iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VIII **Month of publication:** Aug 2023

DOI: https://doi.org/10.22214/ijraset.2023.54999

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

Enhancing Data Security and Predictive URL Analysis: A Comprehensive Approach to Preventing Data Breaches

Dr. J. Sreerambabu[1], Mr. D. Rajkumar[2], Mr. N. Santhosh[3], Mr. S. Vijay Krishnan[5]
[1]Head of the Department, [2, 3]Assistant Professor, [4] PG Scholar

Abstract: ***There has never been a time in history when starting and running a profitable business has been more difficult due to the upward trending rising trend in data breaches. Data breaches can have an immediate impact on hundreds of millions or conceivably billions of individualities in the data-driven world of the moment. Data breaches have grown in scope along with digital metamorphosis as attackers take advantage of our every data. Various measures are taken by many companies to control data breaches in order to prevent them. A business or firm may employ techniques like data encryption, human error, data backup and recovery, and data security software. In the case of middle-level and low-level organizations suffering the most cyber-attacks, Many businesses are successful in defending their data from intruders, typically large multinational corporations which engage a specialist and safeguard their own data. Therefore, we can employ some of the standard data breach prevention strategies in our project to ensure that the domain can receive its user data without any consequences. Our project proposes to improve data security where user data must reach their domain without any disruption.***
Keywords: Data transfer, Encryption, Decryption, Logistic regression, Rigid regression.

I. INTRODUCTION

A general study on encrypting and how to prevent data breaches also predicts the URL whether good or bad is conducted how. There are many different ways to prevent data breaches some of them are accessing antimalware agencies, preventing social engineering, and software updates regularly, which were ineffective in most cases so we implement random encryption methods and predict the URL good or bad before access it and provide distribution key for prospective users will enhance the security purpose and prevent the data breaches. The most pivotal concern in the moment's computer world is securing the data from the interferers there are numerous systems and styles are there but still stoner's opinion is unsure. In this project, we provide an appropriate proposed system that outlines how we can prevent the data from beginning to endpoint in order to win the users, For those first domain registration purposes, the administrator will next establish a virtual box for domain users to store data that is only accessible to the IDCP team. In order to prevent malware attacks, users initially registered their purposes along with URLs and files. A team will then determine if the URL is good or malicious. If the file is sound, the next step is to encrypt the data so that only trustworthy people who input the right access ID that the admin gave can view the data. Finally, the domain receives the encrypted data, and the domain user also receives the access key to decrypt the data. This will increase security and increase trustworthiness.

II. PROPOSED METHODOLOGY

Theft or unauthorized use of data leads to significant losses for prospective businesses. Less common preventive measures, such as anti-malware agencies and file backups, are ineffective against intruders, so businesses began to hash their data, which was effective but required a lot of server storage in order to prevent initially predicting the user data, whether good or bad for the prospective firms. We safeguard user data using the random base64 algorithm for encrypting and decrypting processes, which is effective and uses less space than FDDTH. We employ logistic regression, which has an accuracy of 96%. By using the previously implemented safeguards, we were able to accomplish our primary goal of delivering the data to the target domain without any data breaches.

1) To begin with, you need to implement a user login system that allows users to register and log in to the application.
2) When users register, you need to ensure that their passwords are stored securely.
3) Admin has provided a verified user to allow a work in data exchanging process in application.
4) Once users have logged in, you can create authorization roles that define what actions they are allowed to perform within the application. For example, you might have a role for users who can encrypt data, and another role for users who can decrypt data.

5) With the user login and authorization system in place, you can now implement the encryption and decryption logic for your application. When a user attempts to encrypt or decrypt data, your application should first check whether they are authorized to perform the action. If they are, the data can be encrypted or decrypted using a secure algorithm like AES or RSA.

6) Finally, you need to ensure that the encryption and decryption keys are stored securely.

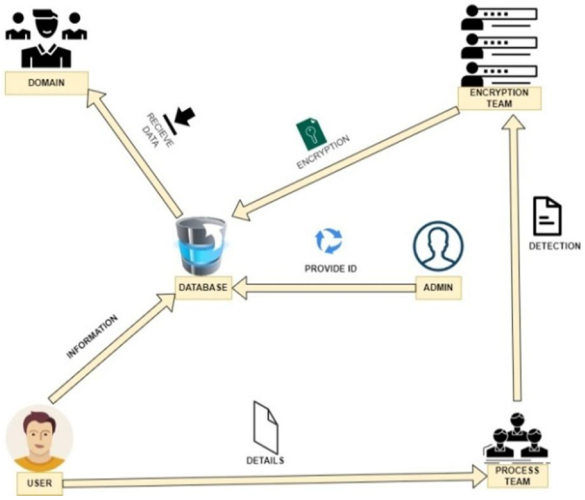


Figure1. Architecture Diagram

A. User

In our project user denotes to the client who register for their own purpose in the concept of IDCP (Information Disclosure Control Data Prevention) which the major motives is prevent the data breach from the intruders many firms/companies follows many statistics to prevent the data breach in order to prevent, Many organisation seeks data security companies to increase the client trustworthy, In our purposes after domain registers their client will enter the basic details which consist (Name, Email, Gender, Address, Password, Queries) which continues with purpose details which includes(City, state , pin code, Address, Url, and project File) now the role of IDCP is to prevent this following data from the intruders and this data must be reach to final hands(Domain) The name domain where initially registered the role of our team is to reach the following user data to safe hands which means corresponding domain.

B. Admin

The Admin has a crucial role to perform in an organisation admin is one of the top level management in the organization or business firms, Initially admin logs into the application with the specified user name and password with the specific password only for admin and then admin will provide initial access id to the specific domain and create the virtual box for the specific domain users after accessing the domain process team will request id from admin to detect the user URL whether good or bad for that purpose admin will grant the access team id to process team after the detection process completed technical team request access id to encrypt the detection data after granting the access id to the technical team finally domain also request the id for the purpose of view the encrypted data for that purpose also admin will provide unique id, after domain process completed admin will provide the payslip for securing the data.

C. Process Team

The role of Process Team in our company is to prevent the the data breach by assisting the file whether good or bad, Initially Admin will create the virtual box for the specific domain users for the purpose of prevent the domain users data from the Intruders after competition of virtual box users start to enter data which consist of personal information and the data files and urls in order to prevent male attack process team will detect the following data and url was about good or bad for that the choose the following prediction algorithm initially process team will request access id from the admin to view the user data after receiving the access id process team will view the user data and starts analysing and predicting the urls if the predicted urls results good the data will be shared for further purpose and then process team will provide the access id to the domain when its needed.

D. Technical Team

The role of technical team in our project was to protect the user data from the intruders for so technical team will initially register and login and will see the application at first technical team will request the access id to view the data after the process team find outs the file or url predict the data whether good or bad after the process team process completed technical team will view the data at the next process technical team will encrypt each and every data. For the purpose of sharing the encrypted data to the domain after encrypting the data technical team will forward encrypted data to the domain, and then domain access into view data but the data in the format of encryption to access the encrypt data domain will request the decrypt key from the technical team through that key domain can decrypt and view the raw data.

E. Domain

The role of domain in our application is initially domain logs into a user webpage then the domain will register the organisation details which consist of Organisation type, Organisation Mail, Organisation Email, and password and then Domain will be enter their purpose form which consist of Purpose and queries after details intimated to Admin , administrator will create virtual box for the following domain where the domain users can transmit data smoothly without any data breach after the data processed and secured entirely Domain access the user data without any intruders and view data by entering the correct access id which was accessed by the corresponding IDCP team following that domain will pay the service to the IDCP Firm.

III. RESULTS

Figure 2. Home Page

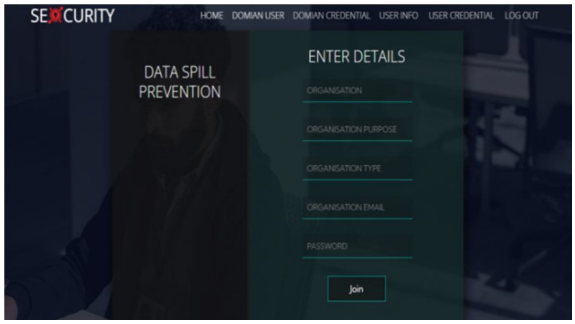


Figure 3. User Data

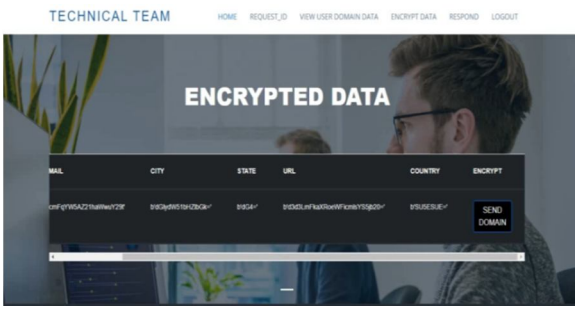


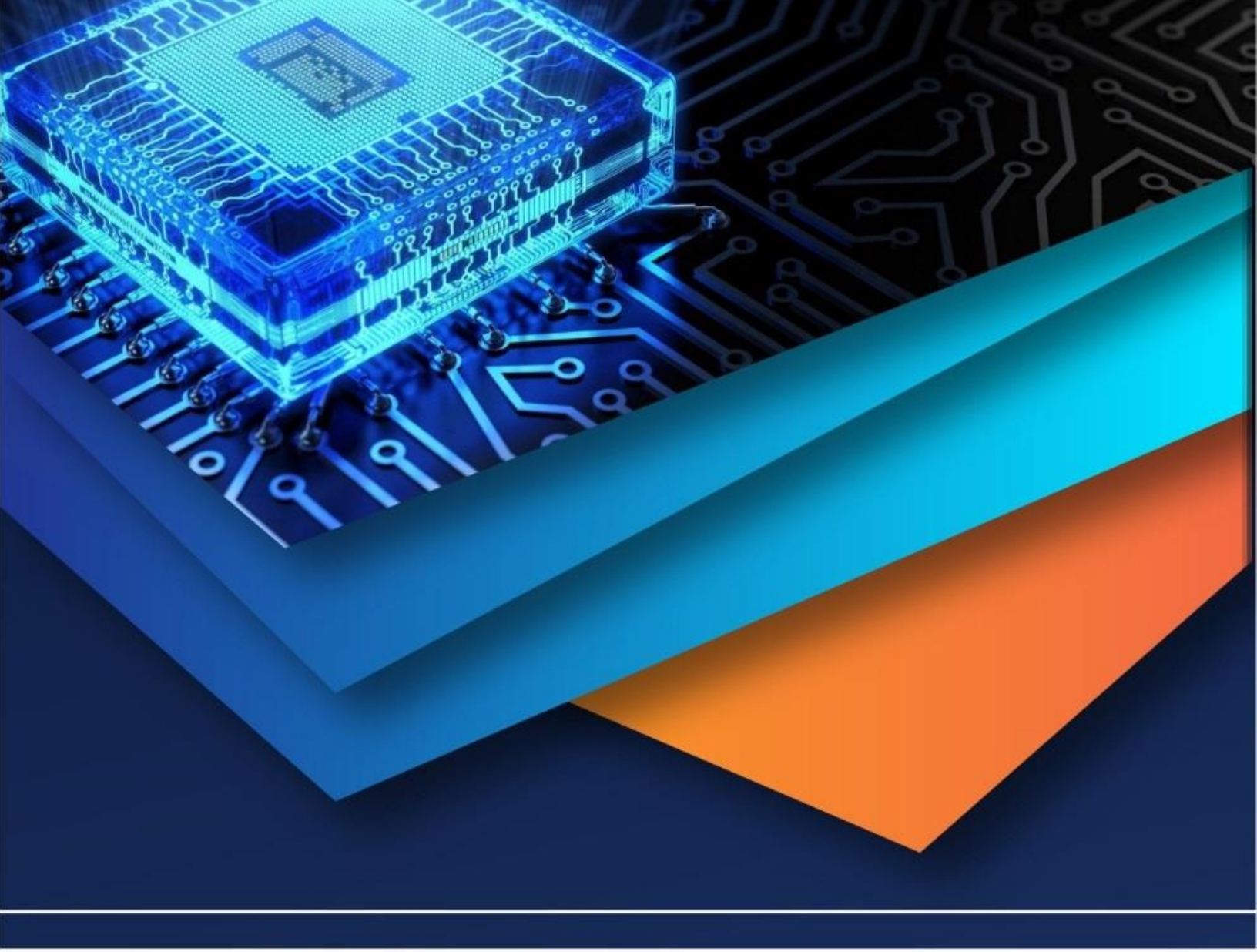
Figure 4. Encrypted Data

IV. CONCLUSION

In this project, a general study encrypting and how to prevent data breaches also predict the URL whether good or bad is conducted how. There are many different ways to prevent the data breaches which some of them are access antimalware agency prevent social engineering, software update regularly, which were ineffective in most cases for so we implement the random encryption methods and predict the url good or bad before access it and provide distribution key for perspective users will enhance the security purpose and prevent the data breaches.

REFERENCES

[1] X. Liu, Z. Hu, H. Ling, and Y.-M. Cheung, "MTFH: A matrix trifactorization hashing framework for efficient cross-modal retrieval," IEEE Trans. Pattern Anal. Mach. Intell., vol. 43, no. 3, pp. 964–981, Mar. 2021.
[2] L. Jin, K. Li, Z. Li, F. Xiao, G.-J. Qi, and J. Tang, "Deep semanticpreserving ordinal hashing for cross-modal similarity search," IEEE Trans. Neural Netw. Learn. Syst., vol. 30, no. 5, pp. 1429–1440, May 2019
[3] Harold F. Tipton - Information Security Management Handbook, Sixth Edition, Volume 2 (2007).
[4] M. L. McCallister and E. J. Immerman. "A methodology for preserving confidentiality in data base management systems.
[5] Gary McGraw - Software Security: Building Security In (2006). Gary McGraw is an American computer scientist and author who specializes in software security.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY