility of the JavaScript language introduces new security challenges in these platforms. Our prototype detection system can automatically build the behavior models for hybrid apps to detect anomalous behaviors.

**2.2 Machine Learning-Based Predictive Techno-Economic Analysis of Power System**

This paper proposes a predictive techno-economic analysis in terms of voltage stability and cost using regression-based machine learning models and effectiveness of the analysis is validated. Predictive analysis of a power system is proposed to address the need for faster and accurate analyses that would aid in the operation and control of modern power system. Predictive ML models for two modified IEEE 14-bus and IEEE-30 bus systems, integrated with renewable energy sources and reactive power compensation device are proposed and developed with features that include hour of the day, solar irradiation, wind velocity, dynamic grid price and system load. An hour-wise input database for the model development is generated from monthly average data and hour-wise daily curves with normally distributed standard deviations. The data feasibility tests, and output database generation is performed using MATLAB. Linear and higher order polynomial regression models are developed for the 8760hr database using Python 3. 0 in JupyterLab and a best-fit predictive ML model is identified by analysing the coefficients of determination. The voltage stability and cost predictive ML models were tested for a 24hr input profile. The results obtained and the comparison with the expected values are furnished. Prediction of the outputs for the test data validate the accuracy of the developed model [4]. Voltage stability is defined as "the ability of a power system to maintain acceptable voltage in the system both under normal conditions and also after being subjected to a disturbance". The stability and reliability of the power system can be improved by providing decision making support in real time [4]. This paper proposes a regression-based machine learning approach to predict both voltage stability and cost of a power system with integrated renewable energy sources and reactive power compensation devices. 2) Prediction of voltage stability of a system and the cost of energy purchased from the grid for faster and precise analysis and control. Developing a Machine Learning model is done in three major stages Most crucial and sensitive part of the model development is to create a valid and accurate dataset. The generated input-output database is then used to develop an ML model by a process of training and testing. The accuracy of the developed model and its prediction is also greatly affected by the features chosen for training a model. A considerable part of the updated database is used to train an ML model, while the remaining data is used to test the developed model. Training the model involves the development of an equation. that relates the input and output variables. Testing, on the other hand, involves computation of the output for the test input data using the developed FIGURE 4. Accuracy of the model is determined by comparing the predicted output with the actual output of the test dataset. A well trained and accurately developed ML model can be used for predicting the output for any futuristic system input condition. The 8760hr input-output database generated is then used to develop ML models through a series of steps which include feature selection, ML model training, testing, and validation. Four ML models namely multi-linear regression and polynomial regression models of order 3, 4 and 5 are developed, and a best-fit model is chosen for the proposed predictive analysis [5]. The IEEE-14 bus system is modified with the incorporation of Renewable Energy sources and a FACTS device as shown in Fig.3. The first factor is the L-index of the bus which indicates the voltage stability of the local bus and the second factor is the load at a particular bus. The FACTS device, STATCOM is a reactive power compensation device when added to the system improves the voltage of the system. In the IEEE 14-bus system, STATCOM is added to bus no 11 based on the voltage profile obtained from the Newton Raphson load flow analysis. Similarly, the IEEE 30-bus system is modified with the incorporation of PV, wind and STATCOM as shown in Fig.4. The renewable Energy sources, PV and wind are added to Bus no 21 and 7 respectively. The STATCOM is connected to bus no 22. [5] The entire process is presented with the help of flow diagram as represented in Fig.5. By analyzing the correlation between features and output, feature selection is performed. This final model is validated by the prediction of voltage stability and cost for a futuristic 24-hour profile. All the ML models for the predictive analysis are developed using the 8760hr database generated for the study. For the prediction of voltage stability, L-index is considered as one of the output variables to be predicted and analyzed. The model developed for this analysis considered the L-index of the entire system which is the maximum of the L-indices computed for each load bus. R2 values of the models developed for predicting the voltage stability is given in Table 3. The best model selected by comparing R2 scores can be used to predict the system's voltage stability for any futuristic input data. For predicting cost of energy purchased from the grid for the best-fit model is chosen by comparing the R2 values of the developed models viz., multi-variable linear regression, polynomial regression and 5-fold cross-validation. The R2 values of the models developed for predicting the cost is given in Table 4. It is also observed from Table 3 and Table 4 that the 4th degree polynomial regression model exhibits a better fit among the other polynomial models. The comparison of R2 scores obtained in the linear regression, 4th degree polynomial regression and 5-fold cross-validation of the 4th degree polynomial regression for base load case is tabulated in Table 5. Queen et al.: ML-Based Predictive TEA of Power System are considered most suitable, for the prediction of both cost and voltage stability in a power system. Analysing the heatmaps of correlations suggested that no two features have a strong correlation, so all the proposed features were suggested for developing the predictive ML models. These models were analyzed in terms of their R2 scores, which suggested that 4th order polynomial regression model with R2 values greater than 9 is optimally suited for all the systems in the prediction of both voltage stability in terms of systems' L-index and cost in terms of energy purchased from the grid. The validation tests for the predictive voltage stability and cost analysis were performed for both IEEE 14-bus and 30-bus systems for a 24hr test data. 9 suggest the effectiveness of the developed ML models. The comparison of predicted and actual values of all the cases were furnished and analyzed in terms of deviation and percentage error. The validation tests conducted for predicting the voltage stability and cost of the considered systems for a 24hr test data confirm the effectiveness of the developed ML models. The proposed method can be extended to predict voltage stability in case of other disturbances or sequence of events (short circuits, tripping of network elements, etc.).by including additional features like bus voltage, line current, line voltage drops etc.to the model development. This can be done by merely adding the values of bus voltage, line current etc.as additional inputs to each datapoint while generating the input-output dataset using MATLAB.

**2.3 Proposing Logical Table Constructs for Enhanced Machine Learning Process**

Machine learning has shown enormous potential in various domains with the wide variations of underlying data types. Because of the miscellany in the data sets and the features, ML classifiers often suffer from challenges, such as feature miss-classification, unfit algorithms, low accuracy, overfitting, underfitting, extreme bias, and high predictive errors. Through the lens of related study and latest progress in the field, this paper presents a novel scheme to construct logical table unit with two internal sub-modules for algorithm blend and feature engineering. The LT unit works in the deepest layer of an enhanced ML engine engineering process. eMLEE consists of several low-level modules to enhance the ML classifier progression. A unique engineering approach is adopted in eMLEE to blend various algorithms, enhance the feature engineering, construct a weighted performance metric, and augment the validation process. The LT is an in-memory logical component, that governs the progress of eMLEE, regulates the model metrics, improves the parallelism, and keep tracks of each module of eMLEE as the classifier learns. Optimum fitness of the model with parallel "check, validate, insert, delete, and update" mechanism in 3-D logical space via structured schemas in the LT is obtained [6]. The LT unit is developed in Python, C#, and R libraries and tested using miscellaneous data sets. To support the built and implementation of the proposed scheme, complete mathematical models along with the algorithms, and necessary illustrations are provided in this. The diversity in the data and features have motivated us to improve the latest state of ML models by building enhanced ML engine engineering process specially to address the challenges such as overfitting, underfitting, bias, low accuracy, poor generalization, and predictive errors. While the details of ML engine engineering are beyond the scope of this article, LT constructs are presented. The thick arrow between eFES, eABT, and LT module shows core integration than the other two modules of eMLEE. Out of these, eCVS is at infancy of the research work. Existing research, as discussed in Section II has shown the limitations of general-purpose algorithms in SL for predictive analytics, decision making, and data mining. [7] Finally, LT is built to coordinate the internal flow of eMLEE. Their findings, results, and discussion showed that active learning algorithms are making great progress especially for image classification and the type of data it involves. However, their contribution was limited to active learning, especially for image classification and may not be suitable to apply for a diverse set of data and features. They provided in-depth analysis and guidelines of various methods

with taxonomy table of their findings. Their work though provided great foundation and motivation for feature processing but did not provide the in-depth experiments of application of the technique on neutral subjects where feature may mislead, and algorithm design must take this into account. Their results showed improved recommendations score for resources and workload but did not address or consider the parallel processing of various algorithms to see if that could further improve their work. Dai and Song work was focused on multiple classifier systems with their contribution of supervised competitive learning algorithm to improve the accuracy of the classifiers. Their work was very limited to EM applications and did not provide the wide applicability to other domains of similar challenges in EM or Electrical engineering domains. They provided a taxonomy of learning approach and their related response time on their experiments. The goal was to justify the need of feature selection problem in-depth concepts of relevance and redundancy. However, their work lacks to address the issues of model fitting when a diverse set of features are involved in datasets. Related study was discussed to highlight the importance of ML latest progress in the research and to justify the invention of LT for eMLEE. This article was accompanied with simulated results (produced in Graphpad, SigmaPlot, MS Excel, and Plotly software’s), mathematical equations/constructs, underlying algorithms, and necessary illustrations to elaborate the conceptual details of the proposed constructs and the promising outcomes [8]. LT model addressed the challenge of trade-off between vital metrics such as complexity, accuracy, speed, etc.LT created parallel processes for each element in each run governed by 3D object coordinates (x, y and z) and then made observations in the real-time of classifier learning and updated its logical rows in the table. This approach was found to be novel to the best of our survey and knowledge. LT model presented in this article was also accompanied by eight mathematical definitions, three sub-procedures, and two by-design algorithms. This article also presented several visuals and frameworks to clarify the mechanics of the proposed unit along with promising results in conjunction with tabular data to draw useful observations. Finally, it was concluded that LT worked efficiently as a centralized module/unit of eMLEE to improve the metrics coordination and learning process for ML. The experimental results were included in this article to support the LT progress at this stage, and it showed that metric correlation and observations were found improved as compared to the learner process that was not trained using LT.

**2.4 An Automatic Reference Aid for Improving EFL Learners’ Formulaic Expressions in Productive Language Use**

Formulaic language is important to language acquisition; however, English language learners are often reported to have problems with formulaic expressions. Several lists of formulaic sequences have been proposed, mainly for developing teaching and testing materials. However, their limited numbers and insufficient usage information seem unable to benefit formulaic language use. To address these issues we have developed GRASP, a reference aid for formulaic expressions, to promote learners' productive competence. Users are allowed multi-word inputs to target their desired phrases or collocations. Utilizing natural language processing techniques, our system categorizes and displays the structures and sequences in a hierarchical way. The corresponding example sentences are also provided. In view of such a pressing need, formulaic sequences clearly should be placed prominently in language teaching textbooks and materials. Several lists of formulaic expressions have been compiled, such as the Academic Formula List and the Phrasal Expressions List, which are detailed in Section 2. To address this issue, we develop GRASP, a reference aid which provides a usage summary of the query phrase in the form of formulaic structures and frequent formulaic sequences. It aims at providing immediate assistance to learners in their writing tasks and helping them develop productive competence in speaking and writing, instead of passively recognizing text meaning only. The students' formulaic sequence use improved markedly and reached the statistical significance level with the help of GRASP. Next, we attempted to explore whether GRASP was of greater benefit to the less proficient students. But the high proficiency students gained less benefit from GRASP than less proficient ones. To further investigate whether the less proficient students showed significant improvement, the improved scores of the four groups were further submitted to ANOVA. Overall, GRASP evidently helped students show better performance on formulaic sequence use in the sentence completion task. Especially for the less proficient students, who need extra help becoming engaged learners, GRASP serves a substantial role in supporting formulaic sequence learning. It seems reasonable to infer that students were unable to manage formulaic language use well due to the restricted functionalities and information display of the existing reference tools[9]. First, single-word query in the Longman English Dictionary Online required students to make several more trials to successfully target the query phrases. Further, the surrounding usage information for the located phrases was largely absent. Even when available, learners needed to deduce the usage patterns by themselves. The limited lexical information provided by the Longman English Dictionary Online seems insufficient to help learners cope with the demand of varied contexts. For example, consider a student attempting to learn the formulaic expression "make a big difference to" in the Longman English Dictionary Online. Suppose he first inputs the "difference" and searches. The experimental group consulted GRASP, whereas the control group was allowed to consult either the Longman English Dictionary Online or Google Translate, or both. First, the analyses of students' scores in the sentence completion task revealed that the students consulting GRASP showed significant progress compared with those consulting the existing tools. GRASP can also be applicable to be incorporated into classroom teaching and activities. In the pedagogical practices, specific instructions on how the formulaic sequences are used in various scenarios could be emphasized, especially regarding verbs and prepositions, in order to promote learners' knowledge and awareness of word concatenation. For example, teachers may assign their students several collocations or phrases and engage them in consulting GRASP to learn the corresponding formulaic expressions. Students' command of formulaic language use could be evaluated through the sentence completion task periodically. In other words, we can group together the formulaic sequences sharing semantic equivalence but different usages, such as the phrases "take a lead in", "set an example by", "play an exemplary role in", and "give a lead in". The Longman English Dictionary Online and Google Translate should be investigated separately to examine their individual impacts on learners. It would be interesting to conduct a usability study on the effectiveness and the learnability of both tools. The system display could be revised. For example, highlighting the verbs and prepositions could enhance language features. Highlighting such as this will contribute to promoting learners' awareness in both the classroom settings and in the self-learning situation. On the other hand, the display of parts-of-speech could also be revised. Many students indicated that the part-of-speech labels were not widely acknowledged. While developing GRASP, we adopted Upenn Tagset to show the parts of speech, but students have been accustomed to the labels used in grammar books. The modifications suggested above should further increase the effectiveness of GRASP and enhance its efficiency in assisting learners in the acquisition of formulaic expressions.

**2.5 Is Your Android App Insecure? Patching Security Functions with Dynamic Policy Based on a Java Reflection Technique**

App wrapping technology can be used to patch the vulnerable code of an app or insert security functions at the bytecode level without the original app source code. In code patching studies the misused code has been detected and patched with the appropriate code, but it is not possible to add the security function provided by the EMM solution for apps that require security. There are two methods of adding new security functions to insecure apps for EMM solutions: inserting the security functions directly into the original Android app source code or inserting the security functions into the APK file of the app via bytecode rewriting. After inserting the security function execution code and repackaging the app, it is possible to execute and control the security function where required according to the dynamic policy. Even when the policy is changed, the new policy can be directly applied by using a Java reflection technique without inserting security execution code and repackaging the app again. Concise Security Function Execution Code The security function execution code consists of the minimum code for calling the security function execution library and has only two local variables and one parameter. The security function execution library dynamically calls the security function of the security app that provides the security function using Java reflection. That is, the security function execution code can be inserted into the method level while minimizing conflicts with the existing code. [10] Apply Security Policy Simply by Changing the Policy When changing the policy, the new policy can be applied immediately without adding security function execution code or repackaging the app. The policy contains the security function classes and methods required to run the security function. Java reflection is used to load the security function classes and methods that are dynamically set in the policy and to execute the security functions as set in the policy. However, the proposed method dynamically calls the security functions of the app that provides security functions from the security library by using Java reflection, minimizing the conflicts with the existing code even if multiple security functions are called. To overcome the limitations of previous research, the AppWrapper toolkit inserts security function execution code at the bytecode level into each method unit of the insecure app needing security functions [11]. Extraction of bytecode level security execution codes and library: To call the security functions of an app that provides various security functions, the security function execution code and library are extracted at the bytecode level. The library calls the security functions of the security app according to a predefined policy file. Insertion of a granular and extensible security function at method level: The security function execution code is inserted into each method unit of an insecure app. The inserted code uses Java reflection to invoke the security functions of the app dynamically. Dynamic policy management without app repackaging: After inserting the security function execution code into each method unit, the dynamic policy determines whether or not to execute the security functions at the method. Policy setting based on app flow: By adding the log function of each method unit in the app, the administrator in charge of security can check the log information in real time and understand the app flow while the app is running. The administrator can check the current class and method name of the app and define the appropriate security functions to be executed at the method where the security functions are required. Decompile the APK file of the insecure app (the app that needs security functions) to obtain the bytecode, AndroidManifest.xml file, and resource file. Insert the security function execution code and copy the security function library to the small file created in Step 1. The patched app works with the downloaded policy file to execute the security function according to the flow of the app. The security function execution code and its library are commonly inserted at the bytecode level. 1, the security function execution code and its library must be extracted at the bytecode level from the app that calls the security function of the security app. The extracted security function execution code and security library are then added to the method unit within the activity class of the insecure app. After the security function execution code is inserted, the security library is copied to the app for repackaging. The inserted security function execution code determines whether or not to execute the security function for each method in the activity according to policies declared on the policy file, and the policy file is copied to the phone. In this paper, we proposed an App Wrapper toolkit that inserts security function execution code into each method unit of the activities declared in the AndroidManifest.xml file and copies the security library for insecure apps. In addition, the log inquiry of the user interface is provided so that the security function execution code can be inserted according to the app flow.

**2.6 Salaxy: Enabling USB Debugging Mode Automatically to Control Android Devices**

Introduction With the rapid development of Internet technology, various new application technologies and patterns are emerging that people's lives more convenient, such as the introduction of edge computing, substantial improvements on the efficiency of network services; the development of wireless sensors  and the improvement of sensor network management schemes, making the Internet of Things more practical and driving the development of Internet of Vehicles and its security solutions [12]. The decentralized mode brought by blockchain technology has provided novel security thinking for network data, and the emergence of mobile smart devices has subverted the status of traditional computers on the Internet and has also brought about tremendous changes to human lifestyles. In fact, the privacy of Android users has been challenged by various malware and attacks, such as Soundcomber which extracts a small amount of sensitive information from the audio sensor; TouchLogger, which exploits the side channel to infer keystrokes; SimBad , which is hidden in the Google Play Store for users to download and install. ADB is a multipurpose command-line tool that allows the developer to communicate with the connected Android device through a USB cable. The first malware to exploit ADB resource exhaustion was DroidDream, which sends malware to Android devices by installing a rootkit on the device. Amarante et al. have already identified three attack scenarios based on the use of ADB and developed proof-of-concept scripts that can extract private data from a USB-connected device connected to a computer. Weizhi Meng et al.designed a new type of charging attack, called a juice filming attacks, based on a standard USB connector and an HDMI port, which is able to steal users' private data through automatically video-capturing their inputs without drawing the attention of users. . It could be seen that many attacks against the Android system exploit the vulnerabilities of the ADB tool if no proper protection of ADB has been enforced when using a USB connection, it may compromise the privacy of smart device users. Consequently, Google has strengthened the protection of ADB, and USB debugging mode is disabled by default and must be explicitly enabled in the developer options menu. This security mechanism ensures that USB debugging and other ADB commands cannot be executed unless the user can unlock the device and acknowledge the dialog. When the Android device is connected to an unknown host, the system will display a dialog window asking whether to accept an RSA key that allows debugging through this computer and needs to be confirmed. In fact, a way to enable secure USB debugging is not given in the above solutions and other ADB-based attacks. This method can bypass the security mechanism of USB debugging mode and bypass the improved security mechanism design of USB debugging mode, which was proposed in. The Salaxy sever is controlled by the attacker, and the client is installed on the victim's Android phone. Salaxy can execute preset scripts to enable USB debugging, connect to the server, and then monitor and manipulate the victim's Android smartphone [13]. The method is simple, easy and does not need to avoid the phone's anti-virus software and is suitable for the Android versions 5. The induced interface is just a simple UI to communicate with the Salaxy Server and does not require sensitive permissions. We develop two kinds of automated JavaScript scripts to turn on the USB debugging mode that are stored on the server-side and do not require the user to download. We test the Salaxy on Huawei Honor 10, OnePlus6 and Xiaomi 6X phones, proving that Salaxy can video-capture and manipulate the target phone whose version is Android 5. We need to investigate the characteristics of a target victim and modify the UI or functions of Salaxy according to those characteristics. Using Salaxy at a Public Charging Station. We propose the use of Salaxy at a public USB charging station, which is inspired by a juice filming attacks; this method can automatically video-capture user inputs during charging, and the attackers can easily manually recover users' private data, such as personal identification numbers and email accounts, based on the recorded video. Before charging the device at a charging station, users must install and register Salaxy. Less vigilant users will do so and connect the phone with a USB cable of the charging station. Then, we have a high probability of turning on USB debugging mode in the victim's Android device and being able to set up a video transmission between the Salaxy server and the victim's device. Compared with juice filming attacks, Salaxy can bypass the security mechanism of USB debugging mode and monitor the screen of the victim's devices without any hardware, such as the VGA/USB interface. Due to the portability of the Android system, most of the smart TVs on the market today are Android-based. Smart IPTVs must rely on the network and a charging cable, which provides the possibility of a Salaxy attack B. So, whether the attack is successful depends on the user's vigilance against the security of the "MTP" mode. If the user just randomly enters a string of numbers, we will not be able to open the developer mode of his phone which will prevent subsequent attacks. Executing this ADB command requires manual operation, but we hope to fully automate the attack process, which will be a challenge in the future.

**CHAPTER – 3**

**METHODOLOGY**

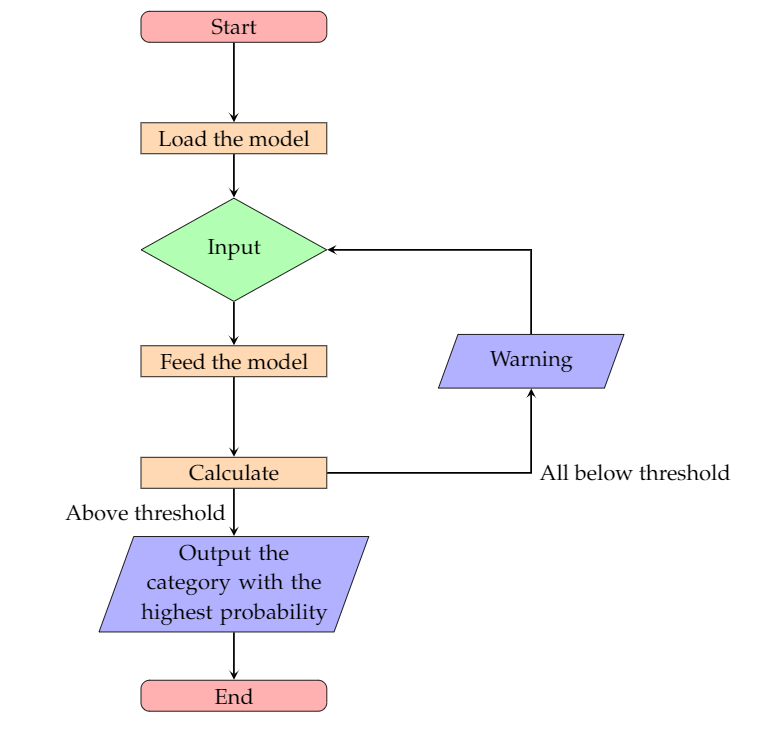
**3.1 METHODOLODY**

1. Data collection
2. Website design and creation
3. API for AQI creation
4. API for water quality index creation
5. API for soil quality creation
6. Integrating APIs to website
7. Dataset creation to store data
8. Testing and error handling
9. Final Website

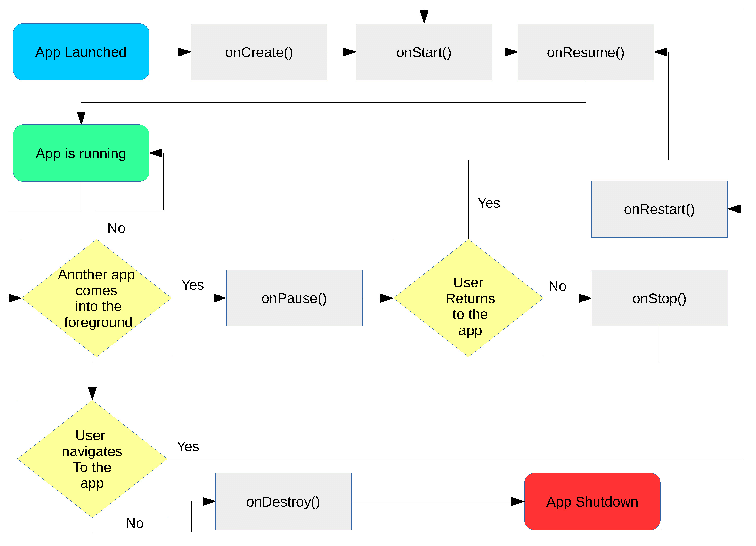
**3.2 TECHNOLOGY USED**

1. HTML
2. CSS
3. Python
4. Bootstrap
5. JavaScript
6. Vs code
7. Fire store
8. React

**3.3 FLOWCHART**



**Figure 1: Flowchart of the Model**



**Figure 2: Flowchart of the Website**

**3.4 DFD DIAGRAM**

**Diagram

Description automatically generated**

**FIGURE-3 DFD OF PROJECT**

**CHAPTER – 4**

**MODULES**

**4.1 FEATURES**

1. Displays the EQI of a certain area i.e., AQI, SQI, WQI.
2. Inform the user about the levels of pollutants present around his location.
3. Talks about the precautions that we need to take regarding the increasing Pollution according to the location.
4. Display details of the pollutants and the effects of them.
5. Detailed analysis of the land topography classifying them from green to red zone.

**CONCLUSION**

After going through the various research papers we are arriving to a conclusion of developing an website to help the people on the various environmental indexes of the elements and the pollutants that are responsible for various diseases from their individual increase like if AQI of a place is high carbon monoxide may lead to carbon poisoning to a person and similarly damage the building and to prevent it we can add certain substances or take certain precautions as per our need and condition.

**FUTURE SCOPE**

**Future Work Include-**

1. To integrate the SQI API.
2. To talk about the details of cleanliness rating.
3. To develop a system to launch a complaint about any large lump of garbage that is decaying.
4. Add a system which can connect directly connect with a doctor in case of an emergency due to pollution.

**REFERENCES**

[1] Z. Tian, W. Shi, Y. Wang, C. Zhu, X. Du, S. Su, et al., "Real-time lateral movement detection based on evidence reasoning network for edge computing environment", *IEEE Trans. Ind. Informat.*, vol. 15, pp. 4285-4294, Jul. 2019.

[2] A. Wray, Formulaic Language: Pushing the Boundaries, Oxford Univ. Press, 2008.

[3] X. Jin, X. Hu, K. Ying, W. Du, H. Yin and G. N. Peri, "Code injection attacks on HTML5-based mobile apps: Characterization detection and mitigation", *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, pp. 66-77, 2014.

[4] 1.Z. Tian, W. Shi, Y. Wang, C. Zhu, X. Du, S. Su, et al., "Real-time lateral movement detection based on evidence reasoning network for edge computing environment", *IEEE Trans. Ind. Informat.*, vol. 15, pp. 4285-4294, Jul. 2019.

[5] *Cross-Site Scripting (XSS)*, Dec. 2015, [online] Available: <https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)>.

[6] X. Jin, X. Hu, K. Ying, W. Du, H. Yin and G. N. Peri, "Code injection attacks on HTML5-based mobile apps: Characterization detection and mitigation", *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, pp. 66-77, 2014.

[7] M. V. Suganyadevi and C. K. Babulal, "Support vector regression model for the prediction of loadability margin of a power system", Appl. Soft Comput., vol. 24, pp. 304-315, Nov. 2014.\

[8] K. S. Sajan, V. Kumar and B. Tyagi, "Genetic algorithm-based support vector machine for on-line voltage stability monitoring", Int. J. Elect. Power Energy Syst., vol. 73, pp. 200-208, Dec. 2015.

[9] P. Branco, L. Torgo and R. P. Ribeiro, "A survey of predictive modeling on imbalanced domains", *ACM Comput. Surv.*, vol. 49, no. 2, pp. 1-50, 2016.

[10] M.H. Chen, "English Collocation Competence of College Students and Learner Factors", Proc. 26th Int'l Conf. English Teaching and Learning in the R.O.C, pp. 239-244, 2009.

[11] J.R. Nattinger and J.S. DeCarrico, Lecical Phrases and Language Teaching, Oxford Univ. Press, 1992.

[12]Mobile Tablet Operating System Market Share Worldwide, Jan. 2020, [online] Available: [https://gs.statcounter.com/os-market-share/mobile-tablet/worldwide/#monthly-201812-201912](https://gs.statcounter.com/os-market-share/mobile-tablet/worldwide/).

[13] A. B. Garba, J. Amerigo and D. Murray, "Bring your own device organizational information security and privacy", ARPN J. Eng. Appl. Sci., vol. 10, pp. 1279-1287, 2015.