|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **BỘ GIÁO DỤC VÀ ĐẠO TẠO**  **TRƯỜNG ĐẠI HỌC HỒNG ĐỨC**  **KHOA CÔNG NGHỆ THÔNG TIN**  **BÁO CÁO BÀI TẬP LỚN**  **DECENTRALIZED CIPHERTEXT – POLICY ATTRIBUTED – BASED ENCRYPTION SCHEMES FOR LIGHTWEIGHT DEVICES**   |  |  | | --- | --- | | **Nhóm sinh viên thực hiện:** | **Trịnh Văn An** | | **Tống Duy Đạt** | | **Lê Hoàng Hiếu** | | **Nguyễn Huy Hoàng** | | **Chu Đình Khánh Hưng** | | **Nguyễn Gia Khiêm** |   *…., tháng… năm….* |

**LỜI MỞ ĐẦU**

Trong thời đại số hóa hiện đại, việc bảo vệ và quản lý dữ liệu cá nhân, doanh nghiệp, và tổ chức trở nên cực kỳ quan trọng. Đồng thời, sự phát triển của các hệ thống trực tuyến và đám mây đã tạo ra nhiều thách thức trong việc đảm bảo tính bảo mật và quản lý quyền truy cập vào thông tin.

Hệ mã ABE (Attribute-Based Encryption) đã nổi lên như một công nghệ mật mã đáng chú ý giúp giải quyết những thách thức này. Với khả năng kiểm soát quyền truy cập dựa trên các thuộc tính của người dùng thay vì các khóa truy cập cụ thể, ABE đã mở ra một loạt các ứng dụng hứa hẹn trong nhiều lĩnh vực khác nhau.

Chúng ta sẽ xem xét cách ABE được sử dụng trong bảo mật dữ liệu đám mây, quản lý quyền truy cập, y tế, giáo dục và nhiều lĩnh vực khác, đồng thời tìm hiểu về những lợi ích và thách thức của công nghệ này trong thế giới kỹ thuật số ngày nay.

**MỤC LỤC**

[CHƯƠNG I. TỔNG QUAN VỀ VẤN ĐỀ TRAO ĐỔI DỮ LIỆU TRONG TRƯỜNG HỌC HIỆN NAY 5](#_Toc149158844)

[1.1. Tổng quan 5](#_Toc149158845)

[1.2. Vấn đề gặp phải 5](#_Toc149158846)

[1.3. Giải pháp 6](#_Toc149158847)

[CHƯƠNG II. PHÂN TÍCH THIẾT KẾ HỆ THỐNG 8](#_Toc149158848)

[1.1. Phân cấp chức vụ trong một trường học hiện tại. 8](#_Toc149158849)

[1.2. Phân tích thiết kế hệ thống 9](#_Toc149158850)

[1.2.1. Tổng quan về hệ thống 9](#_Toc149158851)

[1.2.2. Hệ thống quản lý người dùng 10](#_Toc149158852)

[1.2.3. Hệ thống quản lý bài viết 11](#_Toc149158853)

[1.2.4. Xây dựng cơ sở dữ liệu 13](#_Toc149158854)

[CHƯƠNG III. HỆ MÃ HÓA CÓ THUỘC TÍNH ( ATTRIBUTE-BASED ENCRYPTION ) 15](#_Toc149158855)

[1.1. Giới thiệu chung hệ mã ABE 15](#_Toc149158856)

[1.2. Phân loại 15](#_Toc149158857)

[1.2.1. Ciphertext-Policy ABE (CP-ABE): 15](#_Toc149158858)

[1.2.2. Key-Policy ABE (KP-ABE): 17](#_Toc149158859)

[1.3. Cách hoạt động của hệ mã ABE 18](#_Toc149158860)

[1.3.1. Khởi tạo hệ thông ABE 18](#_Toc149158861)

[1.3.2. Tạo khóa cho người dùng 18](#_Toc149158862)

[1.3.3. Mã hóa 19](#_Toc149158863)

[1.3.4. Giải mã 20](#_Toc149158864)

[CHƯƠNG IV. CÀI ĐẶT TRƯƠNG TRÌNH 21](#_Toc149158865)

[CHƯƠNG V. TỔNG KẾT 22](#_Toc149158866)

1. TỔNG QUAN VỀ VẤN ĐỀ TRAO ĐỔI DỮ LIỆU TRONG TRƯỜNG HỌC HIỆN NAY

## Tổng quan

Trong thời đại chuyển đổi số hiện nay, việc quản lý dữ liệu và học liệu số đã trở thành một phần không thể thiếu của hệ thống giáo dục. Có nhiều lợi ích đáng kể mà công nghệ số mang lại. Một trong những lợi ích chính là tính cá nhân hóa. Quản lý dữ liệu giúp học sinh và giáo viên theo dõi tiến trình học tập và đánh giá kết quả một cách cụ thể, tạo điều kiện cho giảng dạy và học tập cá nhân hóa dựa trên nhu cầu và khả năng của từng học sinh. Hơn nữa, quản lý dữ liệu số tạo ra môi trường học tập linh hoạt và thuận tiện. Học liệu số, bao gồm sách điện tử, tài liệu tham khảo trực tuyến, và khóa học trực tuyến, giúp học sinh truy cập kiến thức mọi lúc, mọi nơi, từ bất kỳ thiết bị nào có kết nối internet. Điều này thúc đẩy sự tự học và tạo cơ hội học tập liên tục.

## Vấn đề gặp phải

Tuy nhiên đạt được nhưng ưu điểm rất ý nghĩa nhưng quản lý dữ liệu và học liệu số cũng đối diện với một số hạn chế.

***Vấn đề về bảo mật thông tin***

Việc trao đổi thông tin giữa các giáo viên hoặc một nhóm cán bộ trong trường hiện đang gặp một hạn chế đó là khi giáo viên muốn thông báo cho một nhóm cụ thể trong tổ của họ mà không muốn tiết lộ thông tin đó cho cả trường. Chẳng hạn, giáo viên cần gửi một tài liệu như một file Word hoặc hình ảnh để chia sẻ với một nhóm làm việc cụ thể, nhưng họ muốn giữ thông tin này bí mật với các tổ khác hoặc toàn bộ trường học. Tuy nhiên, hệ thống quản lý dữ liệu trong trường học thường không đảm bảo tính riêng tư và bảo mật đầy đủ trong trường hợp như vậy. Khi một giáo viên tải lên tài liệu hoặc thông báo vào hệ thống, thông tin này có thể dễ dàng truy cập bởi các thành viên khác trong trường hoặc bởi quản trị viên hệ thống. Hạn chế này có thể dẫn đến việc tiết lộ thông tin nhạy cảm, gây bất lợi cho giáo viên hoặc tổ giảng dạy. Ngoài ra, nó cũng tạo ra tình trạng không đáng tin cậy khi các giáo viên hoặc nhóm làm việc cảm thấy thông tin của họ không được bảo vệ đúng cách. Điều này có thể gây ra sự ngần ngại trong việc chia sẻ và hợp tác trong môi trường giáo dục.

***Vấn đề về quản lý và xác thực thông tin***

Trong quá trình quản lý dữ liệu trong trường học, một vấn đề hạn chế đáng chú ý xuất hiện khi giáo viên và nhân viên trường sử dụng các công cụ trao đổi thông tin như email hoặc các phần mềm chat để truyền đạt công việc và thông tin liên quan đến giảng dạy. Mặc dù có thể hiệu quả trong việc truyền tải thông tin nhanh chóng, nhưng hạn chế xảy ra khi cần tìm kiếm và xác thực thông tin trong tương lai. Cụ thể, việc sử dụng email và các ứng dụng chat cá nhân hóa, thường gây khó khăn trong việc quản lý thông tin liên quan đến công việc. Thông tin này có thể bị tán hoặc phân mảnh trong các hộp thư đến và thư đã gửi, cũng như trong các cuộc trò chuyện trực tuyến. Khi cần tra cứu hoặc xác minh thông tin, việc lục lại tất cả các email hoặc cuộc trò chuyện có thể trở nên rắc rối và mất thời gian. Điều này đặc biệt trở nên quan trọng khi cần đối phó với các thông tin quan trọng về học sinh, lịch giảng dạy, hoặc bất kỳ vấn đề quản lý nào khác. Hạn chế này cũng liên quan đến tính cá nhân hóa của email và ứng dụng chat. Do tính riêng tư, nhiều thông tin quan trọng có thể chỉ được chia sẻ giữa một số người cụ thể, khiến cho việc tìm kiếm và xác thực trở nên phức tạp hơn.

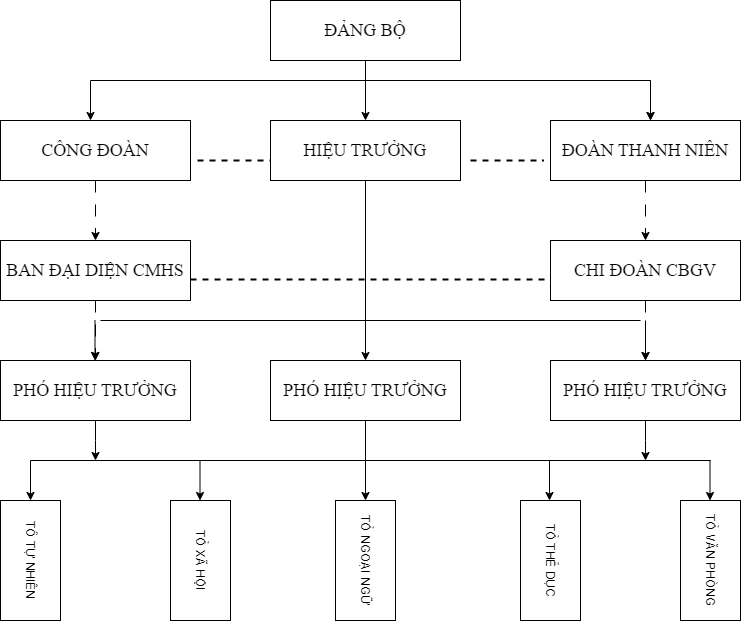
## Giải pháp

Từ những hạn chế của việc trao đổi thông tin trong trường học hiện tại chúng tôi đề xuất một giải pháp tiềm năng để khắc phục vấn đề hạn chế trong việc quản lý dữ liệu và thông tin giữa giáo viên và nhân viên trường học là sử dụng một phần mềm có khả năng mã hóa các file và cung cấp quyền truy cập dựa trên các thuộc tính người mã hóa đã cài đặt. Điều này có thể cải thiện tính bảo mật và quản lý thông tin một cách hiệu quả, đồng thời đảm bảo tính riêng tư cho các thông tin quan trọng. Phần mềm mã hóa file sẽ biến dữ liệu thành dạng không thể đọc được cho đến khi nó được giải mã. Mỗi tệp tin được mã hóa có thể được trao đổi và lưu trữ một cách an toàn, giảm nguy cơ bị truy cập bởi các bên không được ủy quyền. Một hệ mã tiềm năng hiện tại có thể ứng dụng được cho giải pháp trên đó là hệ mã dựa trên thuộc tính Hệ mã ABE (Attribute-Based Encryption) nó có thể dựa trên các thuộc tính đã cài đạt sẵn và mã hóa cũng như giải mã dữ liệu một cách hiệu quả, chi tiết về các hoạt động của mã chúng tôi sẽ giới thiệu ở chương 3.

1. PHÂN TÍCH THIẾT KẾ HỆ THỐNG

## Phân cấp chức vụ trong một trường học hiện tại.

Cấu trúc phân cấp chức vụ trong một trường cấp 3 công lập ở Việt Nam được xây dựng với mục tiêu quản lý hiệu quả và đảm bảo sự hoạt động suôn sẻ của trường. Tuỳ thuộc vào quy mô của mỗi trường học mà mỗi trường sẽ có cấu trúc phần cấp chức vụ khác nhau. Hiệu trưởng đứng đầu trường, đảm bảo sự tổ chức và quản lý toàn bộ hoạt động giáo dục. Phó hiệu trưởng hỗ trợ hiệu trưởng và đối phó với các lĩnh vực cụ thể như quản lý học sinh hay hành chính. Từng tổ giáo viên có một trưởng tổ, người đóng vai trò quan trọng trong việc tổ chức giảng dạy và học tập, lập kế hoạch, và đảm bảo chất lượng giảng dạy. Giáo viên, là người trực tiếp tương tác với học sinh, có nhiệm vụ chính là giảng dạy các môn học và theo dõi tiến bộ của học sinh. Nhân viên hành chính đảm bảo các công việc hành chính của trường suôn sẻ, bao gồm quản lý thông tin và lịch trình. Nhân viên dịch vụ, như nhân viên vệ sinh và bảo vệ, duy trì môi trường sạch sẽ và an toàn cho học sinh. Cụ thể được thể hiện ở sơ đồ phần cấp chức vụ trong hình 1.



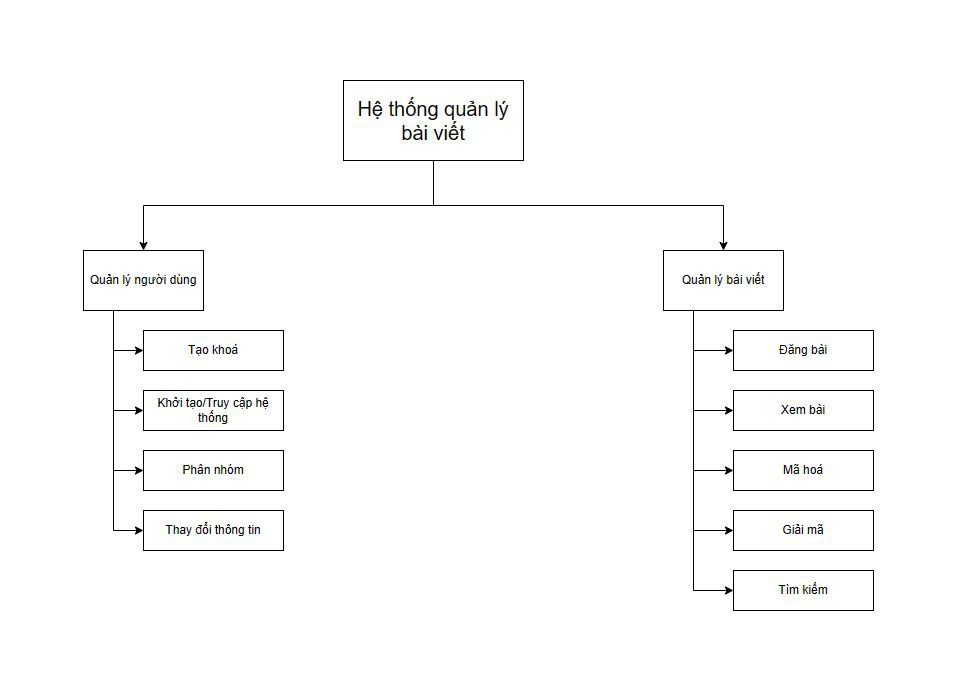
Hình . Sơ đồ phân cấp chức vụ của một trường cấp 3 công lập ở Việt Nam

## Phân tích thiết kế hệ thống

### Tổng quan về hệ thống

Hệ thống khi hoạt động sẽ có khả năng xử lý và lưu trữ các bài viết mà người dùng đăng lên hệ thống. Mỗi người dùng sẽ có một tài khoản tương ứng với một cặp khóa công khai và bí mật được cấp từ admin cũng là quản trị viên của hệ thống khi có một yêu cầu đăng kí tài khoản của một giáo viên hoặc nhân viên trong trường.

Hệ thống sẽ gồm 2 chức năng chính đó là quản lý tin tức và quản lý tài khoản. Ở phần quản lý tài khoản thì hệ thống có thể cho phép admin tạo khóa, thêm các thuộc tính và xóa đi các tài khoản khi cần thiết. Ở phần quản lý tin hệ thống cho phép người dùng có thể đăng tin, sửa tin, xóa tin, mã hóa file, giải mã file cũng như tìm kiếm các tin đã đăng trên hệ thông. Cụ thể các chức năng của hệ thông được thể hiện sơ đồ trong hình 2.



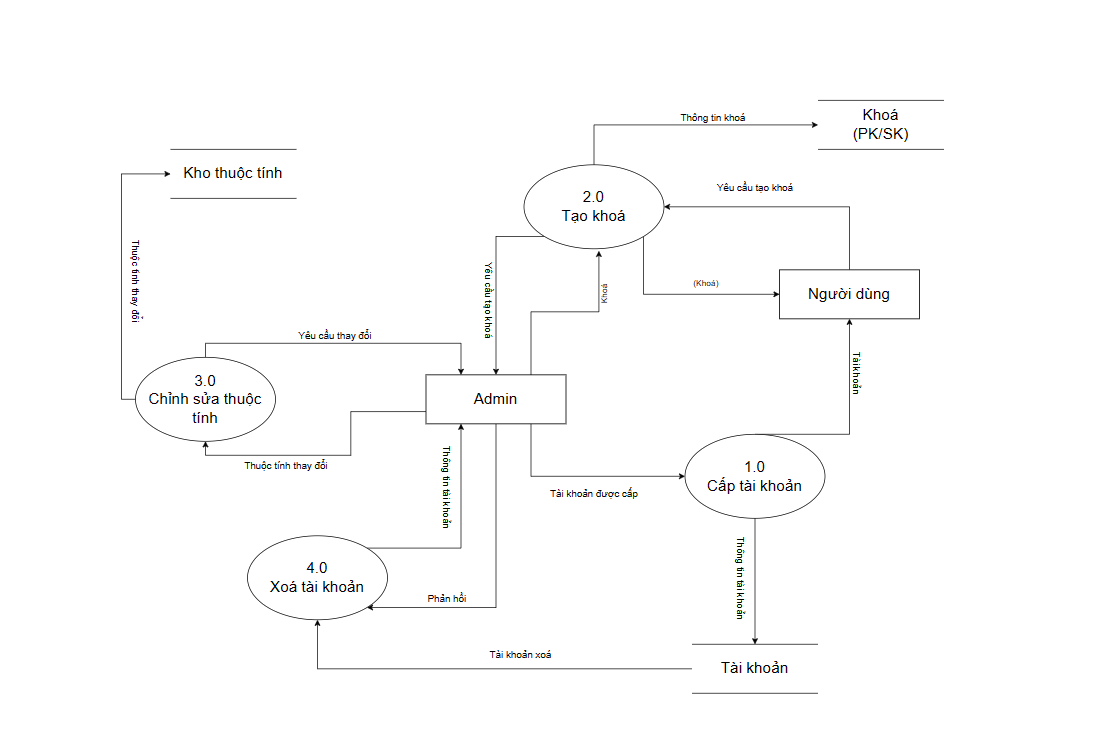
Hình . Sơ đồ phân cấp chức năng của hệ thống

### Hệ thống quản lý người dùng

Quy trình quản lý người dùng hoạt động như sau:

* Khi muốn tham gia hệ thống người dùng có thể thực hiện việc đăng kí tài khoản với hệ thống. Hệ thống sẽ tiếp nhận các thông tin từ người dùng kiểm tra các thông tin mà người dùng đã cũng cấp cho hệ thông xem có đủ điều ki để tham gia hệ thống hay không. Nếu đủ điều kiện tham gia hệ thống sẽ gửi cho người dùng xác nhận đã tạo tài khoản thành công. Nêu không hệ thống sẽ từ chối yêu cầu đăng kí của người dùng và gủi phẩn hồi lại cho người dùng.
* Khi giáo viên hoặc nhân viên trong trường đã có tài khoản yêu cầu tạo khóa, quản trị viên sẽ tiếp nhận yêu cầu và kiểm tra các thuộc tính của giáo viên hoặc nhân viên đó và từ những thuộc tính đó tao khóa cho giáo viên hoặc nhận viên đã yêu cầu tạo khóa. Khi mà tạo khóa thành công quản trị viên sẽ gửi lại một cặp khóa công khai và bí mật tương ứng với tài khoản yêu cầu tạo khóa cho cho họ. Khi các thông tin cung cấp cho quản trị viên, quản trị viên có quyển từ chối tạo khóa cho người dùng.
* Khi quản trị viên muốn xóa một tài khoản từ hệ thống, họ sẽ truy cập thông tin tài khoản từ kho dữ liệu tài khoản và thực hiện việc xóa tài khoản đó khỏi hệ thống.
* Nếu quản trị viên muốn thêm các thuộc tính cho hệ thống, họ sẽ lấy dữ liệu từ kho dữ liệu thuộc tính và sau đó cập nhật thông tin tương ứng. Dữ liệu đã được cập nhật sẽ được lưu trữ lại trong kho dữ liệu thuộc tính.

Toàn bộ quy trình hoạt động của chức năng quản lý hệ thông được trình bày đầy đủ ở sơ đồ luồng dữ liệu của chức năng quản lý người dùng, hình 3



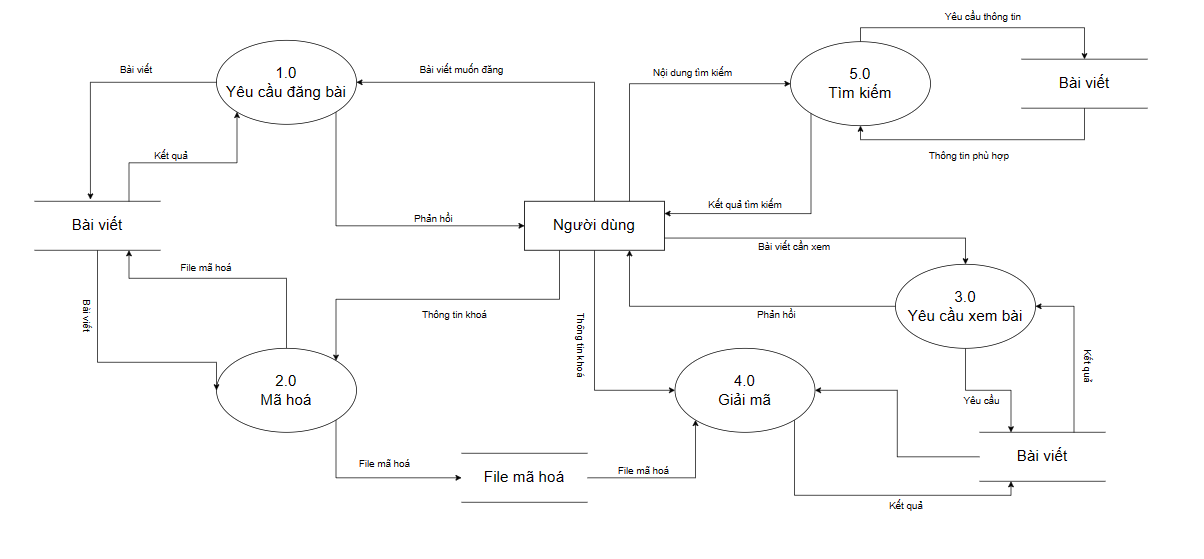
Hình . Sơ đồ luồng dữ liệu của chức năng quản lý người dùng.

### Hệ thống quản lý bài viết

Mô tả luồng dữ liệu của biểu đồ quản lý bài viết như sau:

* Khi người dùng muốn đăng bài lên hệ thống, hệ thống sẽ tiếp nhận yêu cầu và gửi phản hồi xác định xem người dùng có được phép đăng bài lên hệ thống hay không. Nếu quyết định cho phép đăng bài, bài viết sẽ được lưu vào kho dữ liệu bài viết.Nếu bài viết đính kèm theo file mà người dùng muốn mã hóa người dùng sẽ mã hóa file với khóa bí mật của họ sau đó gửi file lên cho hệ thống. Hệ thống sẽ lưu file mã hóa vào kho. Nếu bài viết bị hệ thống từ chối hệ thống sẽ gửi phản hồi cho người đăng bài.
* Khi người dùng muốn xem một bài viết, họ phải gửi yêu cầu xem bài viết lên hệ thống, Hệ thống sẽ gửi thông tin về bài viết cho người dùng. Trong trường hợp người dùng muốn xem một file được đính kèm theo tin thì người dùng sẽ gửi các thuộc tính của bản thân và khóa công khai của người gửi bài cho hệ thống và hệ thống sẽ giải mã file và gửi file cho người dùng.
* Khi người dùng muốn tìm kiếm một bài viết trên hệ thống, họ sẽ gửi nội dung tìm kiếm lên hệ thống. Hệ thống sẽ kiểm tra nội dung tìm kiếm trong kho dữ liệu bài viết. Nếu có sự trùng khớp với dữ liệu trong kho, hệ thống sẽ trả về kết quả tìm kiếm và bài viết cho người dùng. Nếu không có sự trùng khớp, hệ thống sẽ gửi phản hồi cho biết không có bài viết nào trên hệ thống phù hợp với yêu cầu tìm kiếm của người dùng.

Toàn bộ quá trình và luồng xử lý của chức năng quản lý bài viết được thể hiện ở sơ đồ luồng dữ liệu của chức năng quản lý bài viết hình 4.



Hình . Sơ đồ luồng dữ liệu của chức năng quản lý bài viết

### Xây dựng cơ sở dữ liệu

Các bảng cơ sở dữ liệu được sử dụng trong hệ thông như sau:

**NGUOIDUNG**( IDNguoiDung, IDKhoa, UserName, Password, HoTen, NamSinh, SDT, CCCD, QueQuan )

* *IDNguoiDung*: Đây là trường chứa IDmỗi người dùng trong hệ thống. Thông qua ID này, chúng ta có khả năng xác định và theo dõi từng người dùng một.
* *IDKhoa*: Trường này giúp xác định khóa của người dùng.
* *UserName*: Đây là trường lưu trữ tên đăng nhập của người dùng, mà họ sử dụng để truy cập hệ thống.
* *Password*: Trường này lưu trữ mật khẩu đăng nhập của người dùng, một thông tin cần được bảo mật một cách tối đa để bảo vệ tài khoản của họ.
* *HoTen*: Trường này lưu trữ tên đầy đủ của người dùng, bao gồm cả họ và tên.
* *NamSinh*: Trường NamSinh chứa thông tin về năm sinh của người dùng, giúp xác định độ tuổi và quản lý các tính năng liên quan đến năm sinh.
* *SDT* (Số Điện Thoại): Là trường lưu trữ số điện thoại của người dùng, thông tin quan trọng để có khả năng liên lạc và thông báo.
* *CCCD* (Số Căn Cước Công Dân): Trường này chứa thông tin về số căn cước công dân của người dùng, một tài liệu quan trọng để xác minh danh tính.
* *QueQuan*: Là trường dành cho thông tin về quê quán của người dùng.

**KHOA** ( IDKhoa , PK, SK, IDNguoiDung )

* *IDKhoa*: Là trường chứa ID của mỗi khóa.
* *Khóa Công Khai (PK):*Khóa bí công khai của người dùng IDNguoiDung.
* *Khóa Bí Mật (SK):* Khóa bí mật của người dùng IDNguoiDung.
* *IDNguoiDung*: Trường này xác định ID của người dùng sở hữu cặp khóa này.

**BAIVIET**( IDBaiViet, IDNguoiDang, NoiDung, Anh )

* IDBaiViet: Trường này chứa số ID của mỗi bài viết trong hệ thống, đảm bảo tính duy nhất của từng bài viết.
* IDNguoiDang: Trường này xác định người dùng đã đăng bài viết, kết nối bài viết với tài khoản người dùng cụ thể.
* NoiDung: Trường này chứa nội dung của bài viết, bao gồm văn bản hoặc thông tin chi tiết.
* Anh: Là một trường chứa đường dẫn hoặc thông tin về hình ảnh liên quan đến bài viết.

**FILE** ( IDFile, IDBaiViet, Link)

* IDFile: Đây là trường chứa ID của từng tệp, đảm bảo tính duy nhất của từng tệp.
* IDBaiViet: Trường này kết nối tệp với bài viết cụ thể thông qua ID của bài viết.
* Link: Chứa đường dẫn hoặc thông tin liên quan đến tệp đính kèm.

**LOAIBAIVIET**( IDBaiViet, IDNguoiDang, Link, LoaiBaiViet )

* IDBaiViet: Trường này kết nối loại bài viết với bài viết cụ thể thông qua ID của bài viết.
* NameLoaiBaiViet: Trường này chứa thông tin về tên loại bài viết.

1. HỆ MÃ HÓA CÓ THUỘC TÍNH ( ATTRIBUTE-BASED ENCRYPTION )

## Giới thiệu chung hệ mã ABE

Hệ mã ABE (Attribute-Based Encryption) là một loại mã hóa trong lĩnh vực mật mã và bảo mật dữ liệu, nơi quyền truy cập vào thông tin được kiểm soát dựa trên các thuộc tính thay vì sử dụng các khóa truy cập cụ thể. Hệ mã ABE đã xuất hiện như một công nghệ quan trọng trong việc bảo vệ thông tin và quản lý quyền truy cập, và nó đã được áp dụng rộng rãi trong nhiều lĩnh vực khác nhau.

## Phân loại

Hệ mã ABE (Attribute-Based Encryption) có hai biến thể chính: Ciphertext-Policy ABE (CP-ABE) và Key-Policy ABE (KP-ABE). Dưới đây là mô tả cụ thể về mỗi loại:

### Ciphertext-Policy ABE (CP-ABE):

Chính sách truy cập (Access Policy): Trong CP-ABE, chính sách truy cập được gắn liền với dữ liệu đã mã hóa. Điều này có nghĩa là mỗi tài liệu có một chính sách truy cập riêng. Chính sách có thể được biểu diễn bằng cách sử dụng các thuộc tính và toán tử logic như AND và OR. Ví dụ, một chính sách có thể yêu cầu người dùng có thuộc tính "Tuổi" lớn hơn hoặc bằng 18 và thuộc tính "Phòng ban" là "Kế toán" để có thể truy cập tài liệu.

Chìa khóa truy cập (Access Key): Người dùng tạo ra các chìa khóa truy cập dựa trên các thuộc tính của họ và chính sách truy cập của dữ liệu. Điều này có nghĩa là người dùng có thể truy cập các tài liệu phù hợp với chính sách truy cập được đặt bởi chìa khóa của họ.

***Ưu điểm của CP-ABE:***

Tính linh hoạt cao: CP-ABE cho phép người quản trị hệ thống xác định chính sách truy cập dựa trên các thuộc tính của người dùng và tài liệu. Điều này tạo ra một mô hình quản lý quyền truy cập mạnh mẽ và linh hoạt.

Chia sẻ tài liệu dễ dàng: CP-ABE cho phép người dùng chia sẻ tài liệu một cách an toàn với những người khác mà họ muốn, miễn là những người đó đáp ứng các yêu cầu về thuộc tính trong chính sách truy cập.

Bảo mật và quyền riêng tư: CP-ABE bảo vệ tính riêng tư của dữ liệu một cách hiệu quả. Người dùng chỉ có thể truy cập thông tin nếu họ có các thuộc tính phù hợp và chính sách truy cập cho phép.

Tích hợp với các hệ thống sẵn có: CP-ABE có thể tích hợp dễ dàng vào các hệ thống và ứng dụng hiện có mà không cần phải thay đổi quá nhiều cơ sở hạ tầng.

***Nhược điểm của CP-ABE:***

Phức tạp trong triển khai: Hệ thống CP-ABE thường phức tạp hơn trong việc triển khai và quản lý so với các hình thức mã hóa khác. Điều này đòi hỏi kiến thức chuyên sâu và sự quản lý khóa tốn công sức.

Hiệu suất: Việc mã hóa và giải mã dữ liệu CP-ABE có thể đòi hỏi nhiều tài nguyên tính toán hơn so với các hình thức mã hóa khác, đặc biệt là khi quyền truy cập có nhiều thuộc tính.

Quản lý khóa phức tạp: Quản lý và phân phối chìa khóa truy cập cho nhiều người dùng và nhiều tài liệu có thể trở nên phức tạp và đòi hỏi sự quản lý cẩn thận.

Khả năng đánh giá an toàn: Việc kiểm tra tính an toàn của hệ thống CP-ABE có thể khó khăn, và việc thiết lập các cơ chế kiểm tra an toàn hiệu quả có thể đòi hỏi nỗ lực lớn.

### Key-Policy ABE (KP-ABE):

Chính sách truy cập (Access Policy): Trong KP-ABE, chính sách truy cập được gắn liền với chìa khóa truy cập, chứ không phải với dữ liệu. Người quản trị hệ thống quyết định chính sách truy cập cho từng chìa khóa. Điều này có nghĩa rằng nhiều người dùng có thể chia sẻ cùng một chính sách truy cập chung.

Khóa truy cập (Access Key): Người quản trị hệ thống tạo ra các chìa khóa truy cập và đặt chính sách truy cập cho từng chìa khóa. Người dùng cần có chìa khóa phù hợp với chính sách để truy cập dữ liệu.

***Ưu điểm của KP-ABE:***

Quản lý quyền truy cập tập trung: KP-ABE cho phép người quản trị hệ thống xác định chính sách truy cập và kiểm soát chìa khóa chính sách. Điều này có nghĩa rằng quyền quản lý quyền truy cập được tập trung và quyết định quyền truy cập được đưa ra bởi người quản trị hệ thống.

Dễ quản lý và triển khai: So với CP-ABE, KP-ABE thường dễ quản lý và triển khai hơn. Người quản trị chỉ cần quản lý một số lượng chính sách truy cập thay vì phải tạo các chìa khóa truy cập cá nhân cho từng người dùng.

Bảo mật cao: KP-ABE cung cấp mức độ bảo mật cao đối với dữ liệu, vì quyền truy cập chỉ được cung cấp bởi chìa khóa chính sách và người quản trị có quyền kiểm soát chặt chẽ.

Tích hợp dễ dàng: KP-ABE có thể tích hợp dễ dàng vào các hệ thống và ứng dụng hiện có mà không cần phải thay đổi quá nhiều cơ sở hạ tầng.

***Nhược điểm của KP-ABE:***

Thiết lập chính sách phức tạp: Đôi khi việc thiết lập và quản lý chính sách truy cập trong KP-ABE có thể phức tạp và đòi hỏi sự hiểu biết chuyên sâu về cơ chế hoạt động của hệ mã ABE.

Tính linh hoạt thấp: So với CP-ABE, KP-ABE có tính linh hoạt thấp hơn đối với việc thay đổi quyền truy cập hoặc thêm/xóa người dùng, vì việc thay đổi chính sách thường đòi hỏi sự can thiệp của người quản trị.

Quản lý chìa khóa phức tạp: Mặc dù KP-ABE có thể dễ quản lý hơn trong việc quản lý chính sách, quản lý chìa khóa truy cập vẫn có thể trở nên phức tạp khi có nhiều người dùng và nhiều chính sách.

## Cách hoạt động của hệ mã ABE

Hệ mã ABE (Attribute-Based Encryption) hoạt động dựa trên các thuộc tính (attributes) để kiểm soát quyền truy cập và bảo vệ dữ liệu.

### Khởi tạo hệ thông ABE

Trước khi sử dụng hệ mã ABE, một người quản trị hệ thống cần thiết lập các tham số mật mã, bao gồm cấu hình của hệ thống và các thuộc tính sẽ được sử dụng để kiểm soát quyền truy cập. Dựa trên tham số an toàn λ, giải thuật tạo ra hệ thống gồm tối đa N thuộc tính, giả sử (p, G, GT, e) là một hệ thống bilinear maps, giải thuật chọn một phần tử sinh ngẫu nhiên g thuộc G, số mũ ngẫu nhiên a, α thuộc Zp, tạo N phần tử thuộc nhóm G tương ứng với N thuộc tính : h1, …, hN. Giả sử B là tập N thuộc tính trong hệ thống. Khóa bí mật dành cho Authority là :

*MSK* = gα

Khóa công khai của hệ thống là :

*Param* = (g, ga, e(g,g)α, h1, …, hN)

### Tạo khóa cho người dùng

Người dùng muốn truy cập dữ liệu cần phải có chìa khóa truy cập phù hợp. Chìa khóa này được tạo dựa trên các thuộc tính của người dùng. Người quản trị hoặc hệ thống tạo chìa khóa này và gán cho người dùng. Để tạo khóa cho người dùng hệ thông nhận đầu vào là người dùng u và tập thuộc tính tương ứng B(u), Authority với khóa bí mật MSK và khóa công khai param tạo khóa bí mật tương ứng cho người dùng u như sau :

**Key (u, B(u), MSK, param)**

Giả sử B(u) = A1, …, Ak, trong đó k ≤ N, chọn số ngẫu nhiên s\_u thuộc Zp, tính khóa bí mật du = (du0, du’0, du1, …, duk) trong đó :

du0 = gα. ga.s\_u,

du’0 = gs\_u,

du1 = h1s\_u, …, duk = hks\_u

Khi đó khóa bí mật sẽ là du, khóa công khai param.

### Mã hóa

Dữ liệu cần được bảo vệ được mã hóa bằng cách sử dụng chìa khóa mã hóa. Trong quá trình mã hóa, chính sách truy cập cũng được gắn kèm với dữ liệu. Chính sách này được biểu diễn bằng các thuộc tính và toán tử logic, ví dụ: "Người dùng phải có thuộc tính A và B để truy cập dữ liệu này". Đầu vào là bản rõ M, khóa công khai param, và chính sách β = (β1 V … V βm) trong đó mỗi βi là tập các thuộc tính. Bản mã bao gồm tập các phần tử ct = (BM, C, C0, C1, …, Cm) được tính như sau :

**Encryption(M, β, param)**

* Chọn số ngẫu nhiên s thuộc Zp.

|  |
| --- |
|  |

*Note :* Lưu ý rằng ct bao gồm cả .

### Giải mã

Để truy cập dữ liệu đã mã hóa, người dùng cần phải cung cấp khóa truy cập của họ. Hệ thống kiểm tra chìa khóa truy cập và so sánh với chính sách truy cập của dữ liệu. Nếu chìa khóa truy cập phù hợp với chính sách, người dùng có thể giải mã và truy cập dữ liệu.

**Decryption(ct, du, B(u), param) :** Tìm βk sao cho βk là tập con của B(u), tính :

|  |
| --- |
|  |

Khi này hệ file sẽ được giải mã.

1. CÀI ĐẶT TRƯƠNG TRÌNH
2. TỔNG KẾT