https://doi.org/10.31871/IJNTR.6.10.12
International Journal of New Technology and Research (IJNTR)
ISSN: 2454-4116, Volume-6, Issue-10, October 2020 Pages 01-05

Visual Cryptography Based Phishing Suppression for Online Voting System

Nikitha Kaveriappa, Dr. R. Aparna

***Abstract*— In the present world due to the busy schedule of people the casting of their votes for elections is been very less. The main reason for not casting the vote be reaching their voting center because people work in different work location far away from their native places. Many other reasons like waiting in the lengthy queue, few may not be interested in politics, elder people may not be having knowledge of voting and etc. Government and Information Technology (IT) with the means of available electronic infrastructure are parallel improvising the voting system in a timely manner to encourage the people for voting. We go through few online voting system proposals proposed in the recent past and come across few drawback of the systems such as hacking of network, server problems, security breach, and phishing. We take phishing as a major drawback and improvise the system for phishing attacks. Attempting to get the confidential and personal information of an organization or an individual by an unknown suspicious user is defined as Phishing. We reframe the online voting system to prevent such phishing attacks based on Visual Cryptography (VC) which goals at providing a capability to cast poll for confidential and critical commercial assessments. The system allows the users to cast their vote from any remote location in a fully confidential and secure manner so that the casted vote reaches to the participating candidate correctly. When the voter logs into to the voting system, needs to enter a password, generated by the system by combining the two parts of VC methodology. The first part of the password will be sent to the voters registered email id before the election, while the second part of the password will be generated the voting device. The voter needs to enter the combined password during the voting process to cast his vote. The system is been tested with various known phishing attacks and results are obtained as forecasted.**

***Index Terms*— online voting, evoting, pishing, hacking, Visual Cryptography.**

I. INTRODUCTION

Counting or casting of votes during the elections by means any electronic means or devices is defined as Electronic voting (e-voting).

Dependent on specific application, e-voting can use individual electronic polling machineries (EVM) or PCs linked to Internet. It can incorporate a variety of Internet facilities, as of rudimentary broadcast of tabularized outcomes to full-function operational polling through communal connectable domestic strategies. The grade of automation can be restricted to coloration a paper vote, or can remain a broad arrangement of vote input, recording vote, documents communication to servers, encryption, tabulation and amalgamation of poll outcomes.

Internet voting (iVoting) is one such exclusive resolution that merely and suitably assistances to involve people in governance procedure. Estonia was the first nation in the sphere to hold countrywide votes by means of this system, it created headings as leading republic to custom iVoting in governmental polls.

iVoting is a scheme which permits electorates to company their votes through any internet associated computer wherever in sphere. Entirely unconnected to electronic polling schemes cast-off elsewhere, this include expensive and challenging equipment, the Estonian resolution is modest, secure and elegant. In circumstance of iVoting, the accumulative time saved in the previous Estonian polls was 11,100 salaried days.

An earnest e-voting scheme necessity accomplish maximum of these chores while fulfilling with a set of principles recognized by supervisory physiques, and necessity also be proficient to deal effectively with robust necessities accompanying with accuracy, safety, integrity, confidentiality, swiftness, availability, auditability, cost-effectiveness, ecological sustainability and scalability.

Security authorities have originated safety glitches in each effort at online polling, comprising schemes in Estonia Switzerland, Australia, United States and Russia.

It has remained contended political events that partake additional provision from fewer privileged those are unaccustomed with Internet might suffer in polls due to e-voting, that inclines to upsurge polling in middle and upper class. It remains uncertain as to whether tapering the digital division would endorse equal voting occasions for persons transversely numerous communal, economic and cultural circumstances. In extended run, this dependent not only on internet availability, but likewise be contingent on publics glassy of knowledge with Internet.

A reading in 2017 of online polling in two Swiss regions originate that it taken no result on numbers. An article on "distant electronic polling and numbers in Estonian 2007 parliamentary polls" presented that moderately than removing dissimilarities, e-voting potency have improved the digital division amongst lower and higher social and economic classes. Persons who survived superior detachments from voting areas elected at greater levels with this facility now obtainable. The Estonian polls 2017 produced a developed elector numbers from those who survived in developed income areas and who established formal schooling.

E-voting is professed to be preferred besides by a convinced demographic, specifically the earlier generation similar as

Nikitha Kaveriappa, PG Scholar, Cyber Forensics & Information Security, Department of Information Science & Engineering, Siddaganga Institute of Technology, Tumakuru, India.
Dr. R. Aparna, Professor, Department of Information Science & Engineering, Siddaganga Institute of Technology, Tumakuru, India

Generation Y and X electors. Though, in latest polls around a quartier of e-votes remained cast by elder demographic, similar to persons over age of 58. Comprising this, around 21% of e-polls came as of electorates between the ages of 40 and 55. This energies to demonstration that e polling is not sustained solely by newer generations, but result some admiration between Baby Boomers and Gen-X as well.

The complete persistence of online polling is to upsurge political contribution. The custom in determinations in illustrative republics aims at contradicting democratic weariness and lethargy. Growing political contribution is also goalmouth of democratic inventions and new participating mechanisms in political administrations. Liquid republic is mainly active within Pirate Gatherings as an income to democratize party constructions and make new straight, participatory governmental groups. The impression that online polling can upsurge political partaking is likewise at the heart of various techno subjects of the 90s that intended an inclusive cyber republic through the resources of digital ballots.

II. Existing Metods

We brief out few of the existing methodologies in the regard to e-voting, online voting and the effects of these e-voting systems. We also brief out the outcomes and limitations of the system we have surveyed upon and propose the VC based methodology for an efficient online voting system.

A. VC based Phishing avodince [1]

Saloni Sunil Rane et.al proposed a visual cryptography in polling method to stretch endowment for artifact poll for internal conclusions in an association. It is elastic sufficient to cast poll from distant residences. Voting is an entire trustworthy procedure and is detained with extreme secrecy. Henceforth, they have projected an online polling scheme for Maharashtra Carom Connotation where affiliates can troupe their poll with their laptops and computers. To uphold the safety they use a CAPTCHA cypher and image Share equipment. The projected technique proposals concealment of voter individuality, while custody the poll's isolated, and the election translucent and safe.

B. PhishHaven [2]

Maria Sameen et.al, design an collaborative machine learning founded recognition arrangement called PhishHaven to recognize AI produced as fine as human fashioned phishing URL's. To the finest of their awareness, this was the leading study to deliberate perceiving phishing outbreaks by together AI and human aggressors. PhishHaven services vocabulary examination for feature withdrawal. To additional enhance lexical examination, they familiarize html, URL encoding to categorize URL on hover and proactively associate with certain of the prevailing approaches. They also present a URL Hit method to contract with small URLs, that is an exposed problematic yet to be resolved. Furthermore, the final arrangement of URLs is completed on an impartial voting apparatus in PhishHaven, that goals to evade misclassification once the amount of elects is equivalent. To rapidity up the collaborative founded machine learning prototypes, PhishHaven employments a multi-threading method to implement the organization in equivalent, leading to real-time discovery. Theoretical examination of resolution demonstrations that it can continuously identify minute URLs, and in addition it can identify forthcoming AI produced Phishing URLs founded on our designated lexical topographies.

C. PhishBox [3]

Jen-Hao Li et.al, propose a method called PhishBox, to efficiently collect phishing data and produce replicas for phishing authentication and discovery. The projected approach assimilates the phishing websites gathering, validation and discovery into an on-line implement that can observer the prohibit of PhiahTank and authorize and sense phishing websites. The method uses two phase discovery classical to guarantee the presentation. The chief they project an ensemble classical to authenticate the phishing data and smear the active knowledge for plummeting the price of manual classification. The outcome parades that collective confirmation classical can attain high presentation with good accurateness and a smaller amount false-positive ratio. The subsequent stage, the authenticating phishing figures will be castoff to train a recognition model. Associating with unique dataset, the false-positive ratio of phishing recognition was fallen. After contributing the voting process on PhishTank, the outcome shows that projected two-stage prototypical is operative to authenticate phishing websites. Lastly, they display the blacklist and originate that blacklist comprises lots of distinct data.

D. Anti-Phishing for I-Voting [4]

Ramya. R. Nelli et.al, proposed an I-polling scheme VC aims at providing a capability to cast poll for critical and trusted internal commercial conclusions. The operator or the worker is permissible to company his or her poll from any distant residence. The poll is detained in full concealment where the operator is allowable to poll solitary if he logs into the arrangement by inflowing the correct password. The PIN is created by assimilation two parts by VC scheme. Formerly the balloting proprietor directs part 1 to the elector's e-mail id and part 2 will be obtainable in voting arrangement for his login through balloting. Elector then chains part 1 and part 2 by VC to get the undisclosed PIN. No evidence can be exposed by detecting any one part.

E. Unauthorized Login Attempts Detection and Prevention[5]

Shammi Ishara Hewamaddumaal proposed a structure to examination the custom of phishing outbreaks and hazards it postures to clienteles and group, then to discovery out the obtainable approaches to perceive and avoid unauthorized login efforts, the skills and security softness of those approaches and lastly to suggest a resolution to identify and prevent unlawful login efforts by means of interactive based examination, IP and device documentation tools.

III. Proposed Methodology

An image Capatcha algorithm in addition with visual Cryptography based methodology is been proposed for detection and prevention of phishing attacks. Here we use

result reconstruction and share generation algorithms for password creation and verification.

The basic objectives of the system are to define a system that allows the people anywhere in world, old age people and physically disabled can be able to cast their vote from the place they stay in an easy and secure manner. Secondary objective would be allowing only authorized people to cast their vote only one time.

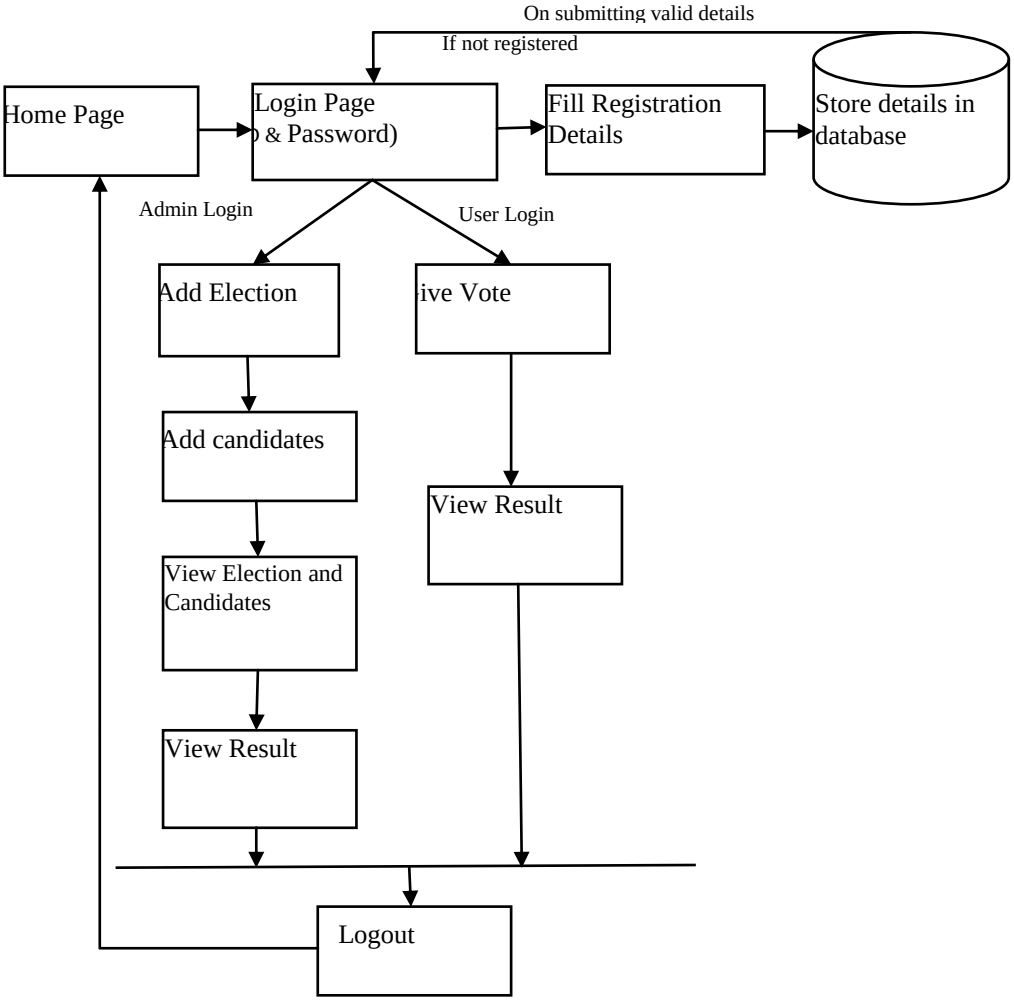

Figure 1. Proposed Online Voting System

Cryptography is a well-known safe method for safeguarding any data. The knack of progressing and gathering encrypted memoranda that be able to decrypt only by the collector or forwarder. Encoding and decoding are skillful by means of procedures in such a way the envisioned receiver can decode and he be able to recite the message. Shamir presented VC structure as a tranquil and safe method to permit the secret allocation of imageries deprived of any cryptographic glitches. In situation of VCS, every pixel in unique imageries encoded into two substitute pixels named shares. Neither dividends deliver any sign about unique pixel since dissimilar pixels in secret images will be encoded by individualistic arbitrary selections. When two parts are stratified, worth of unique pixel be able to be dogged. If a dogged pixel is a dark pixel, we will acquire two dark sub-pixels; if a dogged pixel is gray pixel, we drive get single dark and one white sub-pixel.

IV. Implementation

During the registering stage the greatest significant part is formation of dividends from the images captcha where unique part is directed to elector or operator mail id beforehand the balloting and other part can be reserved with server. For login, the operator wants to enter a lawful username in specified field. Formerly he partakes to browse his portion and procedure in the server adjacent, each pixel as of secret images is encrypted into manifold sub-pixels in every part image by a matrix to decide the shade of the pixels.

A. Binary Image Allocation Technique

An image having only two possible values in its pixel can be defined as a binary image. Black and white are the two colors castoff for such image, where every pixel is stowed as a solitary bit 0/1. For twofold images, in instruction to custom the projected system, the grayscale glassy (k) must be reserved as 2. The remaining part of the process is similar for building of parts and enlightening stage to recuperate the secret image. Essential Thoughts of binary Image Allocation Procedure:

Take a x b size binary image in a sequence manner, each and every pixel is check if it's white or black. For each pixel, we custom a arbitrary function to select a group of pixels as of the code volume that contributes two set of pixels for each selected pixel, one conforming to part 1 whereas other conforming to part 2 of image. At the culmination of the step, dual parts of dimension a x 2b are produced. In the rebuilding procedure collecting together the collective imageries to rebuild the inventive binary image. Enchanting the consistent

pixels as of together the joint imageries we produce a novel pixel by performance the operation not(X plus Y) here, X is pixel as of part 1, Y is pixel as of part 2, plus signifies the twofold OR maneuver, and not signifies the binary negation (NOT) process.

B. Grayscale Image Allocation Technique

The procedure of part building stage and image rebuilding stage of secret images distribution system for grayscale image remain as shadows. Obtaining of jumbled image by means of a PIN to produce a permutation categorization to permute the pixels of image. Produce x-1 arbitrary matrices A1,.....,Ax1, every of matrix of that has size a x b and constituent be [0,.....,z-1] for an images through z gray scale planes. Calculate Gx = (zJ - G1 .....- Gx-1) with mod of z, here G is unitary matrix along with dimension a x b. Calculate Hi = (Gi + Image) mod z. Calculate Sx = (Gn + zJ - (k-2)image) mod z. The Image Rebuilding process is by I'= (S1 +....+ Sx) mod z. Smear converse clambering process to I' to obtain the reassembled image I'.

C. Color Image Allocation Technique:

Aimed at color images, any anticipated colors can be attained by mingling embryonic insignia RGB. In the real time color system, the pixel values of RGB are represented by 8 bit values which are ranging from 0-255. To encompass the projected arrangements for gray scale to color images, three stages are necessary. Initially, crumble color image hooked on three parts as R, G and B, every of part can be realized as gray scale image. Formerly implement the projected structure for gray scale images to every module of RGB. Lastly, combine RGB parts to produce portions. In illuminating stage, again take disintegrated RGB parts of the parts and implement the projected structure distinctly. Lastly combine the produced RGB parts to recuperate the secret images. On the server side the operator's part is joint with the portion in server and an images captcha is produced.

V. Results And Discussion

We explain in details about the outcomes and results of our developed module. We can see initial registration page created for a new user in figure 2. The figure 3 represents the authentication page where the user is required to enter the login id and upload the images received.

If the passcode is not observable formerly it specifies that operator has not delivered the precise part of code. If two inacceptable parts are combined then we don't get the PIN. This specifies that website is not honest and the customer is not authenticated.

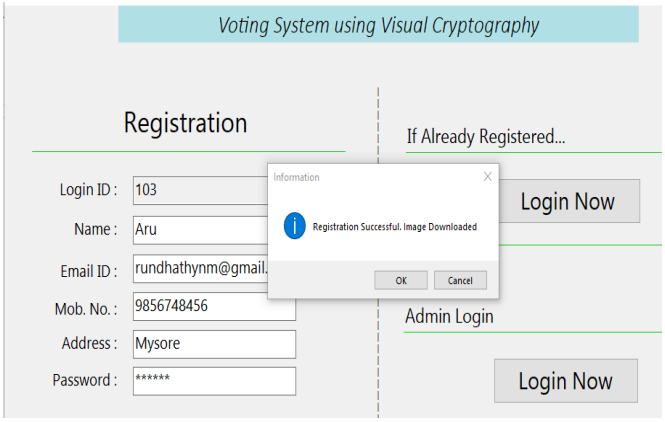

Figure 2. Registration Page

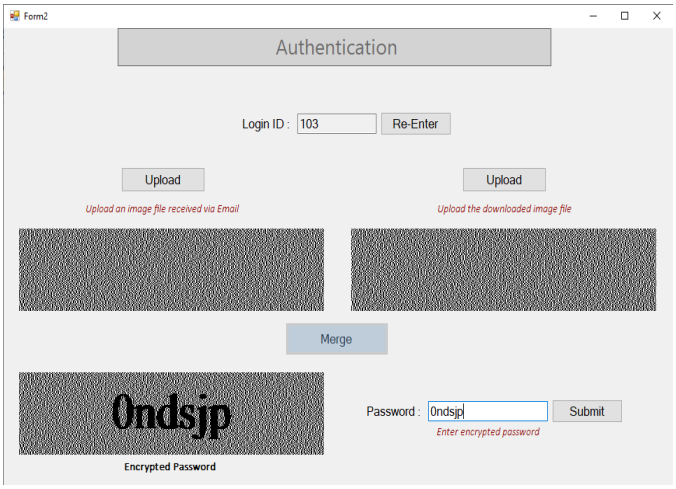

Figure 3. Authentication Page

Figure 4. Voting Page

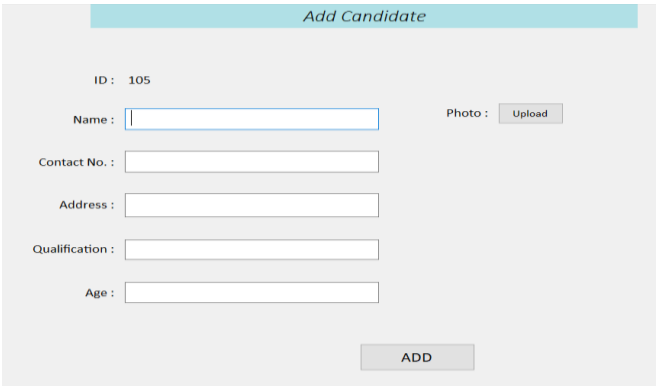

Figure 5. Adding of Candidate

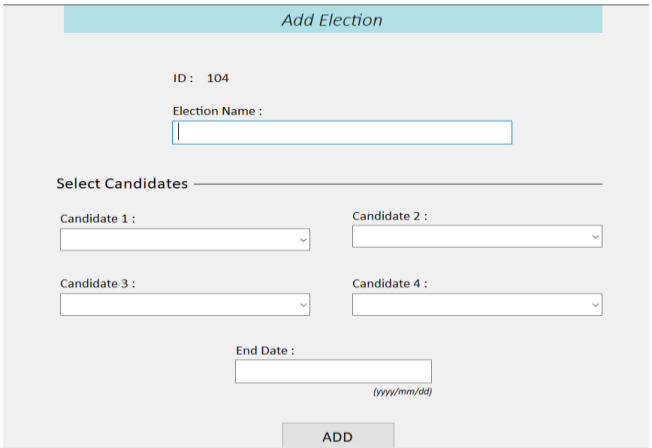

Figure 6. Adding of Election

If unregistered customer attempts to login then a fault message asserting unacceptable user id will be exhibited. If a customer attempts to vote additional than one time for a specific group then an error memo stating applicant already voted will be presented.

Figure 4 shows the online voting page created and tested during our development, few standard images are been displayed as a user. The next figure 5 & 6 display the addition of candidate and election which are explicitly for admin. We also display the result image of the mail received after successful registration.

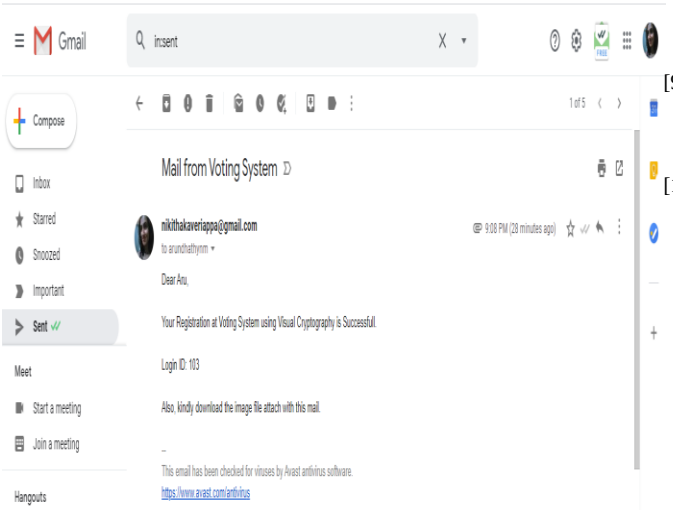

Figure 7. Mail Confirmation after Registration

VI. Conclusion

Voting through elections is a significant part for any independent nation. If the scheme is employed, at that moment the polling percentage can be enhanced more since certain percentage of our people are occupied in international and they are not capable to originate to intuitive nation during the time of polling. For those persons as fine as for persons who are substantially deactivated and identical old also can variety use of the online polling arrangement. Meanwhile Visual Cryptography method is castoff, customer can be capable to discovery out if he is in original or phishing site straightforwardly. Projected online polling scheme is very operative and it will be beneficial for electorates and it will decrease time and cost.

References

[1] S. S. Rane, K. Adwait Phansalkar, M. Y. Shinde and A. Kazi, "Avoiding Phishing Attack on Online Votig System Using Visual Cryptography," 2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2020, pp. 1-4, doi: 10.1109/ICCCI48352.2020.9104071.

[2] M. Sameen, K. Han and S. O. Hwang, "PhishHaven—An Efficient Real-Time AI Phishing URLs Detection System," in IEEE Access, vol. 8, pp. 83425-83443, 2020, doi: 10.1109/ACCESS.2020.2991403.

[3] J. Li and S. Wang, "PhishBox: An Approach for Phishing Validation and Detection," 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), Orlando, FL, 2017, pp. 557-564, doi: 10.1109/DASC-PICom-DataCom-CyberSciTec.2017.101.

[4] Ramya. R. Nelli, Rashi Mehra, Pallavi Madri, Monica S, Rajeshwari J, "Anti-Phishing I-Voting System using Visual Cryptography", I International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Issue 5, May 2017, pp 113-119, DOI10.17148/IJARCCE.2017.6522.

[5] S. I. Hewamadduma, "Detection and prevention of possible unauthorized login attempts through stolen credentials from a phishing attack in an online banking system," 2017 International Conference on Research and Innovation in Information Systems (ICRIIS), Langkawi, 2017, pp. 1-6, doi: 10.1109/ICRIIS.2017.8002440.

[6] Thomas T., P. Vijayaraghavan A., Emmanuel S, "Machine Learning and Cybersecurity. In: Machine Learning Approaches in Cyber Security Analytics," Springer, Singapore, (2020).

[7] Suleman, Muhammad Taseer, and Shahid Mahmood Awan, "Optimization of URL-Based PhishingWebsites Detection through Genetic Algorithms," Automatic Control and Computer Sciences 53, no. 4. pages 333–341, 2019.

[8] Mao, Jian, Pei Li, Kun Li, Tao Wei, and Zhenkai Liang, "BaitAlarm: detecting phishing sites using similarity in fundamental visual features," 5th International Conference on Intelligent Networking and Collaborative Systems, pages 790–795, IEEE, 2013.

[9] I. Waziri, "Website Forgery: Understanding Phishing Attacks and Nontechnical Countermeasures," 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, New York, NY, 2015, pp. 445-450, doi: 10.1109/CSCloud.2015.77.

[10] S. Gupta, A. Singhal and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," 2016 International Conference on Computing, Communication and Automation (ICCCA), Noida, 2016, pp. 537-540, doi: 10.1109/CCAA.2016.7813778.