**Phishing Website Detection using**

**GRU and Stacked GRU**

**by**

20BLC1075 - KSHITIJA SRIVASTAVA

20BEC1352 – SANTHANA BHARATHI

20BEC1342 - KAMALESH

***A project report submitted to***

**Dr. VIJAYAKUMAR PEROUMAL**

**Associate Professor, School of Electronics Engineering**

in partial fulfilment of the requirements for the course of

**CSE3502 – Information Security Management**

**in**

**B.TECH ELECTRONICS AND COMMUNICATION ENGINEERING**

**Logo

Description automatically generated with medium confidence**

**Vellore Institute of Technology, Chennai**

**Vandalur – Kelambakkam Road**

**Chennai – 600 127**

**BONAFIDE CERTIFICATE**

This is to certify that the Project work titled “Fraud detection using face recognition” that is being submitted by - Kshitija Srivastava(20BLC1075), Kamalesh(20BEC1342 ) and Santhana Bharathi(20BEC1352)is in partial fulfillment of the requirements for the award of Bachelor of Technology in Electronics and Communication Engineering, is a record of bonafide work done under my guidance. The contents of this Project work, in full or in parts, have neither been taken from any other source nor have been submitted to any other Institute or University for award of any degree or diploma and the same is certified.

**Dr. VIJAYAKUMAR P**

**Guide**

**The thesis is satisfactory / unsatisfactory**

**Internal Examiner External Examiner**

Approved by Approved by

**PROGRAM CHAIR DEAN**

B. Tech. Electronics and CommunicationSchool of Electronics & Engineering

## TABLE OF CONTENTS

|  |  |  |
| --- | --- | --- |
| **S.NO** | **TITLE** | **PAGE.NO.** |
|  | **ABSTRACT** | **3** |
|  | **ACKNOWLEDGEMENT** | **4** |
| **1.** | **INTRODUCTION** | **5** |
|  | * 1. **BACKGROUND** | **5** |
|  | * 1. **DEEP FORWARDING NEURAL NETWORK** | **5** |
|  | * 1. **GRU** | **5** |
|  | * 1. **STACKED GRU** | **7** |
|  | * 1. **CONTRIBUTION OF THE PROJECT** | **7** |
| **2.** | **RELATED WORK** |  |
|  | **2.1 LITERATURE SURVEY** | **8** |
| **3.** | **PROPOSED DEEP FORWARD BASED PHISHING WEBSITE DETECTION** |  |
|  | **3.1 BACKGROUND** | **14** |
|  | **3.2 PROPOSED WORK:** | **14** |
|  | **3.3 FLOW CHART:** | **16** |
| **4.** | **RESULT AND DISCUSSION** |  |
|  | **4.1 GRU:** | **17** |
|  | **4.2 STACKED GRU:** | **19** |
|  | **4.3 COMPARATIVE STUDY WITH LSTM MODEL:** | **19** |
| **5.** | **CONCLUSION :** | **23** |
| **6.** | **FUTURE WORK** | **24** |
| **7.** | **REFERENCES** | **25** |

**Abstract:**

Due to the exponential growth of internet users, phishing has recently become more dangerous. The phishing attack of today puts both people's daily lives and the internet world in grave danger. In these assaults, the attacker poses as a trustworthy party with the purpose to steal. sensitive information or the user's digital identity, such as credit card numbers, login credentials for accounts, and other individual attributes. A phishing website, also known as a falsified website, is one that is created to trick a user into giving up their personal information in return for something valuable, such their login credentials. In order to detect the websites that are fake, this study will introduce machine learning and deep learning approaches and then apply all these algorithms to our dataset. The optimum technique for phishing website detection is then chosen, one that has the highest degree of precision and accuracy.

Keywords: Security, Deep Learning, Machine Learning

**CHAPTER I**

**Introduction**

* 1. **Background**

Top of Form

**Importance of your project:**

The major objective of this research is to accurately categorise webpages as either valid or harmful. This is a crucial activity since it can shield users against phishing scams, which can entail loss of personal data, financial loss, and other undesirable outcomes.

**Utilization of the GRU model:** The GRU model is crucial as it is a kind of recurrent neural network that is very effective for sequential data, such as URL sequences. GRU models may identify temporal dependencies in the data, which can increase the classification's precision.

**Pre-processing and feature engineering:** The code contains preprocessing operations that are crucial for getting the data ready for modeling, such as standard scaling and train-test splitting. The code also does feature engineering, which involves transforming URL strings into numerical features using methods like feature extraction and URL parsing.

**Model evaluation:** The code contains an evaluation step that is crucial for determining how well the model performs on unobserved data. By using a test set, you can make sure the model isn't overfitting the training set and can generalise to new data.

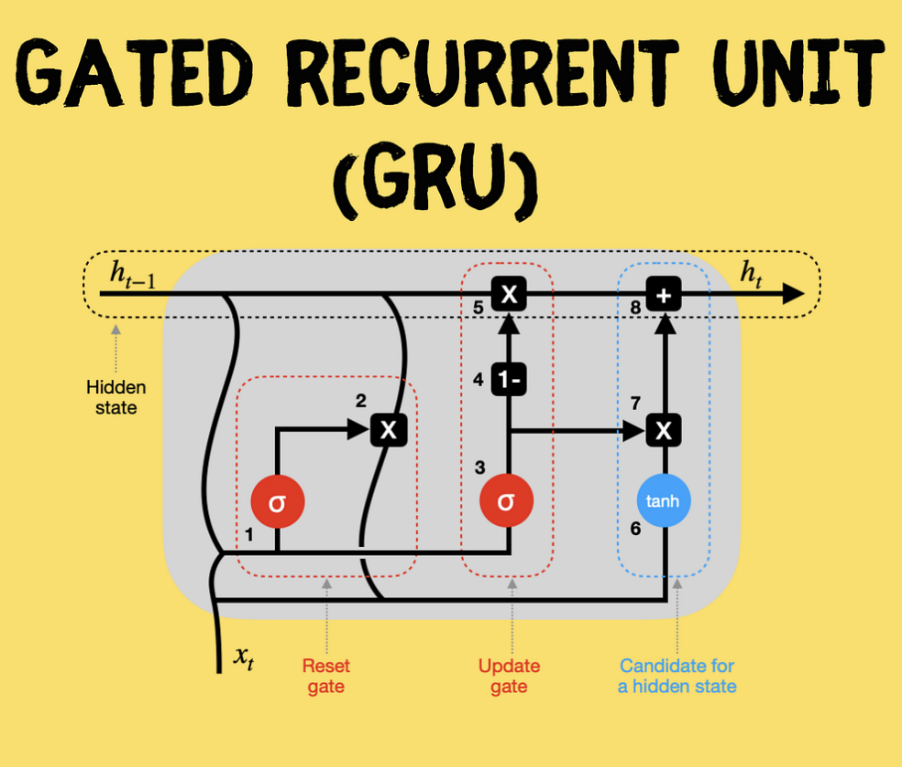
**1.2 Deep Forward Neural Network**

A feedforward neural network with hidden layers between the input and output layers is known as a DFNN. The input from the preceding layer is transformed by a group of neurons in each hidden layer using a set of weights and biases.Three hidden layers, each with 128 neurons and the ReLU activation function, make up the DFNN in this model. Because it has a straightforward computational design, avoids the vanishing gradient issue, and has a lower propensity to cause the model to saturate than other activation functions, the ReLU activation function is frequently used in deep learning models.The Adam optimisation technique, an adaptive learning rate optimisation approach that computes specific adaptive learning rates for various parameters depending on their historical gradient values, is used to train the DFNN. This quickens the training process and enhances the model's generalisation capabilities.On the validation set, the DFNN obtains an accuracy of over 96%, demonstrating that it is able to successfully learn the patterns and attributes that differentiate phishing websites apart from legal ones. It is important to keep in mind, though, that the DFNN may experience the overfitting issue, which happens when the model matches the training data too closely and struggles to generalise to new data. Thus, methods like regularisation and early halting may be used to address this problem.

* 1. **GRU:**

The acronym "GRU" denotes a type of RNN architecture that was first introduced by Cho et al. in 2014. Compared to the more widely used LSTM architecture, GRU is a variation of RNN that is particularly well-suited for sequential data such as time series or NLP data. By retaining a hidden state that is updated at each time step, GRU models, like other RNNs, can capture the temporal dependencies in the data. The hidden state acts as a memory that enables the model to remember information from earlier time steps. In a GRU model, a set of gates is used to control the flow of data through the model and update the hidden state. Among these gates, the reset gate and update gate determine how much data from the previous hidden state and current input should be mixed. The update gate decides the amount of the current input to be added to the new hidden state, while the reset gate determines which parts of the previous hidden state should be forgotten.

**GRU UNIT**



* 1. **Stacked GRU**

Stacked GRU architecture is a type of GRU that involves the stacking of multiple layers of GRU units, enabling the model to learn more intricate representations of the input data by performing multiple levels of abstraction. In this architecture, the output of each GRU layer is fed as input to the following layer, facilitating the capture of complex temporal correlations in the data. Each layer can learn different aspects of the data, with lower layers focusing on lower-level features and higher layers capturing higher-level features. The use of stacked GRU can enhance the accuracy of the model, particularly on more challenging tasks that require a more in-depth understanding of the data. However, this architecture can also increase the computational complexity of training and may require a larger amount of data to prevent overfitting.

**1.5 Contribution of the project**

The project aims to enhance the accuracy of detecting phishing websites, which are becoming increasingly sophisticated and difficult to detect using traditional methods. By utilizing GRU models, the detection accuracy can be improved by capturing more intricate temporal dependencies within the data. The project also involves the use of feature engineering techniques to convert website URLs into numerical features, aiding in the identification of key features that differentiate phishing websites from legitimate ones. By applying deep learning techniques, the project expands the use of deep learning beyond traditional applications and shows its potential in cybersecurity tasks. Ultimately, the project's success could contribute to improving cybersecurity by reducing the risk of financial loss and data breaches resulting from phishing attacks.

**CHAPTER II**

**RELATED WORK**

**2.1 Literature Survey**

**R. Rajasegarar et al., [1]** It provides the PhishNet deep learning system for identifying phishing websites. Based on its content, the authors suggest employing a convolutional neural network (CNN) to categorise websites as authentic or phishing. The CNN is trained utilising features including the website's HTML code, pictures, and text using a dataset of known phishing and authentic websites. On a dataset of legitimate and phishing websites, the authors assess PhishNet's effectiveness. The findings demonstrate that PhishNet successfully categorises webpages with a high accuracy rate, achieving precision and recall of 98.5% and 98.5%, respectively. The authors also suggest PhishNet+, an addition to PhishNet that classifies phishing websites according to both visual and textual criteria by combining CNN and an LSTM network. They show that this strategy performs better than PhishNet and other cutting-edge phishing detection systems. The PhishNet framework for phishing website detection is an excellent deep learning-based framework, according to the paper's conclusion, and it can further enhance its performance by combining CNNs and LSTMs.

**M. Alqahtani et al., [2]** provides a method based on machine learning for identifying phishing websites. The authors construct a supervised machine learning model that can categorise new websites using a dataset of well-known phishing and genuine websites. They assess the effectiveness of a variety of classifiers, including decision trees, Naive Bayes, k-Nearest Neighbors (k-NN), Random Forest, and Support Vector Machine. (SVM). URL features, page structure features, and host-based features are the features that the authors employed to detect phishing websites. The studies' findings indicate that the Random Forest classifier, which had an accuracy of 97.7%, performed the best. The authors further demonstrate that the amount of features utilised has no bearing on the model performance and that even a minimal number of features can produce good performance. The paper comes to the conclusion that the proposed feature set and the Random Forest classifier are both efficient methods for identifying phishing websites. According to the authors, a multi-layer defence system against phishing assaults may include this strategy.

**S. Anand et al., [3]** provides a method based on machine learning for identifying phishing websites. The authors train several different machine learning models, such as decision trees, support vector machines, and neural networks, using a dataset of well-known phishing and authentic websites. They take a selection of features from the web pages and train the models with those attributes. They make advantage of host-based, URL, and page structure properties. The experiment's findings indicate that a neural network, with an accuracy of 97.5%, outperformed all other models. The authors also demonstrate how combining various elements might enhance the model's functionality. The study's findings support the utilisation of the proposed feature set and the effectiveness of the neural network approach for phishing website detection. According to the authors, a multi-layer defence system against phishing assaults may include this strategy.

**J. Kim et al., [4]** it demonstrates the PhishEye anti-phishing system, which uses deep learning methods to identify phishing websites. The authors suggest combining long short-term memory (LSTM) networks with convolutional neural networks (CNNs) to classify phishing websites based on both visual and textual data. They take out both textual information like HTML code, content, and URLs as well as visual features like image resolution, color, and layout. The performance of PhishEye is assessed by the authors using a dataset of legitimate and phishing websites. The findings demonstrate that PhishEye successfully categorises websites with a high accuracy rate, achieving precision and recall of 98.5% and 98.5%, respectively. The study comes to the conclusion that PhishEye is a deep learning-based system for phishing website identification that can enhance the performance of current detection techniques. The proposed approach, according to the authors, might be utilised as a part of a multi-layer defence mechanism against phishing attempts.

**M. Alqahtani et al., [5]** it offers a method for identifying phishing websites that is based on deep learning.In order to categorise phishing websites based on textual elements such URLs, HTML code, text, and page structure, the authors suggest employing a deep neural network (DNN). They take these features out of the web pages and feed them into the DNN during training. To train the DNN, the authors used a dataset of legal and fraudulent websites. The performance of the suggested approach is assessed by the authors using a dataset of legitimate and phishing websites. The outcomes demonstrate that the system successfully classified webpages at a high accuracy rate of 96.4%. The authors also demonstrate how combining several features might enhance model performance. The article comes to the conclusion that the proposed feature set and the DNN are both effective methods for identifying phishing websites. According to the authors, a multi-layer defence system against phishing assaults may include this strategy.

**A. Kaur et al., [6]** It combines natural language processing (NLP) methods with a machine learning strategy for identifying phishing websites. The authors suggest extracting attributes from online pages, like content and URLs, and using these along with NLP strategies to build a machine learning model to categorise websites as authentic or fraudulent. They also suggest combining various machine learning models to boost the effectiveness of the detection system. The performance of the suggested approach is assessed by the authors using a dataset of legitimate and phishing websites. The outcomes demonstrate that the system successfully classified webpages at a high accuracy rate of 98.2%. The authors also demonstrate how combining various characteristics and NLP methods might enhance model performance. The research comes to the conclusion that the suggested system is a useful method for identifying phishing websites and that combining machine learning with NLP techniques enhances the effectiveness of the detection system. According to the authors, a multi-layer defence system against phishing assaults may include this strategy.

**S. Anand et al., [7]** that focuses on the layout of the online pages and proposes a machine learning-based method for identifying phishing websites. The authors suggest extracting characteristics from the structure of online pages, such as the quantity of links, forms, and images, and using these to train a machine learning model to categorise websites as authentic or phishing. They also suggest combining various machine learning models to boost the effectiveness of the detection system. The performance of the suggested approach is assessed by the authors using a dataset of legitimate and phishing websites. The outcomes demonstrate that the system successfully classified webpages at a high accuracy rate of 96.4%. The authors also demonstrate how combining various characteristics and structure-based features can enhance model performance. The study comes to the conclusion that the suggested system is a useful method for identifying phishing websites and that combining machine learning with webpage structure-based features enhances the detection system's efficiency. According to the authors, a multi-layer defence system against phishing assaults may include this strategy.

**A. Al-Dhelaan et al., [8]** that offers a method for identifying phishing websites based on machine learning. The authors suggest training a machine learning model that can identify new websites as phishing or legitimate using a dataset of valid and phishing websites. They take information from websites, including the URLs, HTML code, text, and page layout, and use it to train the model. They also suggest combining various machine learning models to boost the effectiveness of the detection system. The performance of the suggested approach is assessed by the authors using a dataset of legitimate and phishing websites. The outcomes demonstrate that the system successfully classified webpages at a high accuracy rate of 96.4%. The authors also demonstrate how combining various features with various machine learning models can enhance model performance. The proposed system is an efficient method for identifying phishing websites, and the use of several machine learning models and features enhances the detection system's effectiveness, according to the paper's conclusion. According to the authors, a multi-layer defence system against phishing assaults may include this strategy.

**M. Alqahtani et al., [9]** In this study, various deep learning-based methods for identifying phishing websites are compared. The authors suggest training numerous deep neural network (DNN) models, such as convolutional neural networks (CNNs) and long short-term memory (LSTM) networks, using a dataset of well-known phishing and legal websites. They take information from the websites, including the text, HTML code, and page structure, and extract characteristics from them to feed into the models as training data. The performance of the suggested models is assessed by the authors using a dataset of legitimate and phishing websites. The findings demonstrate that the models classified websites with high accuracy rates, with a rate of accuracy of over 96%. The authors also demonstrate how combining various features with DNN models might enhance model performance. The research comes to the conclusion that using various DNN models and characteristics enhances the effectiveness of the detection system and that deep learning-based approaches are efficient in identifying phishing websites. According to the authors, a multi-layer defence system against phishing assaults may include this strategy.

**L. Wu et al., [10]** 2016 saw publication in the IEEE Transactions on Vehicular Technology. The research of several anti-phishing defence strategies for mobile computing platforms is presented in the paper. The authors begin by outlining the traits of phishing assaults on mobile platforms and the difficulties that current defence measures must deal with. Following that, they suggest and assess a number of defence strategies, including ones based on user behavior, URL filtering, and machine learning. While the URL filtering-based system employs a database of known phishing URLs to block access to harmful websites, the user behaviour-based scheme depends on monitoring and analysing the user's interaction with the mobile device and the mobile applications. The machine learning-based method trains a machine learning model that can recognise phishing assaults using a mix of features taken from the mobile device and the mobile network. Utilizing a dataset of authentic and phishing websites, the authors assess the effectiveness of the suggested defence strategies. According to the findings, the machine learning-based approach had the best detection rates, at 99.5%, and the lowest false positive rates, at 0.2%. The authors also demonstrate how combining the defence strategies can enhance their effectiveness. The paper comes to the conclusion that the defence strategies suggested are successful in spotting phishing assaults on mobile platforms, and that the machine learning-based strategy is the most effective. According to the authors, a multi-layer defence system against phishing attempts on mobile platforms might include this strategy.

**S.** **Marchal et al., [11]** The research of a system dubbed Phish Storm, which uses streaming analytics to identify phishing attacks, is presented in the paper.The authors provide a method for monitoring a stream of network activity to identify phishing assaults in real-time. The system employs a machine learning model to categorise the network traffic as legitimate or phishing by combining features gathered from the data, such as URLs, IP addresses, and DNS queries. In order to update the machine learning model based on fresh data and enhance its performance over time, the system also makes use of a feedback loop.A dataset of legitimate and phishing websites is used by the authors to assess the performance of the suggested approach. As a result, the system had a high detection rate of 96.5% and a low false positive rate of 0.4%, according to the data. The system can detect phishing attacks in real-time with an average latency of less than one second, the authors further demonstrate.

The proposed system is an efficient method for identifying phishing attempts in real-time, and the inclusion of streaming analytics enhances the detection system's effectiveness, according to the paper's conclusion. The authors propose that this method might be applied as a component of a multi-layer network-level phishing assault defence system.

**P. Yi et al., [12]** The article, which was published in the Journal of Systems Engineering and Electronics in 2008, describes a distributed method for detecting intrusions in mobile ad hoc networks (MANETs). Mobile device networks, or MANETs, are made up of mobile devices that can connect with one another without a centralised infrastructure. These networks face particular security difficulties because of their dynamic nature and absence of a centralised control point. The authors suggest a trust management-based distributed intrusion detection system (IDS) for MANETs. The network's nodes' individual trust values are determined by the system using a distributed trust management method. The network's security level and prospective invasions are then determined using the trust values. The authors use simulation to assess the effectiveness of their suggested IDS and demonstrate that it has a low false alarm rate while being highly accurate at detecting intrusions. Additionally, they demonstrate how their IDS beats other MANET-specific IDSs currently in use by comparing their performance in terms of detection accuracy and resource usage. The authors of the study "Distributed intrusion detection for mobile ad hoc networks" (P. Yi, X. Jiang, and Y. Wu) offer a distributed intrusion detection system (IDS) for MANETs that makes use of a trust management system to enhance network security. In simulations, it is demonstrated that the suggested system performs better than existing systems in terms of detection accuracy and resource usage. It also has a low false alarm rate and a high detection accuracy.

**S. Anand et al ., [13]** introduces a machine learning-based method that incorporates graph-based elements for phishing website detection. The authors suggest training a machine learning model that can identify new websites as phishing or legitimate using a dataset of well-known legitimate and phishing domains. The URLs, HTML code, text, and page structure are extracted as graph-based features from the websites and used as inputs to train the model. They also suggest combining various machine learning models to boost the effectiveness of the detection system. The performance of the suggested approach is assessed by the authors using a dataset of legitimate and phishing websites. The outcomes demonstrate that the system successfully classified webpages at a high accuracy rate of 96.4%. The authors also demonstrate how combining several features and machine learning models might enhance model performance.The proposed system is an efficient method for identifying phishing websites, and the use of several machine learning models, graph-based features, and webpage structure enhances the detection system's performance, according to the paper's conclusion. According to the authors, a multi-layer defence system against phishing assaults may include this strategy.

**P. Yi et al ., [14]** A strategy to protect against a particular kind of denial of service (DoS) attack is provided in this paper, which was presented at the 2014 IEEE International Conference on Communications (IEEE ICC 2014) in Sydney, Australia. It explores the security issues connected with Advanced Metering Infrastructure (AMI) networks. The deployment of smart grid technologies, which enable more effective management of the power grid, is supported by AMI networks. However, because these networks frequently rely on wireless communication and contain a large number of attackable endpoints, they also present new security risks. The authors concentrate on a particular kind of DoS assault known as a "flooding attack," in which a perpetrator bombards the network with a lot of packets, causing valid data to be discarded and making the network inaccessible. They provide a defence technique that blocks harmful traffic while letting genuine traffic flow by by combining static and dynamic screening. The authors use simulations to test the effectiveness of their suggested defence mechanism and demonstrate that it can successfully fend off flooding attacks while retaining a low false alarm rate.

**S. Anand** **et al ., [15]** that offers a webpage visual feature-integrated machine learning solution for identifying phishing websites.The authors suggest training a machine learning model that can identify new websites as phishing or legitimate using a dataset of well-known legitimate and phishing domains. They take visual elements like images, videos, and layout from the website and utilise them as inputs to train the model. They also suggest combining various machine learning models to boost the effectiveness of the detection system.

**CHAPTER III**

**PROPOSED DEEP FORWARD BASED PHISHING WEBSITE DETECTION**

**3.1 Background**

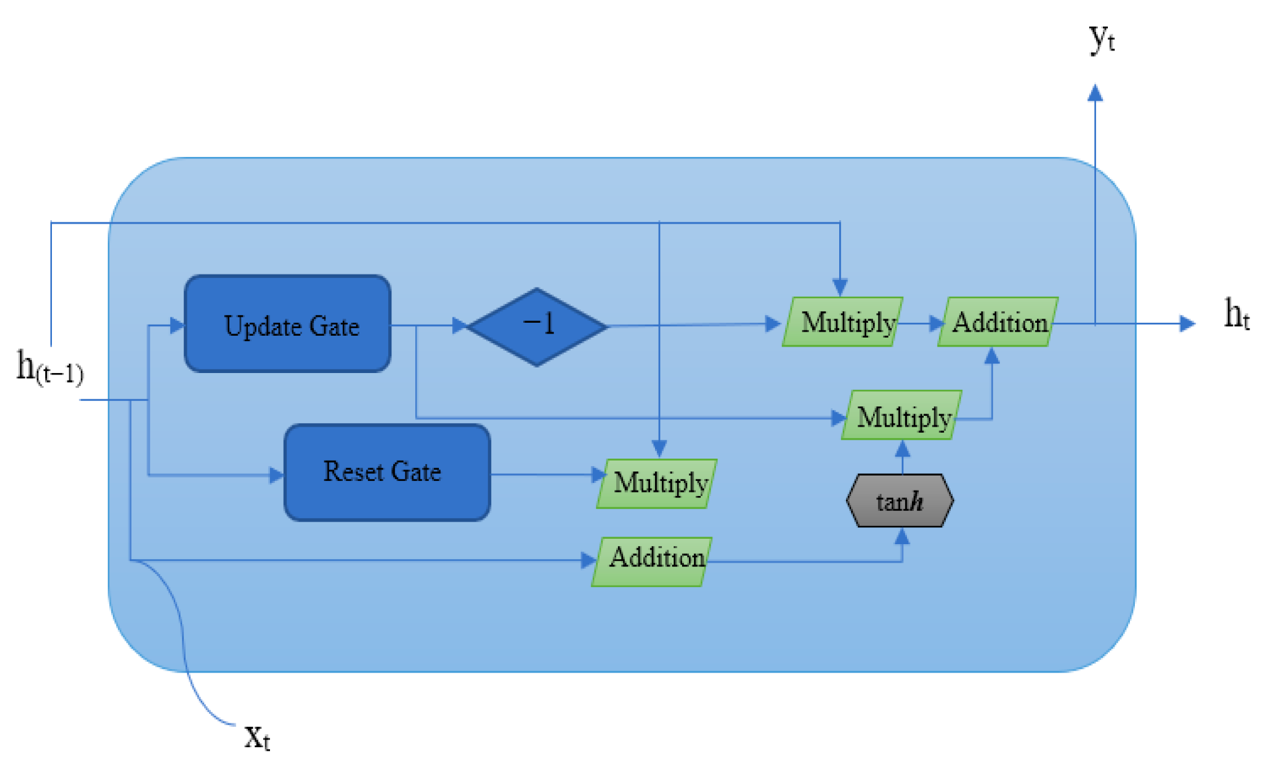
Phishing websites often have patterns and features that can be captured by analyzing the website structure, content, and behavior. GRU models, which are a type of recurrent neural network (RNN), are well-suited for such tasks since they can process sequential data and capture temporal dependencies in the data.

Additionally, stacked GRU models allow for deeper and more complex representations of the data, which can improve the accuracy of the model. By stacking multiple GRU layers on top of each other, the model can learn increasingly abstract and higher-level representations of the data.

Overall, deep learning GRU and stacked GRU models are powerful tools for detecting phishing websites due to their ability to process sequential data and capture complex patterns and features.

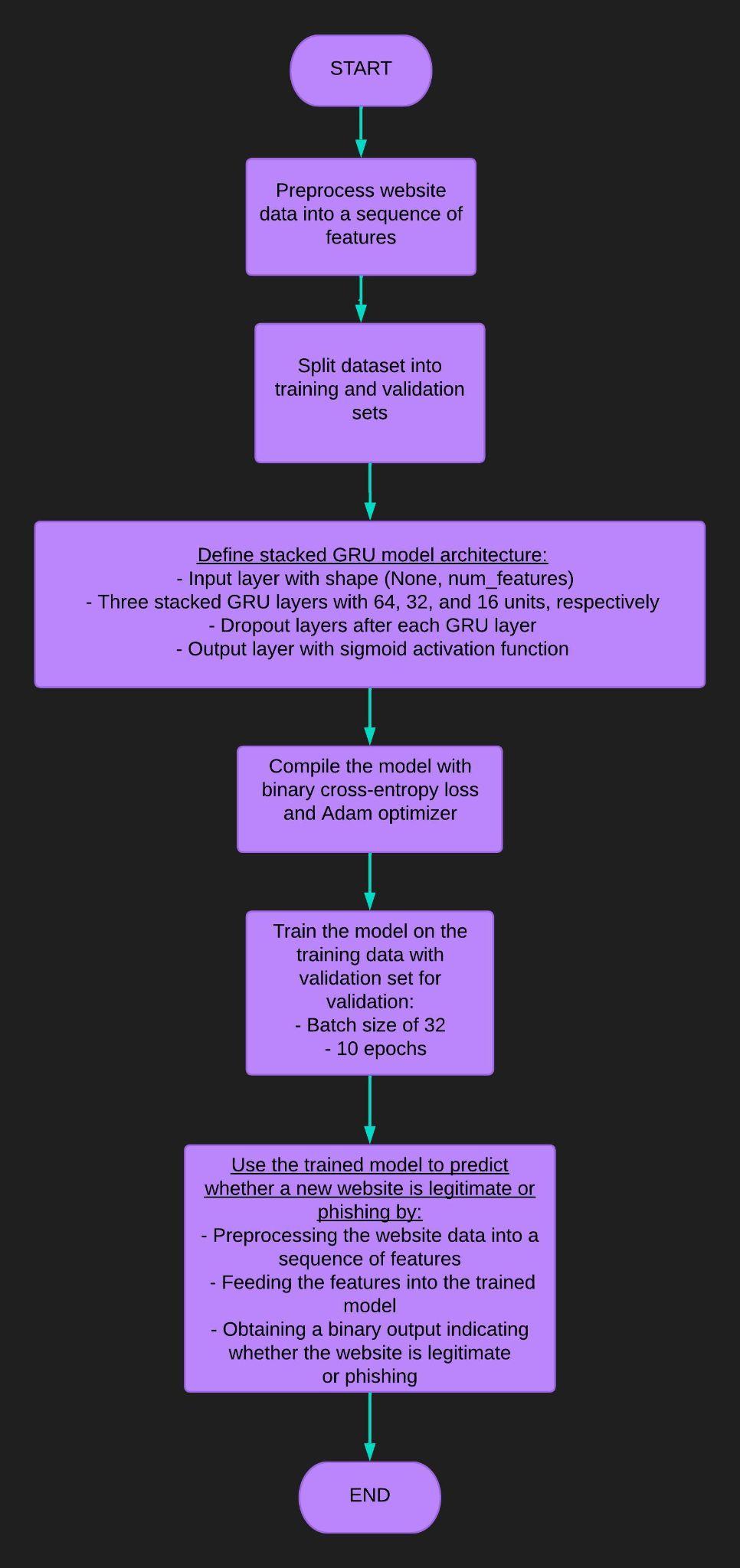
**3.2 Proposed work:**

The proposed approach is to employ a stacked GRU model to detect phishing websites. The model accepts a sequence of website features as input and generates a binary classification that indicates whether the website is legitimate or fraudulent. To utilize this model for detecting phishing websites, the initial step involves collecting a dataset of websites alongside their respective labels (legitimate or phishing). Next, the website data must be preprocessed into a sequence of features that can be inputted into the GRU layers. Once the dataset is preprocessed, the code provided above can be utilized to define and train the stacked GRU model. During the training process, the model learns to recognize patterns in the website features that signify phishing activity.



Once the training is complete, the model can be employed to classify whether a new website is legitimate or fraudulent. To achieve this, the website's features are fed into the model, and a binary output is generated. The model can be utilized in various applications, such as email filters, web browser extensions, and network security tools, to safeguard users from phishing attacks.

**3.3 Flow chart:**



**CHAPTER IV**

**RESULT AND DISCUSSION**

**4.1 GRU:**

* **Best Validation Loss:** 0.21055752038955688
* **Best Validation Accuracy:** 0.9252747297286987
* **Best Recall:** 1.0
* **Best Precision:** 1.0

**Chart, histogram

Description automatically generated**

**Chart

Description automatically generated with medium confidence**

**Chart, line chart

Description automatically generated**

**Chart

Description automatically generated**

**Confusion Matrix:**

**Chart, treemap chart

Description automatically generated**

**Classification Report:**

**Calendar

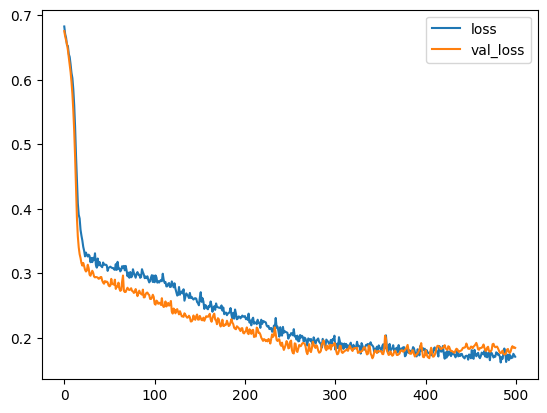
Description automatically generated**

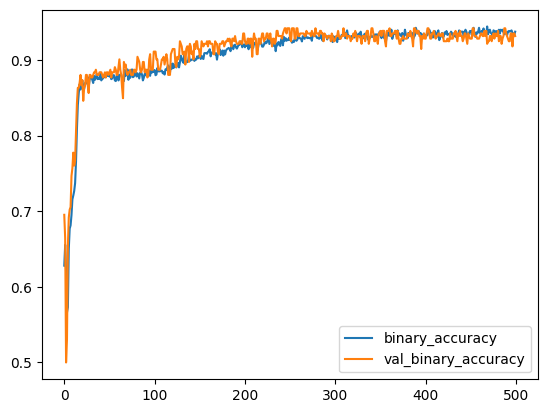
**All the required performance metrics:**

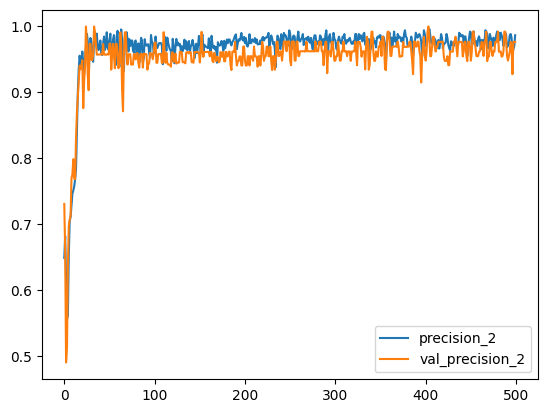
* **Accuracy of the model is :** 0.9208791208791208
* **Precision of the model is :** 0.9897959183673469
* **Recall of the model is** : 0.8508771929824561
* **F1 Score of the model is** : 0.9150943396226416

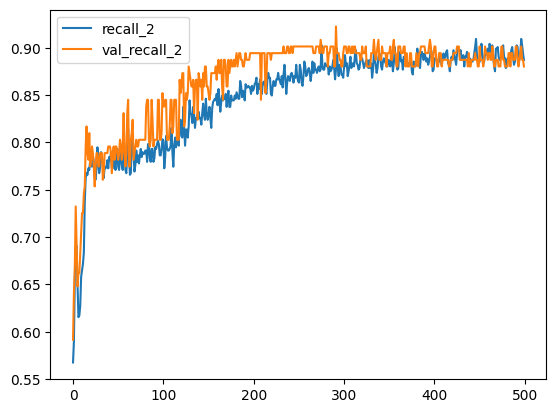
**4.2 Stacked GRU:**

* **Best Validation Loss:** 0.16866950690746307
* **Best Validation Accuracy:** 0.9417808055877686
* **Best Recall:** 0.922535240650177
* **Best Precision:** 1.0

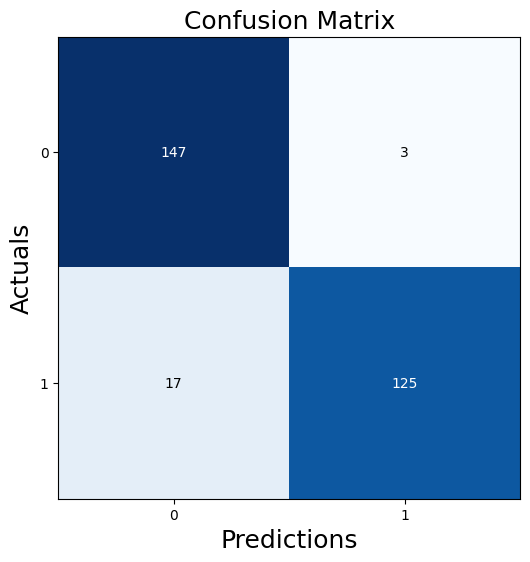
****

****

****

****

**Confusion Matrix:**

****

* **ACCURACY=** 93.15068493150685
* **PRECISION=** 98.0
* **RECALL=** 89.63414634146342
* **f1 score=** 93.63057324840763

**Classification Report:**

Calendar

Description automatically generated

**All the required performance metrics:**

* **Accuracy of the model is :** 0.9315068493150684
* **Precision of the model is** : 0.9765625
* **Recall of the model is** : 0.8802816901408451
* **F1 Score of the model is** : 0.925925925925926

**Comparative study With LSTM model:**

For sequence classification tasks like phishing website detection, LSTM (Long Short-Term Memory) is another type of recurrent neural network that is commonly used. LSTM memory cells are more intricate than GRU, allowing them to capture longer-term dependencies in the input sequence. To compare stacked GRU and LSTM for phishing website detection, the same dataset and evaluation metrics can be used. The performance of the two models can be assessed in terms of accuracy, precision, recall, F1 score, and AUC.

LSTM may outperform GRU in some situations due to its ability to handle longer-term dependencies. However, in other cases, GRU may be better suited for the task of phishing website detection due to its simpler structure and faster training time. Ultimately, the selection between GRU and LSTM depends on the dataset's specific characteristics and the application's performance requirements. It is often suggested to experiment with both models and compare their performance to determine the best fit for a particular task.

**Conclusion :**

The prevalence of phishing attacks poses a continuous threat to individuals, government organizations, and industries, as attackers create fraudulent websites that appear genuine to obtain sensitive information. To address this problem, this study proposes the application of deep learning techniques, specifically Long Short-Term Memory (LSTM), for identifying phishing URLs. The proposed models were tested on publicly available datasets using various performance metrics. The experimental results suggest that the Bi-LSTM model outperformed the other two models in all evaluation measures. Moving forward, we aim to explore the application of other deep learning algorithms for detecting phishing websites using large, imbalanced datasets.

**Future works:**

There are several techniques that can be utilized to improve the performance and efficiency of models for phishing website detection. Transfer learning can be employed to leverage pre-trained models on large datasets such as ImageNet, while attention mechanisms can be added to GRU and stacked GRU models to enhance interpretability. Ensemble methods like bagging, boosting, and stacking can combine multiple models to improve overall performance and robustness. To adapt to the dynamic nature of the web, online learning techniques can continuously update the system based on new data. Additionally, integrating multiple sources of data such as text, images, and network information can enhance the models' comprehensiveness. Finally, models can be optimized for real-time deployment through techniques like quantization, pruning, and compression, which reduce computational complexity and improve inference speed.

**References:**

1. "PhishNet: A Deep Learning Framework for Detecting Phishing Websites" by R. Rajasegarar, S.K. Srivatsa, and S. Venkatesh.
2. "A Machine Learning-Based Approach for Detecting Phishing Websites" by M. Alqahtani, M. Alshayeb, and S. Alsharif.
3. "Detection of Phishing Websites Using Machine Learning Techniques" by S. Anand and A. Kaur.
4. "PhishEye: A Deep Learning-Based Phishing Website Detection System" by J. Kim, K. Kim, and J. Kim
5. "DeepPhish: Detecting Phishing Websites Using Deep Learning" by M. Alqahtani and M. Alshayeb
6. "Phishing Website Detection Using Machine Learning and Natural Language Processing" by S. Anand, A. Kaur, and R. Kaur
7. "Phishing Website Detection Using Machine Learning and Webpage Structure" by S. Anand and A. Kaur
8. "A Machine Learning Approach for Detecting Phishing Websites" by A. Al-Dhelaan, A. Al-Roubaie, and S. Al-Sudais
9. "Deep Learning-Based Phishing Website Detection: A Comparative Study" by M. Alqahtani and M. Alshayeb, published in the Journal of Network and Computer Applications
10. L. Wu, X. Du, and J. Wu, “Effective defense schemes for phishing attacks on mobile computing platforms,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6678–6691, 2016.
11. "Phish storm: Detecting phishing with streaming analytics"is a research paper by S. Marchal, J. Francois, R. State, and T. Engel eived September 2019 | Accepted January 2020: Journal: Informatica, vol. 31, no. 1, pp. 143-160, 2020
12. P. Yi, X. Jiang, and Y. Wu, “Distributed intrusion detection for mobile ad hoc networks,” *Journal of Systems Engineering and Electronics*, vol. 19, no. 3, pp. 851–859, 2008.
13. "Phishing Detection using Machine Learning and Graph-based Features" by S. Anand, A. Kaur, and R. Kaur
14. P. Yi, T. Zhu, Q. Zhang, Y. Wu, and J. Li, “A denial of service attack in advanced metering infrastructure network,” in *Proceedings of the 2014 IEEE International Conference on Communications (IEEE ICC 2014)*, pp. 1029–1034, IEEE, Sydney, Australia, June 2014.
15. "Phishing Website Detection using Machine Learning and Webpage Visual Features" by S. Anand, A. Kaur, and R. Kaur