ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

An Enhanced Model for Detecting and Preventing Fake Uniform Resource Locators (URLs) using Hybridized Algorithms

Isodje, Joseph Omojhevbe[1] and Onuodu, Friday Eleonu[2]

Department of Information Technology, National Open University of Nigeria, Nigeria1

Research Scholar, Department of Computer Science, University of Port Harcourt, Rivers State, Nigeria[2]

ABSTRACT: Malicious URL (Uniform Resource Locator) is a common and serious threat to cyber-security. Malicious URLs host unsolicited content (spam, phishing, drive-by downloads, etc.) and lure unsuspecting users to become victims of scams (monetary loss, theft of private information, and malware installation), and cause losses of billions of dollars every year. It is imperative to detect and act on such threats in a timely manner. In this work, a Hybridized Model for Detecting and Preventing Fake Uniform Resource Locator (URL) using Genetic Algorithm and Support Vector Machine Algorithms was developed. Furthermore, Structured System Analysis and Design Methodology was adopted in this approach, and also implemented with Hypertext Pre-processor (PHP) and MySQL as backend. The expected results of the work showed an efficiency rate of 85% in terms of Time Complexity (TC), Life Cycle Assessment (LCA), Benchmarking (B), Multi-Criteria Decision Making (MCDM), Risk Assessment (RA), Cost Benefit Analysis (CBA) and Speed (S). The assessed values for the mentioned parameters were given as 18, 12, 11, 13, 8, 13 and 10 respectively. In addition, the study could be beneficial to web application users, financial institutions and software developers.

KEYWORDS: Detecting, Fake URL, Hybridized, Malicious, Genetic and Support Vector Machine

I. INTRODUCTION

Malicious URL (Uniform Resource Locator) is a common and serious threat to cyber-security. Malicious URLs host unsolicited content (spam, phishing, drive-by downloads, etc.) and lure unsuspecting users to become victims of scams (monetary loss, theft of private information, and malware installation), and cause losses of billions of dollars every year. It is imperative to detect and act on such threats in a timely manner. Traditionally, this detection is done mostly through the usage of blacklists. However, blacklists cannot be exhaustive, and lack the ability to detect newly generated malicious URLs. To improve the generality of malicious URL detectors, machine learning techniques have been explored with increasing attention in recent years. This article aims to provide a comprehensive survey and a structural understanding of Malicious URL Detection techniques using machine learning [1]. Nowadays, as there are so many people becoming aware of using internet to perform various activities like online shopping, online bill payment, online mobile recharge, and banking transaction. Due to wide use of these, customers face various security threats like cyber-crime. There are many cybercrimes that are widely performed for example, spam, fraud, cyber-terrorism and phishing. Among these, phishing is a new cyber-crime and very popular nowadays. Phishing is a fraud attempt, which is performed to obtain sensitive information of the user. Phishers design websites which look the same as any legitimate site and spoofs users into obtaining their private information such as username, password, banking details etc. for miscellaneous reasons. Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication medium. Phishing attack can be implemented in various forms like Email phishing, website phishing, spear phishing, whaling, tab-napping, evil twin phishing etc. To avoid these phishing attacks, various anti-phishing solutions should be used. There are various anti-phishing solutions such as blacklist, heuristic, visual similarity, and

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

machine learning etc. The blacklist method is the most commonly used approach in which a list of phishing URLs is stored in a database and then if the URL is found in the database, it is identified as a phishing URL and gives a warning to the user otherwise it is legitimate. This approach is easy and faster to implement as it checks to see if URLs are in the database or not. But limitations like a small change in the URL are sufficient to bypass the list-based technique so frequent update of the list is necessary to counter new attacks. The heuristic-based method is the extension of the blacklist and is able to detect new attacks as it uses features extracted from phishing sites to detect phishing attacks. But its limitation is that it cannot detect all new attacks and is easy to bypass once attackers know the algorithm or features used. In addition, this has poor detection because sites may or may not have common features. The visual-similarity method deceives users by extracting images of legitimate sites. The limitation of this method is that image comparison takes more time as well as more space to store the image. It also produces high false negative rate and fails to detect when visual appearance slightly changes. In contrast, the machine learning method works efficiently in large dataset. It also removes the drawbacks of existing approaches and is able to detect zero-day attack. Machine Learning based classifiers are efficient classifiers which achieve accuracies of more than 99%. Performance depends on size of training data, feature set, and type of classifier. The limitation of this method is that it fails to detect when attackers use compromised domains for hosting their site. Many researches have been performed in this area of phishing detection.

II. RELATED WORK

Sherif [2] looked at the Curious Case of Machine Learning in Malware Detection. The work argued that detecting malware attacks in the wild is a unique challenge for machine learning techniques. Given the current trend in malware development and the increase of unconventional malware attacks, we expect that dynamic malware analysis is the future for antimalware detection and prevention systems. However, the work failed to interface with an artificial intelligence tool known as Long Short-Term Memory (LSTM).

Domhnall [3] researched on the effects of traditional anti-virus labels on malware detection using dynamic runtime opcodes. The work developed a new parsed runtime trace data set of over 100 000 labeled samples, which will address these shortcomings, and we offer the data set itself for use by the wider research community. This data set underpins the examination of the run traces using classifiers on count-based and sequence-based data. However, the work could not further discuss individual advanced techniques for training large-scale deep learning models and recently developed method of generative models

Omoyiola [4] researched on the Overview of Biometric and Facial Recognition Technique. According to the work, security has become a major issue globally and in order to manage the security challenges and reduce the security risks in the world, biometric systems such as face detection and recognition systems have been built. These systems are capable of providing biometric security, crime prevention and video surveillance services because of their inbuilt verification and identification capabilities. However, there was no adequate comparative analysis between the textual disclosure model and other existing biometric models.

Jashanpreet [5] looked at Face detection and Recognition: A Review: Face Detection is one of the types of biometric technique which refers to the detection of face automatically by computerized systems by taking a look at face. It is a popular feature used in biometrics, digital cameras and social tagging. Face detection and recognition has gained more research attentions in last few years. However, there was no adequate comparative analysis of the system with other existing ones.

Smriti [6] looked at Detection, Segmentation and recognition of face and its features using neural network. Summary of findings from the work showed that the rampant advent of biometric analysis systems, which may be full body scanners, or iris detection and recognition systems and the finger print recognition systems, and surveillance systems deployed for safety and security purposes have contributed to inclination towards same. Advances has been made with frontal view, lateral view of the face or using facial expressions such as anger, happiness and gloominess, still images and video image to be used for detection and recognition. However, there was no adequate comparative analysis of the system with other existing ones

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

Anitta [7] looked at the World of Malware: An Overview. The work presented an overview of the world of malware with the intent of providing the underlying information for the intended study into developing malware detection approaches. However, there were quite some percentage error levels in the developed model for malware detection.

Davide [8] researched on "Towards Adversarial Malware Detection": Lessons learned from PDF-based Attacks. The work focused on malware embedded in PDF files as a representative case of such an arms race. They started by providing a comprehensive taxonomy of the different approaches used to generate PDF malware, and of the corresponding learning-based detection systems. However, there were quite some percentage error levels in the developed model for malware detection.

Ziyun et al [9] researched on Automatically Engineering Features for Malware Detection by Mining the Security Literature. The work described techniques for mining documents written in natural language (e.g. scientific papers) and for representing and querying the knowledge about malware in a way that mirrors the human feature engineering process. Specifically, they first identified abstract behaviours that are associated with malware, and then they map the behaviors to concrete features that can be tested experimentally. However, the work failed to show improvement measures on the already achieved 2.2% error rate on average

Ryusei [10] researched on Investigation on Sharing Signatures of Suspected Malware Files using Blockchain Technology. The work developed a system for sharing the signatures of suspected malware files using blockchain technology. The developed system can share the signatures of suspected files between users, allowing them to rapidly respond to increasing malware threats. Furthermore, it improves the accuracy of detection and removal of malware by utilizing signatures recorded by the blockchain. However, the work was vulnerable to security threats since it was implemented with scripting languages instead of an enhanced biometric technique.

Muni [11] looked at new ways to fight Malware. The work discusses latest trends and types of malwares, malware attacks techniques, method of propagation and detection additionally, it includes recommendations on various solutions expressed to combat malware attacks. However, there was no adequate comparative analysis of the system with other existing ones.

Daniel [12] researched on a survey of deep learning method for cyber-security. The work described a literature review of deep learning (DL) methods for cyber-security applications. A short tutorial-style description of each DL method is provided, including deep auto-encoders, restricted Boltzmann machines, recurrent neural networks, generative adversarial networks, and several others. However, the performance evaluation of the work showed some deficiency in lifecycle assessment (LCA) and speed.

Abdullah [13] looked at "Detection and Prevention of Mobile Malware". The work discussed techniques to effectively detect and prevent mobile malwares and proposed an improvement towards current techniques which gives better mobile malware detection and prevention. However, the work failed to show improvement measures on the already achieved error rate on averages.

Ida [14] looked at identification of population growth and distribution based on urban zone functions. The work analysed zones with the highest population in Indonesia. The result of the work showed that the zones with the highest population growth and accommodate the highest population increase. However, they could not illustrate any population model-type used in the work.

Markus [15] looked at income and population growth of malware. The work estimated the effects on population growth of shocks to national income that are plausibly exogenous and unlikely to be driven by technological change. The result of the work showed that there is significant relationship between oil induced income growth and population growth. However, they could not illustrate any population model type used in the work.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

David [16] looked at malware population dynamics in India and Implications. The work discussed theoretical and empirical literatures on the effect of demographics on labour supply, savings, and economic growth in India. The result of the work showed that failure to take advantage of the opportunities inherent in demographic change can lead to economic stagnation. However, they could not practically implement the reviewed study.

Heddy et al [17] looked at fake URL Detection using Cloud Computing. The work presented the conception of fake url and its causes. The value of data is incredible, so it should not be leaked or mishandled. Furthermore, the work adopted Rapid Application Development Methodology (RAD). However, a major drawback from the work showed that they could not further prevent the detected fake url.

III. MALWARE AS A VECTOR OF FAKE URL

Malware, short for malicious software is a program code that is hostile and often used to corrupt or misuse a system. Introducing malware into a computer network environment has different effects depending on the design intent of the malware and the network layout. Malware detection and prevention systems are bypassed by malicious files in computer systems as malware become more complex and larger in numbers. The internet and the worldwide web have provided great advancement in how society communicates and the face of business. This has also given rise to the number of propagation avenues available to malware. Introduction of malicious code in one node can create a chain reaction across all the nodes accessible through the network the node seats on as seen in the popular WanaCryptor ransomware. With organizations and countries heavily relying on network technologies, the commercial value of computer networks implies that exploitation of the vulnerability of the business networks can cripple its operations and access to intellectual property and personal information can be acquired by cyber criminals. This creates a commercial opportunity for malware and anti-malware ventures and therefore it is no surprise that it is estimated that cybercrime is expected to rise significantly.

IV. MATERIALS AND METHODS

A. Methodology

The Methodology for the Proposed System Design is Structured System Analysis and Design Methodology (SSADM). Structured Systems Analysis and Design Methodology is a systems approach to the analysis and design of information systems. SSADM was produced for the UK government office concerned with the use of technology in government, from 1980 onwards. System design methods are a discipline within the software development industry which seeks to provide a framework for activity and the capture, storage, transformation and dissemination of information so as to enable the economic development of computer systems that are fit for purpose.

B. Analysis of the Existing System

A major system for fake url detection was developed by Heddy et al which was further illustrated in the work captioned “fake url detection system”. The System developed by them studied the techniques for detecting leakage of objects or records. Specifically, they also studied the following scenario: After giving a set of data to agents, the distributor discovers some of those data in an outside or unauthorized place. For e.g. the data may be found on a website, or may be obtained through a legal discovery process. At this point, the distributor can assess the possibility that the leaked data came from one or more agents, as opposed to having been independently gathered by other means.

Secondly, the developed System enabled the distribution of algorithms to guilty agents, and also considered the option of adding “fake” objects into the distributed set of data given by the distributor as shown in figure 1. In recent years where more services and resources are outsourced, there is an increasing need for maintaining solutions for security. Over the last few years, this problem has been on the increase as various companies or infrastructure may expect their data to remain confidential.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

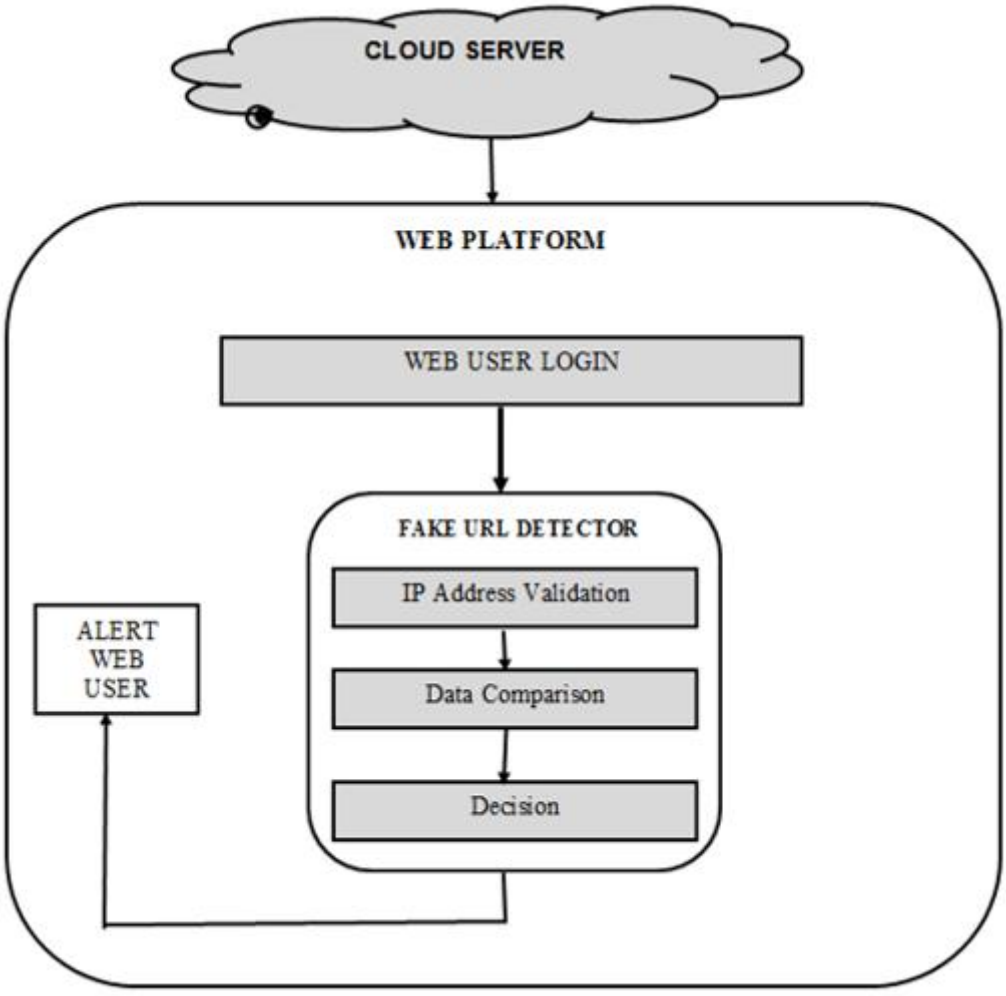

Fig. 1.Existing System Architecture of Fake URL Detector
(**Source:** [17])

Heddy et al also updated the system for identifying data leaks from any agency. The updated system was designed to analyse pop-ups requests by fraudulent online distributors and agents. Thus, every potential data distributor and agent of a website must be granted administrative access to distribute data packets on the said website. In addition, the system has customized software for file sharing and has its own file format. While sharing the file with employees within the organization it will request for admin permission; if admin grants the permission for sharing, the employee will share the file. Login page for all users will be shown, such as agent and distributor. Once users login according to their login details (i.e. username and password), the user will be identified i.e. whether the user is a Distributor or an Agent, once the potential users - agents and distributors are identified; the respective JavaScript page will be shown where the distributors can send files to agents as well as monitor the file sharing among the agents. During this process, the system monitors the behaviour of the agents in order to identify any agent with fraudulent motives to leak data.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

1) Explanation of the Existing System Components

The following components of the Existing System Architecture are:

- **The Cloud Server:**This component is a logical server that is built, hosted and delivered through a cloud computing platform over the internet. Furthermore, the cloud server possesses and exhibits similar capabilities and functionality to a typical server, but is accessed remotely from a cloud service provider.
- **The Web Platform:**According to Heddy et al; the web platforms belong to an organization, and is a collection of technologies developed as open standards by the World Wide Web consortium and other standardization bodies such as the web, hypertext application technology working group. The web platform is a channel of information storage and distribution for the organization.
- **The Detection System:** Heddy et al also referred to this component as one of the most important in the system. This is because; it is a device or software application that monitors a network or systems for malicious activity or policy violations. Any suspected malicious activity or violation will be typically reported to an administration. Furthermore, the detection system sub-components include the web data distributor, the data allocation system, the agents, the leakage detection and probability calculation processes.

2) Disadvantages of the Existing System

The following disadvantages of the Existing System are:

- inability to prevent the detected fake url
- inability of its deployment to social media consumption on Smartphones of users.

C. Analysis of the Proposed System

A major objective of this study is to create awareness on fake url detection and prevention for web users. In realizing the mentioned objective, the study focused on improving the existing system by proposing an enhanced model for fake url detection and prevention. Secondly, the new improvements of the existing system will also support its deployment to mobile web application usage on Smartphones. Another uniqueness of the Proposed System includes the awareness on Data Security. This is because; not every web user takes cyber security seriously. It's not uncommon for people to use the web and never look beyond the default settings. In the same way, they'll buy a mobile device, computer, or some other equipment to access those sites and assume that it's set up in a way that best protects them. Often, the default settings provide the greatest ease of use but are also the least secure.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

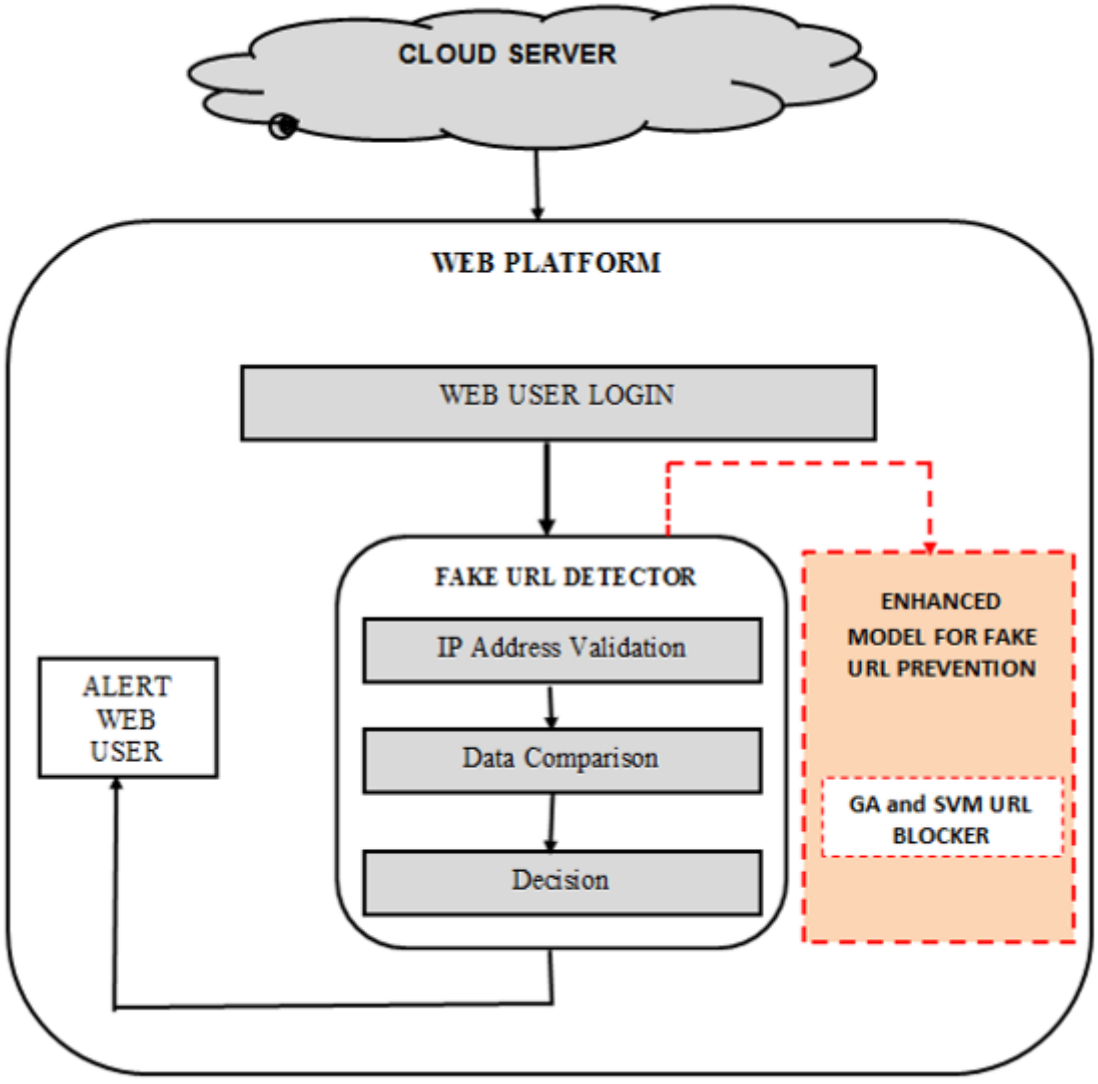

Fig. 2.Proposed System Architecture of an Enhanced Fake URL Detection and Prevention System

1) Explanation of the Proposed System Components

The following component(s) of the Proposed System Architecture is:

- **Enhanced Model for Fake URL Prevention:**This component utilizes Genetic and Support Vector Machine Algorithms in preventing any detected fake url from leaking confidential data.

2) Advantages of the Proposed System Components

The following advantages of the Proposed System are:

- **employee confidence when working with confidential data online:**When employees feel confident about their interactions with data that must follow security protocols, the less likely they are to cause an incident. Human error is after all the leading cause of breaches and attacks.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

- **protection of organizational assets information online:**The Proposed System provides a unique fake url detector and prevention that will protect organizational data online.
- **awareness on malicious and inadvertent URLs on websites:**A major benefit of the proposed system is the awareness on malicious and inadvertent url to website users. This will also enable users to carry out investigative measures on any suspicious url that will perpetuate information leakage.
- **compatibility of mobile web applications:**The proposed system will also support its deployment to mobile web application usage on Smartphones.

3) Existing System Algorithm

STEP ONE:
START
STEP TWO:
DECLARE VARIABLES
WUL, UN, PW, ML, SD, URLD, QS
WHERE
WUL = WEB USER LOGIN
UN = USERNAME
PW = PASSWORD
ML = MALICIOUS LINK
SD = SUBMIT DATA
URLD = UNIFORM RESOURCE LOCATOR DETECTOR
QS = QUIT SYSTEM
STEP THREE
INITIALIZE WUL
STEP FOUR:
WUL = UN + PW
STEP FIVE:
ACTIVATE MALICIOUS LINK
STEP SIX:
SD
STEP SEVEN:
ACTIVATE URLD
STEP EIGHT:
QUIT SYSTEM

4) Proposed System Algorithm (Genetic + Support Vector Machine)

STEP ONE:
START
STEP TWO:
DECLARE VARIABLES
WUL, UN, PW, ML, SD, URLD, URLDP, QS
WHERE
WUL = WEB USER LOGIN
UN = USERNAME
PW = PASSWORD
ML = MALICIOUS LINK

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

SD = SUBMIT DATA
URLD = UNIFORM RESOURCE LOCATOR DETECTOR
URLDP = UNIFORM RESOURCE LOCATOR DETECTOR AND PREVENTION
GA = GENETIC ALGORITHM
SVM = SUPPORT VECTOR MACHINE
QS = QUIT SYSTEM

STEP THREE
INITIALIZE WUL
STEP FOUR:
WUL = UN + PW
STEP FIVE:
ACTIVATE MALICIOUS LINK
STEP SIX:
SD
STEP SEVEN:
ACTIVATE URLD
STEP EIGHT:
IMPLEMENT GA + SVM FOR URLDP
STEP NINE:
INTIAL_POPU <- NULL
STEP TEN:
X <- 1
STEP ELEVEN:
REPEAT {
STEP TWELVE:
CRM <- RUNIF (2,1,10)
STEP THIRTEEN:
CRM <- AS.INTEGER (CRM)
STEP FOURTEEN:
INTIAL_POPU <- RBIND (INTIAL_POPU,CRM)
STEP FIFTEEN:
X = X+1
STEP SIXTEEN:
IF (X == 7){
STEP SEVENTEEN:
QUIT SYSTEM

V. RESULTS AND DISCUSSION

A. Hardware Requirements

The following hardware components were required for the proposed system design:

- Processor: at least 600-MHZ Pentium III-class processor recommended.
- Hard disk: at least 1GB of available space required on system drive, 3.3 GB of available space required on installation drive.
- Display super VGA (1024 x 768) or higher resolution display with 256 colours
- RAM: Minimum requirement of 512 MB
- CD-ROM Drive
- USB port enabled

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

- Sound card and speakers (optional)

B. Software Requirements

The following software components were required for the proposed system design:

- Operating system: windows vista, Microsoft windows 7 and 8
- IDEs and Browsers: notepad++/Sublime text, Firefox/Chrome, Opera or UC browser
- JavaScript, Hypertext Pre-processor and MySQL
- Internet Service Provider (ISP)

C. Outputs and Discussion

The Proposed System is a Web Application that is backed up by a Local Host Server. Hence, we implemented the frontend of the system with Xampp Server as illustrated in figures 3 and figure 4.

1) Application Frontend Procedures:

- Start
- Launch XAMPP
- Launch Notepad++
- Enter source codes for Application Frontend, Run program on Mozilla Firefox or Google Chrome browser

2) Step One: (Setting up Xampp Server Installation):

In order to install the Xampp Server, the user of the system must download the Xampp executable file, before running the installation as an administrator. Once the download is done, the user double clicks on the executable file to commence the installation. A Xampp executable file enables the installation of a local host server on the system. It ranges from 32 to 64 bits.

Fig. 3. Xampp Server Welcome Screen

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

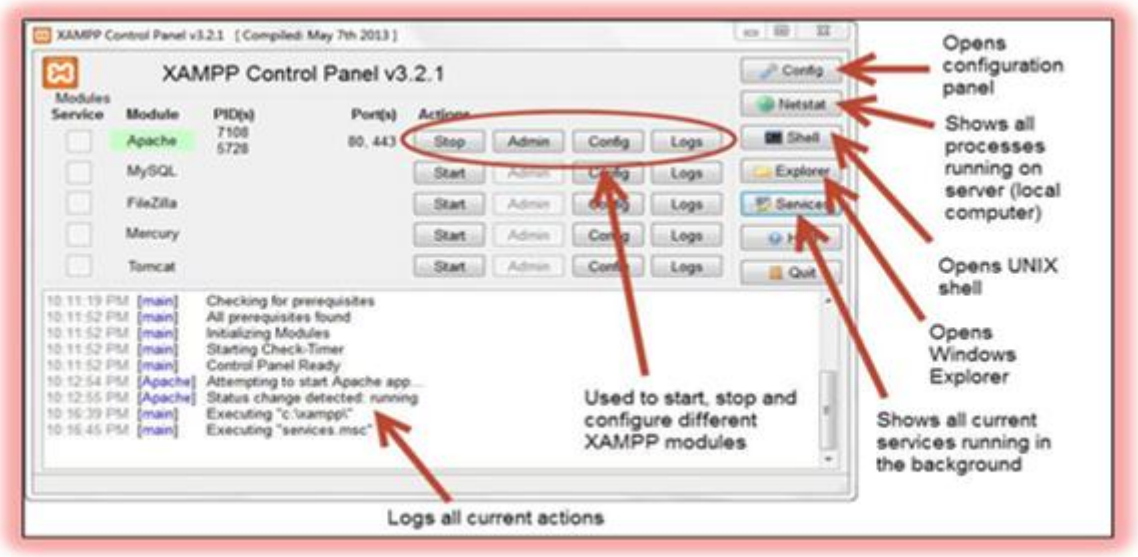

Fig. 4. Xampp Server Control Panel

Fig. 5. Fake URL Detection: Firefox Browser Page

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

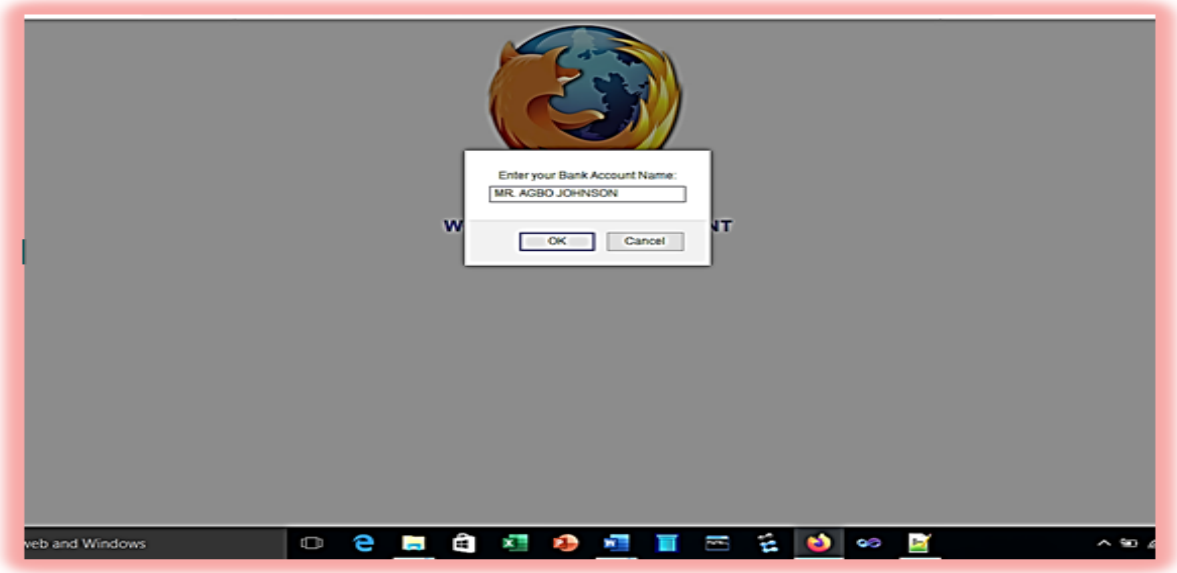

Fig. 6. Fake URL Detection: Financial Information Input Page

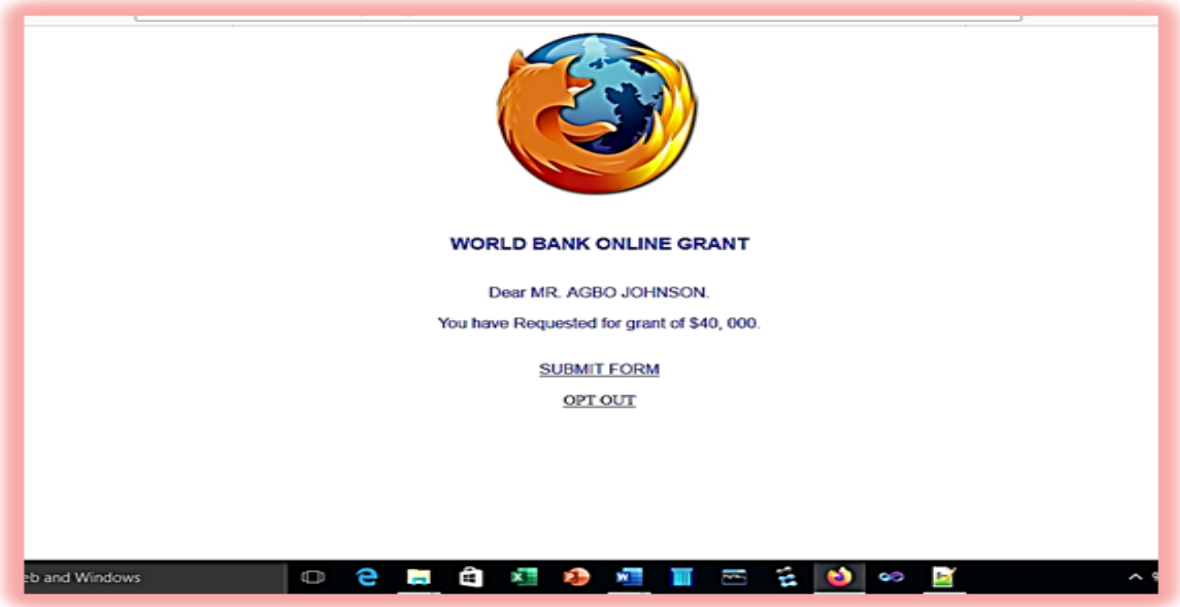

Fig. 7. Fake URL Detection: Form Input Summary

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

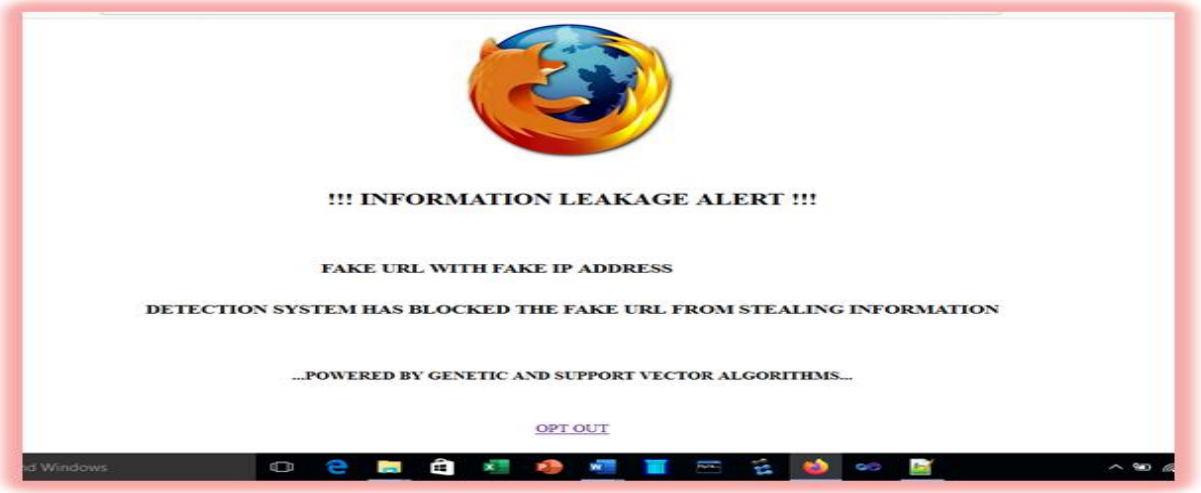

Fig. 8. Fake URL Detection: Fake URL Alert

Figure 5 shows the welcome screen of a Firefox web browser in assumption of a user browsing the internet. On the browser environment, a fake url link is displayed to the user to click and input vital account information such as account name, account number, atm pin, etc. (figure 6). On submitting the inputted data, the system blocks the fake url link from submitting the confidential information to guilty agents or hackers (figure 7). Information leakage through fake URLs can be described as the process of leaking sensitive and confidential information intentionally or unintentionally to unauthorized parties. It can be private or public information. The root cause of data leakage can be caused by malicious and non-malicious insider attacks. This is because; a non-malicious insider could hardly be expected based on their everyday action. In other words, they are not suspected to be harmful or a source of threat to an organization. The importance of data leakage can be verified in the area of data security, especially if it is caused by an insider, which has seriously threatened security and personal privacy. However, there are some traditional technologies for preventing data leakages. These technologies are mainly based on domain that is segmented into security sub-domains according to data protection requirements, and limit the data flow between security domains through firewall, encryption and terminal control.

D. Performance Evaluation

TABLE I
COMPARATIVE ANALYSIS OF THE EXISTING AND PROPOSED SYSTEMS

SN	HEDDY et al (2019)	%	%	PROPOSED SYSTEM (2019)
1.	Time Complexity (TC)	10	18	Time Complexity (TC)
2.	Life-Cycle Assessment (LCA)	5	12	Life-Cycle Assessment (LCA)
3.	Benchmarking (B)	6	11	Benchmarking (B)
4.	Multi-Criteria Decision Making (MCDM)	11	13	Multi-Criteria Decision Making (MCDM)
5.	Risk Assessment (RA)	5	8	Risk Assessment (RA)
6.	Cost Benefit Analysis (CBA)	12	13	Cost Benefit Analysis (CBA)
7.	Speed	7	10	Speed
TOTAL (%)		**56**	**85**	**TOTAL (%)**

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

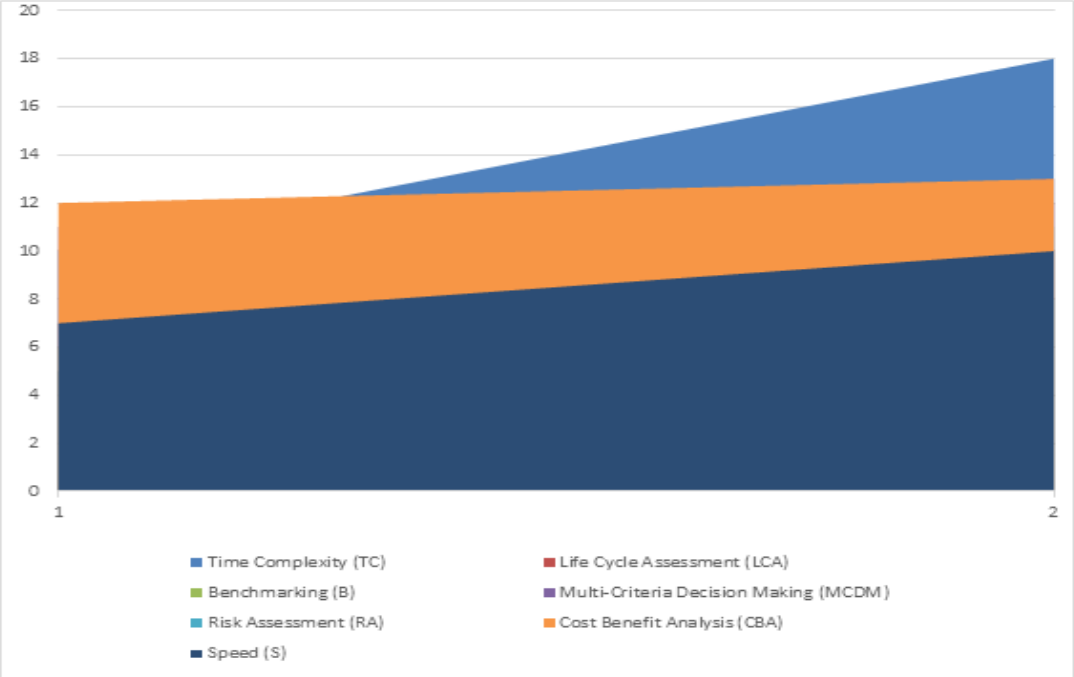

Fig. 9.Performance Evaluation Chart

VI. CONCLUSION

In this study, we have developed an Enhanced Model for Detecting and Preventing Fake Uniform Resource Locators (URLs) using Hybridized Algorithms. This is because, Situational Awareness on Information Leakage via fake URL is very important. This is because, not every web user takes data security seriously. A major challenge faced by most web users is the problem of fake urls. Two major url problems include Malicious information link and Inadvertent url link. Most guilty agents that leak information via fake url always utilize the ignorance of web users that are desperate to release confidential datasets to unknown sources.

REFERENCES

[1] Doyen L., K. Limbest, G. Holmani, Data Leakage, Detection and Prevention of Data Leakages in Web Servers, *International Journal of Computer Science and Information Technology (IJCSIT), 5(2) 2556 – 2558, 2019*

[2] Sheif U., The curious case of machine learning in malware detection, *https://arxiv:1905.075 73v1, 2019*

[3] Domhall H., The Effects of traditional anti-virus labels on Malware Detection using dynamic Runtime Opcodes, *IEEE Access, 10.1109/ACCESS.2017.2749538, 2017*

[4] Omoyiola N., Overview of Biometric and Facial Recognition Techniques, *IOSR Journal of Computer Engineering (IOSR-JCE), 20(4), 1 – 5, 2018*

[5] Jashanpreet W., Face Detection and Recognition; A Review, *6th International Conference on Advancement in Engineering and Technology (ICAET-2018), 2018*

[6] Smriti M., Detection, Segmentation and Recognition of face and its features using Neural Network *https://arxiv.org/ftp/arxiv/papers/1701/1701.08259.pdf, 2018*

[7] Anitta C., the world of Malware: An Overview, *IEEE, 6th International Conference on Future Internet of Things and Cloud, 2018*

[8] Davide B., Towards Adversarial Malware Detection Lessons Learned from PDF based attacks *http://arxivi.1181.008300v2.pdf, 2019*

[9] Ziyun O., B. Ned, S. Priyante, Automatically Engineering Features for Malware Detection by Mining the Security Literature, *https://dx.doi.org/10.1145/2976749.2978304, 2016*

[10] Ryusei M., Investigation on sharing signatures of suspected malware files using blockchain technology, *proceedings of the international multi-conference of Engineers and Computer Scientists IMECS 2019, March 13 – 15, 2019 Hong Kong*

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

[11] Muni J., New ways to fight malware, *International Journal of Scientific and Technology Research (IJSTR), 6(6), 318 – 323, 2017*
[12] Daniel Z., A Survey of Deep Learning method for cyber-security, *MDPI, Information, doi:10.3390/info10040122, 2019*
[13] Abdullah M., Detection and Prevention of Mobile Malware, *International Journal of Scientific and Research Publications, 5(5), 1 – 3, 2015*
[14] Ida V., Identification of Population growth and distribution based on urban zone functions, an International Article published at sustainability 2018, 10, 930; *doi: 10.3390/su10040930 https://www.mdpi.com/journal/sustainability, 2018*
[15] Markus A., Population projection by age, sex and educational attainment in rural and urban regions of 35 Provinces of India, 2011 – 2101; *International Institute for Applied Systems, Analysis Schlossplatz 1, A-2361 Laxenburg, Austria, www.iiasa.ac.at, 2013*
[16] David C., Biometrics implementations and the implications for strategy in security and privacy management, *International Journal on private policy Management in Nigeria and beyond, Vol. 1 344-780, 2011*
[17] Heddy I., G. Craig, F. Meffilin, Fake URL Using Cloud Computing, *International Research Journal of Engineering of Engineering Technology (IRJET), 6(3), 6939 – 6945, 2019*