ĐỒ ÁN AN TOÀN VÀ BẢO MẬT THÔNG TIN

Họ và Tên: Nguyễn Thành Bắc ( Nhà phát triển của trang web **SafeStorage**)

Msv : 2174801040739

Ý tưởng : Một trang web tên **SafeStorage** ( dùng thuật toán đa bảng cho phép người dùng truy cập vào để lưu trữ dữ liệu, tài liệu , thông tin quan trọng và bảo mật chúng )

**I . Tổng quát**

1. Mục tiêu: Cung cấp một nền tảng cho các tổ chức, cá nhân và doanh nghiệp để chia sẻ và lưu trữ các tài liệu quan trọng một cách an toàn và bảo mật trên internet.
2. Trang web lưu trữ dữ liệu: Trang web sẽ được xây dựng trên một hệ thống máy chủ được quản lý bởi chúng tôi. Điều này giúp đảm bảo rằng dữ liệu của khách hàng được lưu trữ an toàn và bảo mật. Khách hàng của tôi sẽ được cung cấp tài khoản riêng để truy cập vào trang web của tôi.
3. Thuật toán mã hóa đa bảng: Để bảo mật thông tin của khách hàng, trang web của tôi sẽ sử dụng thuật toán mã hóa đa bảng. Thuật toán này sẽ mã hóa dữ liệu người dùng và chuyển nó thành một chuỗi ký tự không đọc được, trước khi lưu trữ nó trong cơ sở dữ liệu của tôi. Điều này đảm bảo rằng dữ liệu của khách hàng được bảo mật và chỉ có người dùng có chứng chỉ đăng nhập đúng mới có thể giải mã dữ liệu.
4. Quá trình mã hóa: Quá trình mã hóa sẽ được thực hiện trên máy chủ của tôi bằng cách sử dụng một khoá mã hóa đa bảng. Khi người dùng tải lên dữ liệu của mình lên trang web của tôi, dữ liệu sẽ được chia thành các khối và mã hóa mỗi khối bằng một thuật toán mã hóa đa bảng. Sau khi mã hóa hoàn tất, dữ liệu sẽ được lưu trữ trên máy chủ của tôi. Khi người dùng muốn truy cập dữ liệu của mình, hệ thống của tôi sẽ sử dụng một chứng chỉ đăng nhập để giải mã dữ liệu và trả về cho người dùng.
5. An toàn và bảo mật: Để đảm bảo an toàn và bảo mật cho người dùng, trang web của tôi sẽ sử dụng các biện pháp bảo mật như mật khẩu mạnh, mã hóa SSL, xác thực hai yếu tố và giám sát an ninh hệ thống.

**II .Quá trình mã hóa**

Quá trình mã hóa được diễn ra như sau :

Bước 1 : Chuẩn bị khóa mã hóa

* Tạo khoá mã hóa ngẫu nhiên, sử dụng thuật toán mã hóa đa bảng AES 128-bit hoặc AES 256-bit, để đảm bảo tính bảo mật cao.
* Lưu khoá mã hóa an toàn trên máy chủ.

Bước 2: Chia dữ liệu thành cách khối dữ liệu

* Dữ liệu của người dùng sẽ được chia thành các khối dữ liệu nhỏ hơn để tiện việc mã hóa và lưu trữ .

Bước 3: Mã hóa các khối dữ liệu

* Mỗi khối dữ liệu sẽ được mã hóa bằng thuật toán AES và khoá mã hóa tương ứng.
* Kết quả mã hóa được lưu trữ an toàn trên máy chủ.

Bước 4: Giải mã dữ liệu

* Khi người dùng muốn truy cập dữ liệu của mình, dữ liệu sẽ được giải mã bằng cách sử dụng khoá mã hóa tương ứng.
* Dữ liệu được giải mã sẽ chỉ được truy cập bởi người dùng có quyền truy cập.

**III. Tính bảo mật và an toàn của quá trình mã hóa**

1. Khoá mã hóa được tạo ngẫu nhiên: Khoá mã hóa được tạo ngẫu nhiên, đảm bảo tính ngẫu nhiên và bảo mật của khoá mã hóa.
2. Quá trình mã hóa được thực hiện trên máy chủ: Quá trình mã hóa được thực hiện trên máy chủ, đảm bảo tính bảo mật và an toàn của quá trình mã hóa.
3. Dữ liệu được mã hóa trước khi được lưu trữ: Dữ liệu của người dùng được mã hóa trước khi được lưu trữ trên trang web, đảm bảo tính bảo mật và an toàn của dữ liệu.

**IV. Mô Phỏng**

Giả sử , nếu tôi nhập vào tên của mình là ” Nguyễn Thành Bắc “ vào web , thì quá trình mã hóa sẽ diễn ra như sau :

Bước 1: chuẩn bị mã hóa

* Tạo khoá mã hóa AES 128-bit ngẫu nhiên, ví dụ: "b61c57d8b2e92c292704405d3dc3f3c9"
* Lưu khoá mã hóa an toàn trên máy chủ của tôi

Bước 2: Chia tên thành các khối dữ liệu

* Tên “Nguyễn Thành Bắc“ sẽ được chia thành 2 khối dữ liệu: “Nguyễn Thành” và “Bắc”

Bước 3: Mã hóa các khối dữ liệu

* Mỗi khối dữ liệu sẽ được mã hóa bằng thuật toán AES 128-bit và khoá mã hóa tương ứng được sử dụng.
* Ví dụ: khối "Nguyễn Thành" được mã hóa bằng khoá mã hóa "b61c57d8b2e92c292704405d3dc3f3c9", kết quả là "cGwN2XdW+YYmxIK3dUEOdw=="
* Khối "Bắc" được mã hóa bằng khoá mã hóa "b61c57d8b2e92c292704405d3dc3f3c9", kết quả là "ldG9W8V0Qdi+H1rVv1yj0g=="

Bước 4: Lưu trữ dữ liệu mã hóa

* Lưu trữ các khối dữ liệu đã được mã hóa an toàn trên máy chủ của tôi.

Bước 5: Giải mã dữ liệu

* Khi người dùng muốn truy cập tên của mình, họ sẽ đăng nhập vào hệ thống của tôi bằng chứng chỉ đăng nhập.
* Máy chủ của tôi sẽ sử dụng khoá mã hóa đã lưu trữ an toàn để giải mã các khối dữ liệu.
* Sau đó, các khối dữ liệu sẽ được kết hợp lại để tạo ra tên đầy đủ "Nguyễn Thành Bắc".

Bảng Tra:

|  |  |
| --- | --- |
| Ký tự | Giá trị |
| A | 41 |
| B | 42 |
| C | 43 |
| … | … |
| Z | 5A |
| a | 61 |
| b | 62 |
| c | 63 |
| … | … |
| z | 7A |
| 0 | 30 |
| 1 | 31 |
| 2 | 32 |
| … | … |
| 9 | 39 |
| + | 2B |
| / | 2F |
| = | 3D |

Bảng dữ liệu :

| **Giá trị cần mã hóa** | **Khóa mã hóa** | **Kết quả** | **Giải mã** |
| --- | --- | --- | --- |
| Nguyễn Thành | b61c57d8b2e92c292704405d3dc3f3c9 | cGwN2XdW+YYmxIK3dUEOdw== | Nguyễn Thành |
| Bắc | b61c57d8b2e92c292704405d3dc3f3c9 | ldG9W8V0Qdi+H1rVv1yj0g== | Bắc |

**V. Kết luận**

Trong bối cảnhTrong bối cảnh mà việc lưu trữ và bảo mật dữ liệu trở nên ngày càng quan trọng, việc tìm ra giải pháp đảm bảo an toàn và bảo mật thông tin của người dùng trên trang web **SafeStorage** là cực kỳ cần thiết. Với ý tưởng của chúng tôi, việc sử dụng thuật toán mã hóa đa bảng và lưu trữ dữ liệu trên máy chủ an toàn sẽ giúp người dùng yên tâm khi lưu trữ và chia sẻ thông tin của mình.

Chúng tôi hy vọng rằng ý tưởng này sẽ đem lại lợi ích lớn cho cộng đồng người dùng trên toàn thế giới và giúp cho cuộc sống của họ trở nên an toàn và bảo mật hơn.

Chúng tôi xin chân thành cảm ơn bạn đã tin tưởng và sử dụng trang web của chúng tôi để lưu trữ thông tin của mình. Chúng tôi cam kết luôn đem đến cho bạn những trải nghiệm tốt nhất và sẵn sàng tiếp thu ý kiến đóng góp để cải thiện dịch vụ của mình.

**Nhà phát triển web SafeStorage : Nguyễn Thành Bắc**