JINTEKS (Jurnal Informatika Teknologi dan Sains) ISSN 2686-3359 (Online)
Vol. 5 No. 1, Februari 2023, hlm. 13 – 17

ANALISA *MACHINE LEARNING* DENGAN ALGORITMA *MULTI-LAYER PERCEPTRON* UNTUK PENANGANAN KEJAHATAN *PHISHING*

Rian Handoko[1], Tata Sutabri[2]
[1,2]Program Studi Magister Teknik Informatika, Universitas Bina Darma Palembang
email: rian.ndok@gmail.com

Abstrak: Setelah pandemic merajarela, semua kebijakan mengharuskan bekerja dan bersekolah dari rumah. Oleh karena itu banyak pekerjaan dikomunikasikan melalui *email*. Dengan meningkatnya penggunaan *email* dikalangan pekerja, diimbangi juga dengan kriminalitas *cyber*. Dan salah satunya adalah tindak pidana *Phishing* melalui *email*. Motif kejahatan *Phishing* ini adalah untuk mendapatkan data pribadi dari korban, yakni user dan password agar mendapatkan keuntungan baik secara material dan non-material. Oleh karena itu penulis ingin melakukan penangan tindak kejahatan cyber dengan menggunakan machine learning yaitu *Multi-layer Perceptron*. Diharapkan dengan machine learning tersebut dapat mencegah terjadinya kejahatan *Phishing* secara maksimal dan akurat. Dalam penelitin ini, peneliti menggunakan dataset *email* yang bersumber dari Kaggle yang terdiri dari 1368 *email Phishing* & 4538 yang bukan *email Phishing*. dan pengguna akan menguji tingkat akurasi dengan menggunakan algoritma *Multi-layer Perceptron*. Setelah dilakukan pengujian, tingkat akurasi didapatkan 99.65%. ini membuktikan bahwasanya algoritma model *Multi-layer Perceptron* cukup efektif untuk menangani tindak pindana kejahatan *Phishing* melalui email.

Kata Kunci : *Phishing, Multi-layer Perceptron, email.*

Abstract: *After the pandemic was rampant, all policies required work and school from home. Therefore a lot of work is communicated by e-mail. With the increasing use of e-mail among workers, it is also offset by cyber crime. And one of them is the criminal act of Phishing via email. The motive for this phishing crime is to obtain personal data from victims, namely users and passwords in order to gain both material and non-material benefits. Therefore the author wants to handle cyber crime by using machine learning, namely the Multi-layer Perceptron. It is hoped that this machine learning can prevent Phishing crimes maximally and accurately. In this study, researchers used an email dataset sourced from Kaggle which consisted of 1368 Phishing emails & 4538 which were not Phishing emails. and the user will test the level of accuracy using the Multi-layer Perceptron algorithm. After testing, the accuracy rate was 99.65%. This proves that the Perceptron Multi-layer model algorithm is effective enough to deal with criminal acts of phishing via email***.**

Keywords **:** *Phishing, Multi-layer Perceptron, email.*

PENDAHULUAN

Awal tahun 2020 adalah tahun dimana *covid* pertama kali terdeteksi di indonesia. Dimana pemerintah Indonesia menerapkan kebijakan kepada rakyatnya untuk melakukan segala aktifitas dari rumah baik itu sekolah maupun pekerjaan. Oleh karena itu semua pekerjaan dilakukan secara *online.* Dimana banyak pekerja menggunakan *email* untuk komunikasi pekerjaan dengan atasan, rekanan maupun bawahan. Dengan banyaknya aktifitas *online* maka disitu ada celah kejahatan yang dimanfaatkan oleh orang yang tidak bertanggung jawab untuk melakukan tindak *cyber-crime* salah satunya *Phishing*.

Phishing adalah teknik untuk mengelabuhi seseorang untuk mendapatkan data pribadi yakni user, password, dan lain-lain yang sifatnya rahasia. Informasi ini dimanfaatkan oleh pelaku *Phishing* untuk dijual ke pihak lain atau dimanfaatkan untuk mendapatkan keuntungan dengan cara membobol data pribadi.

Menurut perusahaan keamanan siber asal Switzerland, Acronis memprediksi angka kejahatan siber ditahun 2023 akan meningkat tajam. Ancaman itu adalah *Phishing* yakni meningkat sebesar 60% melalui *email*. Pelaku kejahatan *Phishing* melalui *email* umumnya mengelabui korban menggunakan *email* yang hampir mirip dengan *email* resmi. Tindak kejahatan *phishing* tidak cuma berpura- pura selaku menggunakan *email* institusi formal. Mereka juga menulis e- mail palsu dan membangun web yang mirip semacam aslinya. Web *phishing* memanglah lebih gampang dideteksi lewat link yang berbeda dari web aslinya.

Akan tetapi, e-mail *phishing* sangat sulit diidentifikasi oleh karena pelaku kejahatan memakai teknik *spoofing*, ialah membuat nama akun serta alamat e-mail yang seakan-akan sama dengan alamat asli. e-mail *phishing* isinya menipu dengan membuat korban mengeklik link dalam e-mail tersebut, setelah itu korban memberikan informasi sensitif semacam alamat e-mail serta password di dalamnya.

Ketidaksadaran warganet Indonesia akan *phishing* membuat permasalahan makin bertambah. Tidak hanya itu, pelakon *phishing* cenderung memakai lebih dari satu nama domain buat melancarkan aksinya.

Untuk menghindari *Phishing*, kita bisa mengenali ciri-cirinya yaitu

1. Bahasa tidak rapi
2. Terdapat tautan mencurigakan
3. Domain E-mail tidak professional

Terkadang walaupun kitab bisa mengenali ciri-ciri *Phishing* tidak serta merta kita terhindar oleh

 ISSN 2686-3359 (Online)

kejahatan tersebut. Karena teknik *Phishing* dari tahun ke tahun berkembang pesat. Oleh karena itu Penulis akan mencoba melakukan Analisa kejahatan tersebut dengan memanfaatkan machine learning dan algoritma yang digunakan adalah *Multi-layer Perceptron*.

Sebetulnya banyak sekali algoritma machine learning yang bisa dipakai untuk Analisa kejahatan tersebut. Akan tetapi algoritma multi layer perceptron memiliki kelebihan yakni memiliki kemampuan untuk melakukan Analisa atau deteksi untuk permasalahan yang lebih kompleks. Dengan kelebihan tersebut akan mampu untuk menganalisa isi dari pada *email Phishing* yang sangat kompleks.

Dalam tulisan ini, penulis akan menilai seberapa tingkat akurasi algoritma muli-layer perceptron dalam hal penangan kejahatan *Phishing* melalu *email*. Dan setelah itu penulis akan melakukan percobaan Tindakan pencegahan dengan membaca *email* yang dikirim dari pihak lain. Apakah jenis nya *Phishing* atau bukan.

TINJAUAN PUSTAKA

Machine Learning (ML) adalah mesin yang dirancang untuk belajar sendiri tanpa perlu di program oleh pengguna. Mesin tersebut mengacu displin ilmu lain seperti *data mining*, ilmu statistik tanpa perlu di program.

Mesin diharapkan mampu mempelajari data dengan tanpa di perintah. Mesin diharapkan mampu melakukan Analisa data dan mendapatkan sebuat pattern dari data tersebut agar dapat digunakan untuk memberikan suatu solusi, prediksi dan lain-lain.

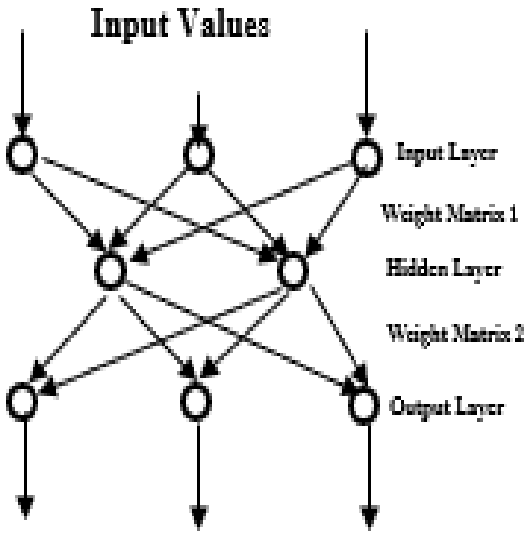
Cara kerja machine learning sebenarnya bergantung pada teknik atau metode pembelajaran apa yang Anda gunakan di ML. Namun pada dasarnya, prinsip-prinsip pembelajaran mesin masih sama, termasuk pengumpulan data, eksplorasi data, pemilihan model atau teknik, melatih model yang dipilih, dan mengevaluasi hasil ML. Untuk memahami cara kerja ML.

Ada beberapa teknik di dalam machine learning, tapi pada dasarnya secara luas hanya 2 teknik pembelajaran, yaitu terbimbing dan tidak terbimbing.

Teknik pembelajaran terbimbing adalah teknik pembelajaran mesin dengan memberikan informasi dan data tersebut sudah memiliki informasi label. Dengan begitu hasil yang didapatkan dengan membandingkan dengan data masa lalu.

Teknik pembelajaran tidak terbimbing adalah teknik dimana mesin tidak diberikan data untuk pembelajaran akan tetapi mesin dapak melakukan klasifikasi terhadap data walaupun tidak pernah diberikan data sebelumnya

Teknik algoritma multi layer perceptron merupakan salah satu teknik pembelajaran terbimbing yangmerupakan salah satu model teknologi jaringan syaraf tiruan (JST), yang memiliki nilai bobot yang lebih baik dari model lainnya, yang juga mengarah pada klasifikasi yang lebih akurat. Perceptron multilayer pertama kali diperkenalkan pada tahun 1969 oleh S. Papert dan M. Minsky. Seperti namanya, perceptron multilayer adalah pengembangan dari perceptron tunggal sedemikian rupa sehingga memiliki banyak lapisan, atau lapisan tersembunyi, yang terletak di antara status lapisan input dan output. Di bawah ini adalah ikhtisar dari lapisan/lapisan tersembunyi MLP:



Gambar 1. Gambar Lapisan Pada MLP

Perceptron multilayer juga mencakup jaringan saraf tiruan maju dengan banyak neuron atau saraf yang terhubung ke neuron lain, dengan neuron berat terhubung. Ketika setiap neuron hadir adalah unit yang tugasnya memproses dan menghitung nilai aktivasi, atau tipe input yang mewakili himpunan nenek moyang setiap unit, dari output ke output atau dari satu unit ke unit lainnya.

METODE

Metode yang diusulkan adalah dengan cara mengklasifisikasikan pesan *email* yang masuk dengan melakukan penambangan data untuk dapat mengklasifikasikan *email* secara cerdas yakni klasifikasi pesan *email* baru yang benar atau *Phishing*.

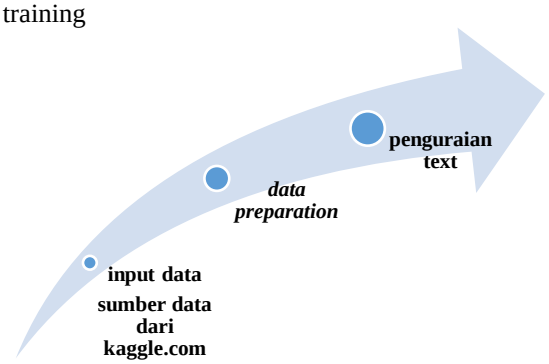
Model yang diusulkan untuk klasifikasi *email* menggunakan teknik pemrosesan linguistik dan ontologi untuk meningkatkan kesamaan antara *email* dengan arti istilah semantik yang mirip, juga prinsip frekuensi dokumen istilah diterapkan dalam pembobotan istilah *phishing* di setiap *email* sedemikian rupa sehingga pembobotan istilah *phishing email* membantu dalam membedakan *phishing* dari *email* yang benar. Dan dengan menggunakan machine learning untuk mempelejari data collection pesan *email Phishing* dan pesan *email* yang benar agar dapat membedakan kedua jenis *email* tersebut.

Langkah pertama dalam membangun pengklasifikasi *email phishing* yang diusulkan adalah

 ISSN 2686-3359 (Online)

memilih pelatihan yang sesuai kumpulan data yang merupakan contoh nyata dari *email* yang ada yang terdiri dari *phishing* dan *email* yang sah.Kumpulan data pelatihan akan digunakan untuk menemukan hubungan yang berpotensi prediktif yang akan berfungsi sebagai blok penyusun training data. kumpulan data terdiri dari 1368 *email Phishing* & 4538 yang bukan *email Phishing*.

Berikut adalah skema *preprocessing* data training



Gambar 2. *Pre-Proccesing Data*

Dari *pre-processing* diatas dibagi 3 bagian yaitu input data/training dari Kaggle.com. setelah itu dilakukan data preparation dengan menggunakan kdd, dan setelah itu text akan diurai menjadi beberapa bagian agar dapat dijadikan data training agar dapat membedakan mana *email Phishing* mana *email* yang bukan *Phishing*.

Berikut adalah gambar table training yang akan digunakan sebagai input data

This email is being sent to you because of violation security breach that was detected by our servers. Our server detected that one of the messages you received from a contact has already infected your mail with a dangerous virus. You can no longer be allowed to send messages or files to other users to prevent the spread of virus to other mail users. Please follow the link below to perform maintenance work needed to improve the protection of the web-mail for us to verify and have your account cleared against this virus. CLICK HERE WARNING!!! E-MAIL OWNERS who refuses to upgrade his or her account within 48hrs after notification of this update will permanently be deleted from our data base and can also lead to malfunctioning of the client or user's account and we will not be responsible for loosing your account.

Gambar 3. Contoh *data training Phishing*

Setelah mempelajari data latih di atas, penulis akan mengecek akurasi model menggunakan multilayer perceptron.

Multilayer Layer (MLP) adalah kelas jaringan saraf tiruan *feedforward* (ANN) yang terhubung sepenuhnya. Istilah MLP digunakan secara ambigu.

MLP terdiri dari setidaknya tiga lapisan node. lapisan masukan, lapisan tersembunyi dan lapisan keluaran. Kecuali node input, setiap node adalah neuron yang menggunakan fungsi aktivasi non-linear. MLP menggunakan teknik pembelajaran terawasi yang disebut propagasi balik untuk pelatihan. Multilayer dan aktivasi nonliniernya membedakan MLP dari perceptron linier. Itu dapat membedakan data yang tidak dapat dipisahkan secara linear.

Multi-layer Perceptron memiliki fungsi aktivasi linier di semua neuron, yaitu fungsi linier yang memetakan input berbobot ke output setiap neuron, kemudian aljabar linier menunjukkan bahwa sejumlah lapisan dapat direduksi menjadi input-output dua lapis model. Dalam MLP beberapa neuron menggunakan fungsi aktivasi nonlinier yang dikembangkan untuk memodelkan frekuensi potensial aksi, atau penembakan, neuron biologis.

Dua fungsi aktivasi yang umum secara historis adalah sigmoid, dan dijabarkan sebagai berikut

$$y(v_i) = \tanh(v_i)\ and\ y(v_i) = (1 + e^{-v_i})^{-1}$$

Dalam perkembangan deep learning belakangan ini, rectifier linear unit (ReLU) lebih sering digunakan sebagai salah satu cara yang mungkin untuk mengatasi masalah numerik yang berkaitan dengan sigmoid.

Yang pertama adalah tangen hiperbolik yang berkisar dari -1 hingga 1, sedangkan yang lainnya adalah fungsi logistik, yang bentuknya serupa tetapi berkisar dari 0 hingga 1. Berikut y_i adalah keluaran dari i simpul (neuron) dan v_i adalah jumlah bobot dari koneksi input. Fungsi aktivasi alternatif telah diusulkan, termasuk fungsi penyearah dan softplus. Fungsi aktivasi yang lebih khusus termasuk fungsi basis radial (digunakan dalam jaringan basis radial, kelas lain dari model jaringan saraf yang diawasi).

MLP terdiri dari tiga atau lebih lapisan (lapisan masukan dan keluaran dengan satu atau lebih lapisan tersembunyi) dari node pengaktif nonlinier. Karena MLP terhubung sepenuhnya, setiap node dalam satu lapisan terhubung dengan bobot tertentu w_{ij}ke setiap node di lapisan berikutnya.

Pembelajaran terjadi di perceptron dengan mengubah bobot koneksi setelah setiap potongan data diproses, berdasarkan jumlah kesalahan pada keluaran dibandingkan dengan hasil yang diharapkan. Ini adalah contoh pembelajaran terawasi, dan dilakukan melalui propagasi balik, generalisasi dari algoritma kuadrat rata-rata terkecil dalam perceptron linier.

kita dapat merepresentasikan tingkat kesalahan dalam simpul keluaran j di titik data ke n contoh $e_j(n) = d_j(n) - y_i(n)$ di mana d adalah nilai target dan y adalah nilai yang dihasilkan oleh perceptron. Bobot simpul kemudian dapat disesuaikan berdasarkan koreksi yang meminimalkan kesalahan di seluruh keluaran, yang diberikan oleh

 ISSN 2686-3359 (Online)

$$\varepsilon(n) = \frac{1}{2}\sum_j e_j^2(n).$$

Menggunakan penurunan gradien, perubahan pada setiap bobot adalah

$$\Delta\omega_{ji}(n) = -\eta \frac{\partial \varepsilon}{\partial v_j(n)} y_i(n)$$

di mana y_i adalah output dari neuron sebelumnya dan η adalah kecepatan pembelajaran, yang dipilih untuk memastikan bahwa bobot dengan cepat menyatu menjadi respons, tanpa osilasi., Turunan yang akan dihitung tergantung pada medan lokal yang diinduksi v_j yang dengan sendirinya bervariasi. Sangat mudah untuk membuktikan bahwa untuk simpul keluaran, turunan ini dapat disederhanakan

$$-\frac{\partial \varepsilon(n)}{\partial v_j(n)} y_i(n)$$

di mana $\emptyset'$ adalah turunan dari fungsi aktivasi yang dijelaskan di atas, yang tidak bervariasi. Analisis lebih sulit untuk perubahan bobot ke simpul tersembunyi, tetapi dapat ditunjukkan bahwa turunan yang relevan adalah

$$-\frac{\partial \varepsilon(n)}{\partial v_j(n)} = \emptyset'(v_j(n)) \sum_k -\frac{\partial \varepsilon(n)}{\partial v_{k(n)}} w_{kj}(n).$$

Hal ini tergantung pada perubahan berat dari titik k^{th}, yang mewakili lapisan output. Jadi untuk mengubah bobot lapisan tersembunyi, bobot lapisan keluaran berubah sesuai dengan turunan dari fungsi aktivasi, sehingga algoritma ini merepresentasikan backpropagation dari fungsi aktivasi.

Metode yang digunakan untuk mengukur tingkat akurasi machine learning *Multi-layer Perceptron* diatas adalah dengan menggunakan rasio prediksi Benar dengan keseluruhan data testing. Akurasi menjawab seberapa mirip hasil data testing setelah model diimplementasikan

$$akurasi = \frac{banyaknya\ klasifikasi\ prediksi\ yang\ sama}{total\ data}$$

HASIL DAN PEMBAHASAN

Untuk melatih, memvalidasi, dan menguji model, penulis membuat kumpulan data terdiri dari 1368 *email Phishing* & 4538 yang bukan *email Phishing*.. *Email-email* ini dulu dikumpulkan dari dataset yang bersumber dari Kaggle. Berikut table total dataset

Tabel 1. Dataset *Phishing* yang dikumpulkan

Total Sample	5906
Total *Phishing* Mail	4538
Total *email* yang benar	1368
Total training sample	4580
Total testing sample	1146

Karena beberapa pengklasifikasi tidak dapat dilatih pada data kategorikal, dataset melewati proses pra-pemrosesan di mana semua text akan diurasi dan nilai nominal diubah menjadi nilai numerik. model konversi yang sama digunakan untuk memetakan data nominal ke nominal satu di seluruh dataset.

Evaluasi kinerja dari algoritma adalah mengukur tingkat akurasi machine learning Multi-layer Perceptron diatas adalah dengan menggunakan rasio prediksi Benar dengan keseluruhan data testing. Akurasi menjawab seberapa mirip hasil data testing setelah model diimplementasikan.

```
text_clf.fit(trainX, trainY)
predicted = text_clf.predict(testX)
result = np.mean(predicted ==  testY)
result
```

```
Out[26]: 0.9965095986038395
```

Gambar 4. Hasil Prediksi model

Dari gambar diatas dengan meggunakan Multi-layer Perceptron prediksi model didapatkan tingkat akurasi 99.65%. dengan hasil ini dapat disimpulkan bahwasanya penganganan keajahatan Phishing dengan menggunakan algoritma Multi-layer Perceptron cukup berhasil.

```
Results on the test set:
              precision    recall  f1-score   support

          no       1.00      1.00      1.00       868
         yes       1.00      1.00      1.00       278

    accuracy                           1.00      1146
   macro avg       1.00      1.00      1.00      1146
weighted avg       1.00      1.00      1.00      1146
```

Gambar 5. Hasil klasifikasi report

Dari hasil klasifikasi report diatas didapatkan tingkat akurasi 100%. Dari dua evaluasi diatas didapatkan tingkat akurasi model Multi-layer Perceptron sangat berhasil untuk mengatasi penanganan kejahatan Phishing.

KESIMPULAN DAN SARAN

Dari evalusi performansi model *Multi-layer Perceptron* menggunakan dataset *email* yang bersumber dari Kaggle yang terdiri dari 1368 *email Phishing* & 4538 yang bukan *email Phishing*..dan pengguna pengguna akan menguji tingkat akurasi dengan menggunakan algoritma *Multi-layer Perceptron*. Setelah dilakukan pengujian, tingkat prediksi didapatkan 99.65%. dan dari klasifikasi report tingkat akurasi mencapai 100 % ini membuktikan

 ISSN 2686-3359 (Online)

bahwasanya model *Multi-layer Perceptron* cukup efektif untuk menangani tindak pindana kejahatan *Phishing*.

Sebaiknya untuk penelitian selanjutnya agar model *Multi-layer Perceptron* untuk penangan kejahatan *Phishing* dapat di impmentasikan dengan menambahkan hyper parameter dan juga bisa dilakukan dengan Teknik deep learning.

DAFTAR PUSTAKA

[1] Tata Sutabri, R. Pandi Selvam, K. Shankar, Phong Thanh Nguyen, Wahidah Hashim, Andino Maseleno, 2019, *Machine Learning for Healthcare Diagnostics*, Blue Eyes Intelligence Engineering & Sciences Publication, BHOPAL, Madhya Pradesh 462021, IN

[2] Tata Sutabri, 2012, *Komputer dan Masyarakat*, Penerbit Andi, Yogyakarta

[3] Adwan Yasin, Abdelmunem Abuhasan, 2016, *AN INTELLIGENT CLASSIFICATION MODEL FOR PHISHING EMAIL DETECTION*, International Journal of Network Security & Its Applications (IJNSA)

[4] Fatima Salahdine, Zakaria El Mrabet, Naima Kaabouch, 2022, *Phishing Attacks Detection A Machine Learning-Based Approach*, Cornell University, New York City.

[5] Meha Desai, Manan Shah, 2020, *An anatomization on Breast Cancer Detection and Diagnosis employing Mul- ti-layer Perceptron Neural Network (MLP) and Convolutional Neural Net- work (CNN),* Elsevier B.V. on behalf of KeAi Communications Co. Ltd.

[6] Jaswinder Singh, Rajdeep Banerjee, 2019, *A Study on Single and Multi-layer Perceptron Neural Network*, IEEE, New York City.

[7] Ali Asghar Heidari, Hossam Faris, Seyedali Mirjalili, Ibrahim Aljarah & Majdi Mafarja, 2019, *Ant Lion Optimizer: Theory, Literature Review, and Application in Multi-layer Perceptron Neural Networks*, Springer, Nature Switzerland AG.

[8] Areej Alhogail, Afrah Alsabih, 2021, *Applying machine learning and natural language processing to detect phishing email*, Elsevier Ltd.

[9] Sikha Bagui, Debarghya Nandi, Subhash Bagui, 2019, *Classifying Phishing Email Using Machine Learning and Deep Learning*, IEEE, New York City.

[10] Sikha Bagui, Debarghya Nandi, Subhash Bagui, 2019, *Classifying Phishing Email Using Machine Learning and Deep Learning*, IEEE, New York City.

[11] Naghmeh Moradpoor, Benjamin Clavie, Bill Buchanan, 2017, *Employing machine learning techniques for detection and classification of phishing emails*, IEEE, New York City.

[12] Harikrishnan NB, Vinayakumar R, Soman KP, 2018, *A Machine Learning approach towards Phishing Email Detection*, IWSPA.

[13] Tianrui Peng, Ian Harris, Yuki Sawa, 2018, *Detecting Phishing Attacks Using Natural Language Processing and Machine Learning*, IEEE, New York City.

[14] Panagiotis Bountakas, Konstantinos Koutroumpouchos, Christos Xenakis, 2021, *A Comparison of Natural Language Processing and Machine Learning Methods for Phishing Email Detection*, Association for Computing Machinery, New York City.

[15] Bagui, Sikha; Nandi, Debarghya; Bagui, Subhash, 2021, *Machine learning and deep learning for phishing email classification using one-hot encoding*, University of West Florida, Pensacola.