International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-10 Issue-2, December 2020

Homograph Attack Warning System

Muhammad Uwais, Arpit Sharma, Akhil Kumar, Lakshya Singh

Abstract*— As we are living in the era of social media apps, from Facebook to WhatsApp which are using everywhere. All these apps are being used by everyone. Although this may seem to be a very good sign that we are moving to the new era of "THE DIGITAL WORLD" but it may have some consequences like spreading of artificial news, crack of personal information like credit card, debit card, passwords or digital wallets etc. The users believe that every message shared on social media might be true. So, to protect our internet users we have come up with an idea that provides the ability to discover homonym attack and malicious links which warns the user before they can access the site. The Social engineering attacks have stirred terribly removed from this like fraudulent attack within which we tend to completely rely upon our browser to present north American nation a warning. This situation may worry some computer users, but we generally do not think much about when we perform any action on our mobile phones. But all these so called to do steps are not the right way to deal with these situation .The primary commitments of this paper are understanding a working meaning of IDN satirizing assaults and how those IDN spaces are being introduced in the URL bar in some Internet programs, proposing a working arrangement that reports IDN ridiculing assaults which convert URL into Unicode and punycode.

***Keywords*: Internationalized Domain Name (IDN), UNICODE, PUNYCODE, Universal Resource Locater (URL), HOMOGRAPH**

I. INTRODUCTION

The venture will be a versatile application for any individual who is utilizing any internet based life applications like WhatsApp, Facebook and so forth., This will assist the client with using the protected connections on their portable which is imparted to them. The framework will incite the client an admonition every time he visits an awful connection it won't simply manage straightforward and surely understand awful connection which can be identified effectively by any individual who have some fundamental learning about the PC however it might likewise hinder any connection which may even trick a weirdo.

Revised Manuscript Received on December 30, 2020.
***** Correspondence Author
Muhammad Uwais*, Department of Computer Science and Engineering, Ganeshi Lal Bajaj Institute Of Technology and Management, Greater Noida, India. Email: muhduwais007@gmail.com
Arpit Sharma, Department Of Electronics and Telecommunications Engineering, K.J. Somaiya Institute of Engineering and Information Technology, Mumbai, India. Email: arpit14@somaiya.edu
Akhil Kumar, Department of Computer Science and Engineering, Ganeshi Lal Bajaj Institute Of Technology and Management, Greater Noida, India. Email: akhil.bhardwaj1998@gmail.com
Lakshya Singh, Department of Computer Science and Engineering, Ganeshi Lal Bajaj Institute Of Technology and Management, Greater Noida, India. Email: lrajpoot592@gmail.com

The primary advantage of this undertaking is that it will totally kill the assistance of the program to recognize such assaults and any client connection to confirm the area provoke the client and will identify any assault which may even go through the program insurance. The venture will be a portable application for any individual who is utilizing any internet based life applications like WhatsApp, Facebook and so forth., This will assist the client with using the sheltered connections on their versatile which is imparted to them. The framework will an admonition every time the client visits a horrendous connection. It is a simple thing when the user visits a vicious link which is known. If the user already known's that the particular link is a vicious link the user will not visit the link. The problem occurs when the link which is received through the social appswill exactly looks like the usual safe link then the user will visit the link. In this paper, we have developed a warning system which removes most of the drawbacks of the current system. Only when the user visits the safe link the user visits the browser otherwise the user is given an alert message so that he may not access that particular link and the user will not be affected by the cybercrimes like homograph and the phishing attacks etc.

II. EXISTING WORK

In the existing system they are using machine learning concepts to detect the malicious system. The user have to fetch the link from the social media's and have to search in the web browser to detect the URL's. Since we are using machine learning concepts it is a time taking process and the user device may easily attack by the hackers and also the device may hang easily with in a fraction of seconds.

The machine learning concepts like deep learning and neural networks [1] are used to detect the malicious link. In neural network, it splits the URL into single character and the detection of the malicious link is done by classifying the single character. In deep learning they use blacklist detection.

III. RELATED WORK

In the Fig 2.a the user asks his/her friend to send the Link of an Apple website, but the friend mislead him and shared the Unicode domain [6] which looks identical to the original Apple website.

If this to be put in the way of an attacker then the result could have been different, it may be possible that he may enter his credentials onto the website assuming it is all good. So, to stay our caring web and users safe we've got return up with this project plan that provides the user with the flexibility to sight attack links that warns them before they will access the positioning.

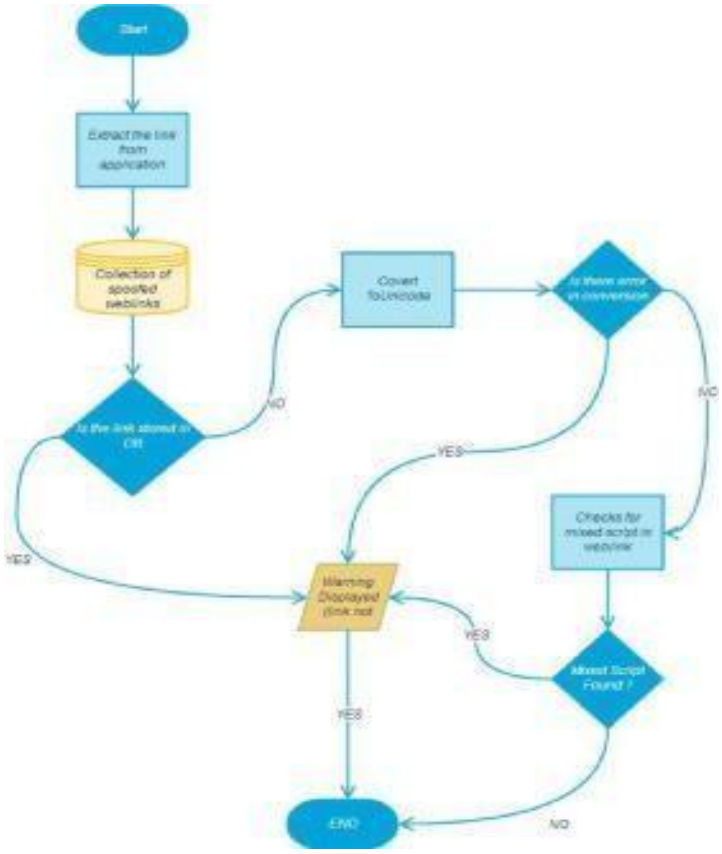


Fig 2.a. After clicking on the link that has received the we will get an error which was displayed in the fig2.b.The error will be detected after the user visits the browser.

IV. PROPOSED WORK

As India is moving towards Digitization the increasing in cybercrimes will affect the day to day life a common man [7].The primary focal point of this undertaking is to carry arrangement to the present framework by wiping out every one of these issues and giving a protected situation structure digital wrongdoings . It is likewise a prospect for Digital India.

The essential plan requirement is the Mobile Application. Since the application is assigned for Android Mobiles, effective GUI [8] and well ease of use will be the significant plan contemplations.

Making a UI which is both effective and effectively navigable is significant.

We are using the database to store the different data of the mock web links so extra room should be considered for smooth working of framework.

Other restriction, for example, memory and handling force are likewise worth considering.

Efficiency should be considered since it is one of the significant reasons of having a robotized framework.

The information and yield created and their individual working efficiency and its commitment to the general programming application should likewise be considered. The product will give the ideal outcomes as output,now framework work process as demonstrated as follows.

This System works in four steps:

1) Module 1:

The system will starts working when the user links the link which is received from the social media.

The system will extract the link from the app and search the subsequent link in the database. If the link if found in the database if will alert the user else the link is forwarded to the next module of the system.

2) Converter:

In this module we fetch the link from the first module and convert the ASCII characters into the UNICODE format.

If there is any error in the Unicode the system will alert the user,else the obtained Unicode is transferred to the next module of the system. To convert the fetched link, we use UTF-8[3] encoding algorithm.

3) Module 2:

In this module the system will generate the puny code for the obtained Unicode.

After generating puny code, the system will check for errors along with the certain conditions that have to be followed by the puny code of the givenURL [4].

If the obtained puny code does have any errors then the system will alert the user, else it is forwarded to the next module of the system.

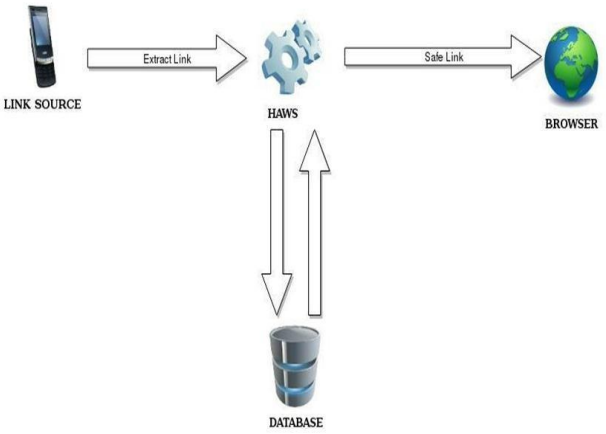
4) Premonitory System:

In this module it will alert the user if the user visits any malicious link and if the user visits a safe link then it will direct it to that particular website .So that the user can access the link safely.

V. SYSTEM DESIGN

The planning of the project may be divided into three phases that are as follows:

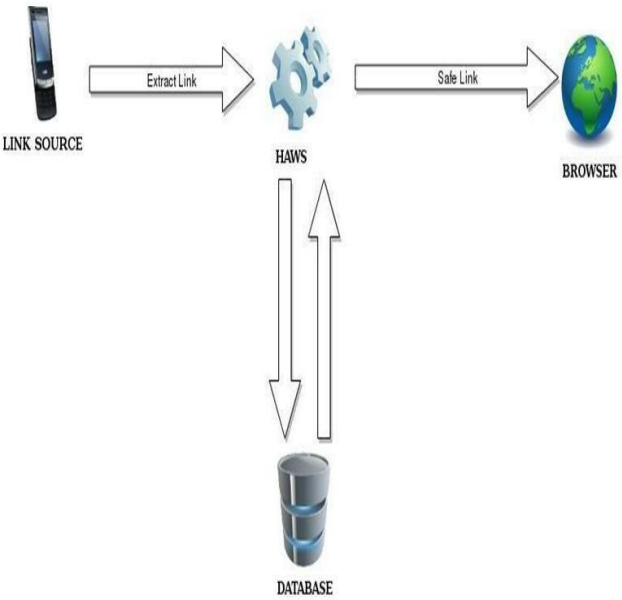
- **User Interface Style**: During this section, the Computer Program of the project is developed. That is, the planning of our application via that the user can move for the warning issued as per the cases.
- **Database**: The database is the pool of information for every application .
  In our application, the database is used to store the most popular websites spoofed link and malicious sites link that appearance the same as high 10k domains of Alexa. The information also will store each web site that it will observe as “Not Safe” and so create our method quick to observe the identical issue within the next future occurrence.
  The below diagrams show the representation between different entities of our project.



- **Complete Design**: In this section a complete flow diagram of the working system is designed.
  As per the following three stages, we will now start our implementation of the project.

VI. RESULTS

The below diagram shows the implementation and working of the project.



Warning System: This module will come into the action as soon as it gets the Punycode Security researcher have sounded the alarm bells and warned that Firefox, Chrome and Opera, have a vulnerability that creates phishing attacks easier.

The vulnerability lies within the ease with thatassociate in nursing offender will produce a spoof website with a computer address that appears precisely the same as the real thing.

It relies on the way that many browsers interpret Punycode, or the extracted link is found in the database.

PUNYCODE: Punycode be the simplest way of representing Unicode, the standard method by which computers encode text of non-Roman languages such as Arabic or Mandarin and accented characters such as "ü". Using Punycode, URLs containing Unicode characters are diagrammatical as American Standard Code for Information Interchange characters consisting of letters, digits and hyphens [8][9].

The issue emerges in the way that comparative characters are difficult to distinguish from one another. While a Cyrillic little letter "a" (Unicode character U+0430) is unique in relation to a Latin little letter "a" (U+0061), in a defenseless program they look a similar when the Punycode is translated.

Therefore, the owner of the name xn--80ak6aa92e.com, which is displayed as "apple.com" could create a convincing phishing site.

The Below flow chart shows our proposed work explained clearly in diagrammatical representation. Our assessment of the proposed implementation shows that the proposed solution to the IDN-based homograph attack protect user’s mobile phone with no noticeable overhead. Punycode is a simple and efficient transfer coding syntax designed to be used with Internationalized Domain Names in Applications (IDNA).

It unambiguously and reversibly transforms a Unicode string into a computer code string.

ASCII characters within the Unicode string square measure drawn virtually, and non-ASCII characters are represented by ASCII characters that are allowed in host name labels (letters, digits, and hyphens).

This document defines a general rule known as called Bootstring that enables a string of basic code points to unambiguously represent any string of code points drawn from a bigger set. Punycode is an instance of Bootstring that uses a particular parameter values specified by this document, appropriate for IDNA.

VII. CONCLUSION

To make Internet progressively available to individuals whose essential dialects are not English, IETF started the IDN standard and numerous recorders have opened the enrollment for IDNs. Through quantitative investigation, our examination demonstrates the volume of IDNs has been relentlessly developing over years, and now more than 1.4 million IDNs are enlisted.

Despite the expansion in volume, their incentive to Internet clients is far under desire. Through stratified examining examination, we found just 19.8% IDNs convey important substance, contrasted with 33.6% of ASCII areas. Additionally, visits to them are far less regular than non-IDNs under gTLDs like com. What makes IDN progressively tricky is that new assault vectors have been empowered and manhandled for digital assaults like brand phishing. IDN is known to empower homograph assault and we found 1,516 IDNs taking after known brands. In any event 100 of them are affirmed malevolent. All things considered, assailants have a huge up-and-comer pool of beguiling IDNs, given that 42,671 IDNs can be utilized for homograph assault and a large portion of them are unregistered. What stays less known is thatIDN can be intended to befuddle clients by cushioning watchwords or interpreting English brand names (called semantic assault). We found 1,497 IDNs under the main case, and a few brands (like 58.com) are focused by more than 100 IDNs. We accept the improvement of IDN needs amendment and endeavors ought to be saved by all elements in Internet, including libraries, enlistment centers and Internet software. To make clients security we go over the homograph assault which is running on application before getting to any connection that application will give us ready notice whether the connection is protected or not. If ready notice is sheltered at that point continue to that connection further else, it diverts to that application from where that connection we clicked.

REFERENCES

1. KumaravelA., MeeteiO.N.,An application of non-uniform cellular automata for efficient cryptography,2013 IEEE Conference on Information and Communication Technologies, ICT 2013,V-,I-,PP-1200-1205,Y-2013
2. KumaraveA., Rangarajan K.,Routingalogrithmover semi-regular tessellations,2013IEEEConferenceonInformationandCommunication Technologies, ICT 2013,V-,I-,PP-1180-1184,Y-2013
3. DuttaP.,KumaravelA.,Anovelapproachtotrustbasedidentificationof leaders in social networks,Indian Journal of Science and Technology,V-9,I-10,PP--,Y-2016
4. KumaravelA., Dutta P.,Application of Pcafor context selection for collaborative filtering,Middle - East Journal of Scientific Research,V-20,I-1,PP-88-93,Y-2014
5. KumaravelA., Rangarajan K.,Constructing an automatonfor exploring dynamic labyrinths,2012 International Conference on Radar, Communication and Computing, ICRCC 2012,V-,I-,PP-161-165,Y-2012
6. KumaravelA.,Comparison of two multi-classification approaches for detecting network attacks,WorldApplied Sciences Journal,V-27,I-11,PP-1461-1465,Y-2013
7. TariqJ.,KumaravelA.,Constructionofcellularautomataoverhexagonal andtriangulartessellationsforpathplanningofmulti-robots,2016IEEE InternationalConferenceonComputationalIntelligenceandComputing Research, ICCIC2016,V-,I-,PP--,Y-2017
8. Sudha M., KumaravelA.,Analysisand measurement of wave guides using poissonmethod,IndonesianJournal of Electrical Engineering and ComputerScience,V-8,I-2,PP-546-548,Y-2017
9. AyyappanG.,NaliniC.,KumaravelA.,Variousapproachesofknowledge transferinacademicsocialnetwork,InternationalJournalofEngineering andTechnology,V-,I-,PP-2791-2794,Y-2017
10. Kaliyamurthie, K.P., Sivaraman, K., Ramesh, S. Imposing patient data privacy in wireless medical sensor networks through homomorphic cryptosystems2016, Journal of Chemical and Pharmaceutical Sciences
11. Kaliyamurthie, K.P., Balasubramanian, P.C. An approach to multi secure to historical malformed documents using integer ripple transfiguration 2016 Journal of Chemical and Pharmaceutical Sciences 9
12. A.Sangeetha,C.Nalini,"Semantic Ranking based on keywords extractions intheweb",InternationalJournalofEngineering&Technology,7(2.6) (2018)290-292
13. S.V.GayathiriDevi,C.Nalini,N.Kumar,"Anefficient software verificationusingmulti-layeredsoftwareverificationtool"International Journal of Engineering &Technology, 7(2.21)2018454-457
14. C.Nalini,ShwtambariKharabe,"A Comparative Study On Different Techniques Used For Finger – Vein Authentication", International Journal Of Pure And Applied Mathematics, Volume 116 No. 8 2017, 327-333, Issn:1314-3395
15. M.S. Vivekanandan and Dr. C. Rajabhushanam, "Enabling Privacy Protection and Content Assurance in Geo-Social Networks", International Journal of Innovative Research in Management, EngineeringandTechnology,Vol3,Issue4,pp.49-55,April2018.
16. Dr. C. Rajabhushanam, V. Karthik, and G. Vivek, "Elasticity in Cloud Computing", International Journal of Innovative Research in Management,EngineeringandTechnology,Vol3,Issue4,pp.104-111, April2018.
17. K.RangaswamyandDr.C.Rajabhushanamc,"CCN-BasedCongestion Control Mechanism In Dynamic Networks", International Journal of InnovativeResearchinManagement,zEngineeringandTechnology,Vol 3, Issue 4, pp. 117-119, April2018.
18. Kavitha, R., Nedunchelian, R., "Domain-specific Search engine optimization using healthcare ontology and a neural network backpropagation approach", 2017, Research Journal of Biotechnology, Special Issue2:157-166
19. Kavitha, G., Kavitha, R., "An analysis to improve throughput of high-powerhubsinmobileadhocnetwork",2016,JournalofChemical and Pharmaceutical Sciences, Vol-9, Issue-2:361-363
20. Kavitha,G.,Kavitha,R.,"Dippinginterferencetosupplementthroughput inMANET",2016,JournalofChemicalandPharmaceuticalSciences, Vol-9, Issue-2:357-360
21. Michael, G., Chandrasekar, A.,"Leaderelection based malicious detection and response system in MANET using mechanism design approach", Journal of Chemical and Pharmaceutical Sciences(JCPS) Volume9Issue2,April-June2016.
22. Michael,G.,Chandrasekar,A.,"Modelingofdetectionofcamouflaging worm using epidemic dynamic model and power spectral density", JournalofChemicalandPharmaceuticalSciences(JCPS)Volume9Issue 2, April - June 2016.
23. Pothumani, S., Sriram, M., Sridhar, J., Arul Selvan, G., Secure mobile agents communication on intranet,Journal of Chemical and PharmaceuticalSciences,volume9,Issue3,PgNoS32-S35,2016
24. Pothumani, S., Sriram, M., Sridhar , Various schemes for database encryption-asurvey,JournalofChemicalandPharmaceuticalSciences, volume 9, Issue 3, Pg NoS103-S106,2016
25. Pothumani, S., Sriram, M., Sridhar, A novel economic framework for cloud and grid computing, Journal of Chemical and Pharmaceutical Sciences,volume9,Issue3,PgNoS29-S31,2016
26. Priya, N., Sridhar, J., Sriram, M. "Ecommerce Transaction Security Challenges and Prevention Methods- New Approach" 2016 ,Journal of Chemical and Pharmaceutical Sciences, JCPS Volume 9 Issue 3.page no:S66-S68.
27. Priya, N.,Sridhar,J.,Sriram, M."Vehicular cloud computing security issues and solutions" Journal of Chemical and Pharmaceutical Sciences(JCPS) Volume9Issue2,April-June2016
28. Priya,N.,Sridhar,J.,Sriram,M."Mobilelargedata storagesecurityin cloudcomputingenvironment-anewapproach"JCPSVolume9Issue2. April - June2016
29. Anuradha.C, Khanna.V, "Improving network performance and security inWSNusingdecentralizedhypothesistesting"JournalofChemicaland PharmaceuticalSciences(JCPS)Volume9Issue2,April-June2016.

AUTHORS PROFILE

Muhammad Uwais Student, Department of Computer science and Engineering, Ganeshi Lal Bajaj Institute of Technology and Engineering, Greater Noida, Uttar Pradesh, India

Arpit Sharma Student, Department of Electronics and Telecommunications Engineering, K.J. Somaiya Institute of Engineering and Information Technology, Mumbai, Maharashtra, India

Akhil Kumar Student, Department of Computer science and Engineering, Ganeshi Lal Bajaj Institute of Technology and Engineering, Greater Noida, Uttar Pradesh, India

Lakshya Singh Student, Department of Computer science and Engineering, Ganeshi Lal Bajaj Institute of Technology andEngineering, GreaterNoida, Uttar Pradesh, India