IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

URL Indemnity and Bookmark Enshroud using AES Algorithm

Rama Rajesh R[1], Zennera Fathima K A[2], Nivedhitha V[3], Dheeptha M[4]
Assistant Professor, Department of Information Technology[1]
Students, B.Tech, Final Year, Department of Information Technology[2,3,4]
Anjalai Ammal Mahalingam Engineering College, Thiruvarur, India

Abstract: *The goal is to get access to the computer or the information it holds, as well as to collect personal information in various methods. Because the security of electronic data is such a critical problem, the commercial and governmental sectors have adopted a variety of approaches and procedures to secure sensitive data from hackers. As a result, we made an attempt to suggest an enhanced way for securing our data from threats through the use of encryption and decryption. The system's recommended strategy is to use encryption and decryption methods to safeguard URLs and bookmarks. The Advanced Encryption Standard (AES) technique is used to encode and decode URLs in this project. By adding a password to the link, this tool encrypts and decrypts URLs. When visiting an encrypted URL, the user will be prompted for a password. If the password is correct, this software will link viewers to the hidden web page. Otherwise, you'll get an error notice. Each encrypted URL is fully stored in the link generated by this software. Knocking sequence is used to hide bookmarks; only users who know the correct order of the series may access the bookmark*

Keywords: Decryption, URL, AES

I. INTRODUCTION

The goal of this technique is to protect and secure our data and information against cyber-attacks. Cybercriminals, pirates, non-malicious (white-capped) attackers, and hacktivists are all capable of carrying out attacks. The goal is to get access to the computer or the information it holds, as well as to collect personal information in various methods. Because the security of electronic data is such a critical problem, the commercial and governmental sectors have adopted a variety of approaches and procedures to secure sensitive data from hackers. As a result, we've made an attempt to suggest an enhanced way for securing our data from threats through the use of encryption and decryption. The system's recommended strategy is to use encryption and decryption methods to safeguard URLs and bookmarks. The Advanced Encryption Standard (AES) technique is used to encode and decode URLs in this project. By adding a password to the link, this tool encrypts and decrypts URLs. When visiting an encrypted URL, the user will be prompted for a password. If the password is correct, this software will link viewers to the hidden web page. Otherwise, you'll get an error notice. Each encrypted URL is fully stored in the link generated by this software. Knocking sequence is used to hide bookmarks; only users who know the correct order of the series may access the bookmark.

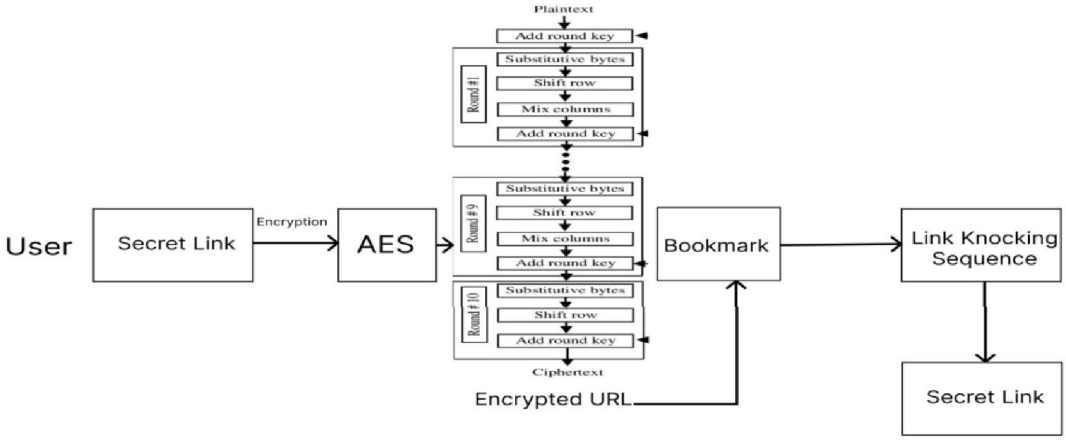
II. SYSTEM ARCHITECTURE

Encryption: The three primary components of the encryption process are data, encryption engine, and key management. An encryption algorithm is used to encrypt the data to be protected. The type of algorithm to be utilised and the variable to be used as a key are both decided by the sender. Then, only a valid key shared by the sender may decode this encrypted data.

AES: The security provided by AES algorithm's security in comparison to the other algorithms has to be rated on its capacity to survive assaults when compared to the other cyphers. The competition's most significant criteria has to be the strength of the security system. This method provides the most versatility, appropriateness for hardware or software implementation, and overall simplicity when it comes to AES implementation. This system

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

encrypts passwords with AES in GCM mode, Base64 encryption, and a random salt for safe key generation. Encryption, decryption, and key elaboration have all been completed.



Link knocking sequence: A method called Link Knocking is used to do this. A user who wants to access a hidden link must know how to click on the correct bookmark in the correct "click sequence". If he does, he will be redirected to the hidden page and if not he will be redirected to the bait bookmark.

Boomark: Hidden bookmarks seem just like regular bookmarks, with the difference that clicking them in the correct order will reveal a hidden link. To access the secret link, first click the disguised bookmark, then the decrypt bookmark. All disguised bookmarks may be decrypted with the same decrypt bookmark

III. LIST OF MODULE

Inscribe and Elucidation: In this module, we used Inscribe and Elucidation the other name of encryption and decryption techniques to create a system for securely safeguarding URLs and concealing bookmarks. The URLs in this project are encrypted and decrypted using the Advanced Encryption Standard (AES) algorithm. Encryption is the process of encoding data in cryptography. This procedure turns plaintext, or the original representation of the data, into ciphertext, or an alternate representation of the data. Once the user has picked the file, the javascript will begin to encrypt it, and the encrypted file will be ready for download.

Link knocking: It is a security technique used to protect network services from unauthorized access. It involves a specific sequence of connection attempts, often used to predetermined ports on a system. By sending these connection attempts to the correct ports in the right sequence, a previously closed port will open .The target system's firewall monitors incoming connection attempts. It is configured to watch for the correct knocking sequence. If the correct sequence of connection attempts is detected, the firewall dynamically opens the desired port or ports for a specified duration or until the connection is closed.

Bookmark Hiding: Bookmark hiding is the practice of hiding a secret message inside of (or even on top of) something that is needed to protect. Or hiding a secret message or script inside of a Word or Excel document. Hiding bookmarks is a technique that allows users to hide their bookmarks using features that are already built into every web browser. A method called Port Knocking is used to do this. A user who wants to access a hidden link must know how to click on the correct bookmark in the correct "click sequence". If he does, he will be redirected to the hidden page and if notit will be redirected to the bait bookmark.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

IV. SCREEN SHOTS

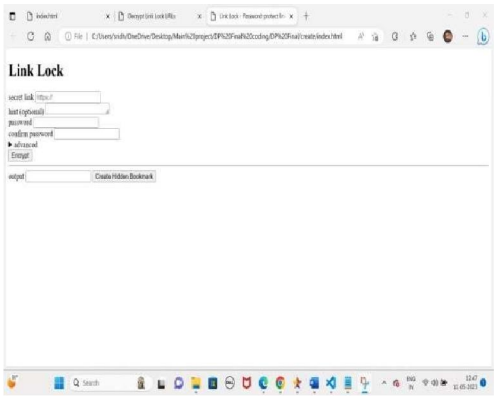


Fig .1 Link Encryption Page

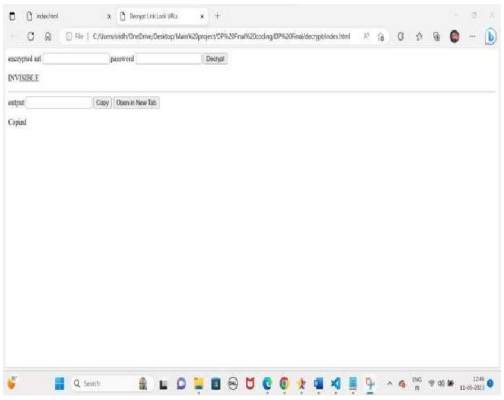


Fig .2 Link Decryption Page

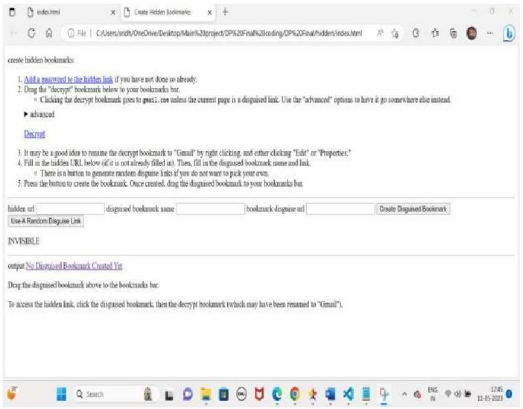


Fig .3 Bookmark Hiding Page

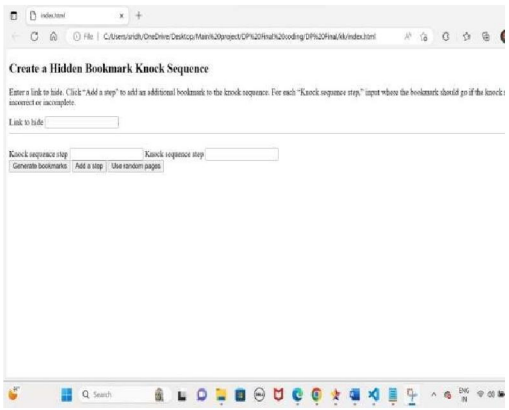


Fig.4 Link Sequence Hiding Page

V. FUTURE ENHANCEMENT

Future work will be developing this project to its full potential by improving it to work efficiently on mobile devices and browsers, for now the project is tested and gave satisfactory results on desktop Firefox and Chrome.

VI. CONCLUSION

The media pays a lot of attention to web apps and related security breaches. Every day, new dangers are found, thus developing a web application to protect your data from them is critical. The majority of security threats target system weaknesses. phishing, on the other hand, targets the vulnerabilities of human end users. As a result, it is critical that we safeguard our data from hackers. To protect the data in this work, we used the AES method and bookmark concealing with the knocking sequence to develop a phishing detection system. The suggested solution attempts to improve user pleasure by allowing them to safely share links and favourites. The achieved result demonstrates the desired application of the AES-256 bit encryption technique for data security.

REFERENCES

[1] MuhammetBaykara , ZahitZiyaGürel, ” Detection of phishing attacks”, International Symposium on Digital Forensic and Security (ISDFS), 2018.

[2] Malaikarastogi. Anmolchhetri , Divyanushkumarsingh, “Survey on detection and prevention of phishing websites using machine learning”, 2021 International Conference On Advanced Computing And Innovative Technologies In Engineering (ICACITE),2021

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

[3] Fei Shao, Zinan Chang, Yi Zhang, "AES Encryption Algorithm Based on the High Performance Computing of GPU," Second International Conference on Communication Software and Networks, 2010.
[4] M. Babagoli, M. P. Aghababa, and V. Solouk, "Heuristic nonlinear regression strategy for detecting phishing websites," Soft Computing, vol. 23, no. 12, pp. 4315–4327, 2018.
[5] E. Buber, B. Diri, and O. K. Sahingoz, "NLP Based Phishing Attack Detection from URLs," Advances in Intelligent Systems and Computing Intelligent Systems Design and Applications, pp. 608–618, 2018.
[6] R. S. Rao, T. Vaishnavi, and A. R. Pais, "CatchPhish: detection ofphishing websites by inspecting URLs," Journal of Ambient Intelligence and Humanized Computing, vol. 11, no. 2, pp. 813–825, Oct. 2019.
[7] Thomas T., P. Vijayaraghavan A., Emmanuel S, "Machine Learning and Cybersecurity. In: Machine Learning Approaches in Cyber Security Analytics," Springer, Singapore, 2020.
[8] Zhu, Erzhou, Yuyang Chen, Chengcheng Ye, Xuejun Li, and Feng Liu, "OFS-NN: An Effective Phishing Websites Detection Model Based on Optimal Feature Selection and Neural Network," IEEE Access, 2019.
[9] R. S. Rao, T. Vaishnavi, and A. R. Pais, "CatchPhish: detection of phishing websites by inspecting URLs," Journal of Ambient Intelligence and Humanized Computing, vol. 11, no. 2, pp. 813–825, Oct. 2019.
[10] M. Babagoli, M. P. Aghababa, and V. Solouk, "Heuristic nonlinear regression strategy for detecting phishing websites," Soft Computing, vol. 23, no. 12, pp. 4315–4327, 2018.

BIOGRAPHY

Mr. R. Rama Rajesh M.E.,MBA.,Assistant Professor, Department of Information Technology, 14 Years of Experience , AnjalaiAmmalMahalingam Engineering College, Kovilvenni, Thiruvarur-614 403

Ms.K.A.ZenneraFathima , Pursuing B.Tech – Information Technology (IT) Final Year in Anjalai AmmalMahalingam Engineering College, Kovilvenni, Thiruvarur-614 403

Ms.M.Dheeptha, Pursuing B.Tech – Information Technology (IT) Final Year in AnjalaiAmmal Mahalingam Engineering College, Kovilvenni, Thiruvarur-614 403

Ms.V.Nivedhitha, Pursuing B.Tech – Information Technology (IT) Final Year in AnjalaiAmmal Mahalingam Engineering College,Kovilvenni,Thiruvarur-614 403