**ANNA UNIVERSITY: CHENNAI 600025**



**BONAFIDE CERTIFICATE**

Certified that this project report “**BCX MODEL FOR CROSS-SITE REQUEST FORGERY**” is the bonafide work of **“R.HARINI (312415104033) and**

**C. M. KANIMOZHI (312415104042)”,** who carried out the project work under my supervision.

# SIGNATURE SIGNATURE

**Dr. J. DAFNI ROSE M.E, Ph.D., Mr. K. S. ARIKUMAR M.E, (Ph.D.),**

**Professor, Assistant Professor,**

**Head of the Department, Computer Science and Engineering, Computer Science and Engineering,** St. Joseph’s Institute of Technology, St. Joseph’s Institute of Technology, Old Mamallapuram road,

Old Mamallapuram road, Chennai - 600 119. Chennai - 600 119.

# ACKNOWLEDGEMENT

We take this opportunity to thank our honourable Chairman **Dr. B. Babu Manoharan, M.A., M.B.A., Ph.D.** for the guidance he offered during our tenure in this institution.

We extend our heart felt gratitude to our honourable Managing Director **Mrs. B. Jessie Priya, M.Com.** and Director **Mr. B. Sashisekar, M.Sc. (INTL Business)** for providing us with the required resources to carry out this project.

We are indebted to our Principal **Dr. P. Ravichandran, M.Tech., Ph.D.**

for granting us permission to undertake this project.

We would like to express our earnest gratitude to our Head of the Department **Dr. J. Dafni Rose, M.E., Ph.D.** for her commendable support and encouragement for the completion of the project with perfection.

We also take this opportunity to express our profound gratitude to our guide **Mr. K. S. Arikumar, M.E., (Ph.D.),** Assistant professor for his guidance, constant encouragement, immense help and valuable advice for the completion of this project.

We wish to convey our sincere thanks to all the teaching and non-teaching staff of the department of **Computer Science and Engineering, St. Joseph’s Institute of Technology** without whose co-operation this venture would not have been a success.

**CERTIFICATE OF EVALUATION**

College Name : St. JOSEPH’S INSTITUTE OF TECHNOLOGY Branch : COMPUTER SCIENCE AND ENGINEERING

Semester VIII

|  |  |  |  |
| --- | --- | --- | --- |
| **Sl.No** | **Name of the Students** | **Title of the project** | **Name of the Supervisor with designation** |
| 1 | R. Harini | BCX Model for | Mr. K. S. Arikumar M.E, (Ph.D.) |
|  | (312415104033) | Cross-Site Request | Assistant Professor, |
| 2 | C. M. Kanimozhi | Forgery. | CSE Department, |
|  | (312415104042) |  | St. Joseph’s Institute of |
|  |  |  | Technology. |

The report of the project work submitted by the above students in partial fulfilment for the award of Bachelor of Engineering Degree in **Computer Science and Engineering** of Anna University were evaluated and confirmed to be report of the work done by above students.

Submitted for project review and viva voce exam held on

# (INTERNAL EXAMINER) (EXTERNAL EXAMINER)

**ABSTRACT**

Cross-Site Request Forgery is a widely exploited Website vulnerability. The CSRF is a major security threat to the Online Transaction, in which the user is forced to enter into some malicious websites and reveal their login credentials, or the attacker enter into the user’s authenticated session, without the user’s knowledge. The existing approaches to prevent CSRF such as OTP, Tokens and removal of the Same-site cookies from the web application doesn’t yield the expected security to the applications. Hence, this proposal uses the Mathematical Binary Conversion, Combination and X-OR (BCX) Model to remove CSRF attacks. In order to confirm that the user who makes the login and the Money transaction is one and the same and to prove that there is no Attacker intervention into the logged on session, the MAC address off the system is taken and subjected to the BCX Algorithm and the hash value of the MAC is saved on login and verified on making a transaction. Moreover, the Anti-Forgery Token(AFT) is produced from the combination of the IP Address and the password of the user and it is also subjected to the BCX Algorithm. The AFT is generated and saved during Login and verified on making a transaction. Thus, by using the BCX model, the security threats to the end user of the various applications is reduced and the Cross Site Request Forgery attacks on the web pages during the transaction is avoided.

# TABLE OF CONTENTS

|  |  |  |
| --- | --- | --- |
| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |
|  | **ABSTRACT** | **iv** |
|  | **LIST OF FIGURES** | **ix** |
|  | **LIST OF TABLES** | **xi** |
|  | **LIST OF ABBREVIATIONS** | **xii** |
| **1.** | **INTRODUCTION** | **1** |
|  | 1.1 Overview | 1 |
|  | 1.2 Problem Statement | 3 |
|  | 1.3 Existing system | 5 |
|  | 1.3.1 Secured Connection | 5 |
|  | 1.3.2 Https POST Method | 5 |
|  | * + 1. Same-Site Cookies     2. Token Authentication and Captcha | 5  6 |
|  | 1.3.5 Avoiding Transition between  Web pages | 6 |
|  | 1.3.6 Time-Out and  Re-Authentication | 6 |
|  | 1.4 Proposed System | 7 |

* + 1. Login Validation 7
    2. BCX Hash Algorithm for

Mac Address 8

* + 1. BCX Hash Algorithm for

Anti-Forgery Token Generation 9

* + 1. Transaction Validation 9

# LITERATURE REVIEW 11

# SYSTEM DESIGN 19

* 1. Unified modelling language 19
     1. Use case diagram of

BCX model for Cross-Site

Request Forgery 19

* + 1. Class diagram of

BCX model for Cross-Site

Request Forgery 21

* + 1. Sequence diagram of BCX model for Cross-Site

Request Forgery 22

* + 1. Activity diagram of

BCX model for Cross-Site

Request Forgery 23

* + 1. Collaboration diagram of BCX model for Cross-Site

Request Forgery 24

* + 1. Component diagram of BCX model for Cross-Site

Request Forgery 25

* + 1. Deployment diagram of BCX model for Cross-Site

Request Forgery 26

* + 1. Package diagram of

BCX model for Cross-Site

Request Forgery 27

* + 1. Object diagram of

BCX model for Cross-Site

Request Forgery 29

# SYSTEM ARCHITECTURE 31

* 1. Architecture Description 31
  2. Client Module 33
     1. BCX Hash Algorithm in Client Module for Generating Hash

Value of MAC Address 34

* 1. Server Module 35

4.2.1 BCX Hash Algorithm in Server Module for Generating the

Anti-Forgery Token 36

# SYSTEM IMPLEMENTATION 37

* 1. Implementation of BCX Model for

Cross-Site Request Forgery 37

* 1. Pseudo code for generating hash value

of MAC Address 40

* 1. Pseudo code for generating Anti-

Forgery Token 41

# RESULTS AND OUTPUT 43

* 1. BCX Model for Cross-Site

Request Forgery 43

* 1. Output and Comparison 54
     1. Hash Value of the MAC Address 54
     2. Generation of the Anti-Forgery Token 55
     3. Result Analysis 56

# CONCLUSION AND FUTUREWORK 58

|  |  |  |
| --- | --- | --- |
| 7.1 | Conclusion | 58 |
| 7.2 | Future work | 58 |

**REFERENCES**

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **LIST OF FIGURES** | **NAME OF THE FIGURE** | **PAGE NO.** |
| 3.1 | Use case diagram of |  |
|  | BCX Model for Cross-Site |  |
|  | Request Forgery | 20 |
| 3.2 | Class diagram of |  |
|  | BCX Model for Cross-Site |  |
|  | Request Forgery | 21 |
| 3.3 | Sequence diagram of |  |
|  | BCX Model for Cross-Site |  |
|  | Request Forgery | 22 |
| 3.4 | Activity diagram of |  |
|  | BCX Model for Cross-Site |  |
|  | Request Forgery | 23 |
| 3.5 | Collaboration diagram of |  |
|  | BCX Model for Cross-Site |  |
|  | Request Forgery | 25 |
| 3.6 | Component diagram of |  |
|  | BCX Model for Cross-Site |  |
|  | Request Forgery | 26 |
| 3.7 | Deployment diagram of |  |
|  | BCX Model for Cross-Site |  |
|  | Request Forgery | 27 |
| 3.8 | Package diagram of |  |
|  | BCX Model for Cross-Site |  |
|  | Request Forgery | 28 |

3.9 Object diagram of

BCX Model for Cross-Site

Request Forgery 30

* 1. System Architecture of BCX Model for Cross-Site

Request Forgery 31

* 1. Interactions between Client Module,

Server Module and Database 32

* 1. Login Page 38
  2. Transaction Page 39
  3. Hash Value of the MAC Address 54
  4. Generation of the Anti-Forgery Token 55
  5. Performance Analysis 57

|  |  |  |
| --- | --- | --- |
| **LIST OF TABLES** | **LIST OF TABLES**  **NAME OF THE TABLE** | **PAGE NO.** |
| 5.1 | Structure of Login Table | 39 |
| 5.2 | Structure of Hash Table | 40 |
| 6.1 | Comparison of Hash Algorithm’s | 56 |

|  |  |
| --- | --- |
|  | **LIST OF ABBREVATIONS** |
| CSRF | Cross-Site Request Forgery |
| BCX | Binary conversion-Combination-eXclusive OR |
| HTTP | Hyper Text Transfer Protocol |
| HTTPS | Hyper Text Transfer Protocol Secure |
| MAC | Medium Access Control |
| IP | Internet Protocol |
| AFT | Anti-Forgery Token |
| ASCII | American Standard Code for Information Interchange |
| SHA | Secured Hash Algorithm |
| URL | Uniform Resource Locator |
| XSS | Cross-Site Scripting |
| DOM | Document Object Model |
| MD | Message Digest |
| AES | Advanced Encryption Standard |
| DES | Data Encrytion Standard |
| RSA | Rivest Shamir Adleman |
| CPU | Central Processing Unit |
| PHP | Hypertext Preprocessor |
| HMAC | Hash Message Authentication Code |
| UML | Unified Modelling Language |
| CSS | Cascading Style Sheet |
| IMEI | International Mobile Equipment Identity |