MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE ABDELHAMID IBN BADIS - MOSTAGANEM

Faculté des Sciences Exactes et d'Informatique

Département de Mathématiques et informatique

Filière : Informatique

RAPPORT DE MEMOIRE

Option : **Ingénierie des Systèmes d'Information**

THEME :

Conception et réalisation d'une application sécurisée pour la gestion de l'archive numérisée de l'université de Mostaganem

Etudiant(e) : « **Mokred Houari** »

Encadrant(e) : « Bahnes Nacéra »

Année Universitaire 2020-2021

Remerciements

Je voudrais tout d'abord exprimer mes plus profonds remerciements à mon encadreur **Pr. BAHNES Nacéra** pour son accord d'être mon encadreur et de sa disponibilité et son aide pendant toute la préparation de ce mémoire.

Je remercie ainsi **Mr l'examinateur** pour avoir accepté d'examiner ce mémoire de Master.

Je remercie tous les enseignants du département de mathématique et Informatique ainsi que le staff administratif et technique de la faculté. Tout spécialement **Mr Mokritar Nordine** responsable du centre de calcul de la faculté.

Je ne saurais oublier de remercier mes parents ainsi que l'ensemble de ma famille pour leur soutien moral, leurs encouragements et leur patience durant les étapes de réalisation de ce travail.

Enfin, Que tous ceux qui directement ou indirectement m'ont apporté leur aide, trouvent ici l'expression de mes sincères remerciements.

Résumé

L'archive est l'un des secteurs les plus importants dans lesquels nous devons accorder une attention particulière à tous les aspects, notamment dans le stockage des informations au niveau des universités.

Pour atteindre cet objectif, la numérisation des archives de l'université de Mostaganem est devenue une obligation, ce qui facilite le travail des archivistes en générale et les demandeurs des services de l'archive en particulier.

Dans ce mémoire, nous avons présenté la numérisation des archives et la sécurité des archives numériques au niveau des centres de l'archivage de l'Université de Mostaganem.

Nous avons réalisé une application sécurisé pour la numérisation de l'archive avec notre approche de sécurité qui consiste au cryptage des données au niveau de la base des données pour rendre les données inaccessible pour les Hackers.

Mots-clés:

Archive; archivage; numérisation; cryptographie, sécurité.

Abstract

The archive is one of the most important areas in which we must pay special attention to all aspects, especially in the storage of information at university level.

To achieve this goal, the digitization of the archives of the University of Mostaganem has become an obligation, which facilitates the work of archivists in general and applicants for archive services in particular.

In this mini project we talked about the digitization of archives and digital archive security at the archive centers of University of Mostaganem.

So we have made a secure application for Archive scanning with our security approach of Encrypting data at the database level to make the data inaccessible to hackers.

Keywords:

Archive; archiving; digitization; cryptography, safety.

Liste des figures

Liste des tableaux

Liste des abréviations

Abréviation	Expression Complète	Page
CIA	Conseil international des Archives	15
IDS	Intrusion Detection System	27
NIDS	Network Based Intrusion Detection System	27
HIDS	HostBased Intrusion Detection System	27
TCP/IP	Transmission Control Protocol/Internet Protocol	28

Table des matières

Introduction Générale

Le développement des technologies numériques dans les organisations conduit les professionnels des archives à repenser leurs méthodes de travail. Les compétences acquises dans la gestion des archives papier demeurent pertinentes dans de nombreux cas de figure, mais peuvent se décliner différemment dans la pratique.

L'archivage de documents et données numériques nécessite une adaptation des méthodes d'évaluation, de sélection, de tri, de collecte, d'organisation, de description, de communication et de conservation. De nouvelles compétences sont également indispensables, qu'elles soient techniques ou qu'elles concernent la gestion des archives. Il est essentiel de bien évaluer les charges dans les différents projets d'archivage électronique, voire le retour sur investissement car, en dehors des contraintes juridiques qui pèsent sur les organisations, les contraintes budgétaires constituent un élément fondamental pour construire une politique d'archivage efficace[1].

La numérisation des documents comporte de nombreux avantages que ce soit une plus grande accessibilité aux documents pour le personnel des établissements ou pour le public, la facilité d'exploitation des documents à des fins de recherche ou encore la préservation et la conservation des documents originaux. De plus, la numérisation doivent faire l'objet d'une veille technologique post-réalisation afin d'offrir toutes les garanties possibles en matière de pérennité et d'accessibilité (lisibilité) des documents numérisés.

[1] Editeur : Association des archivistes français, Collection : Les petits guides des archives 2e édition Parution : 01/2020, https://www.lgdj.fr/les-archives-electroniques-9782900175101.html (visité le 28/02/2021)

Ce rapport est organisé en trois chapitres :

Le premier chapitre nous avons présenté la numérisation des archives par définition ; type des archives ; numérisation des archives et les étapes de numérisation.

Le second chapitre illustre la sécurité des archives numériques par définition de la sécurité ; objectifs ; risques et les techniques de sécurité.

Le troisième chapitre une représentation générale de l'application et les outils utilisés pour le développement de cette application et la contribution proposée pour la sécurité de l'application.

Chapitre 1

Numérisation des archives

1.1 Introduction

La numérisation des documents est un moyen de diffuser ces documents de manière immatérielle. Au départ, il existe une image réelle, dessinée, imprimée ou photographiée sur papier, c'est le document, parfois vieux de plusieurs siècles, auquel on va donner une nouvelle vie. Il pourra se transmettre par des réseaux de communication «**web**», et être restitué à l'autre bout de la planète sans perte de qualité.

L'exemple le plus significatif est celui **des journaux**. Ainsi pour l'impression quotidienne, il fallait des tonnes de papier qui étaient distribuées aux coins du monde. Maintenant d'un simple clic, le fameux journal apparaît à l'écran du PC, tablette ou téléphone mobile[2].

1.2 Archive

1.2.1 Définition de l'archive

Le Conseil international des archives **(CIA)** donne une définition des archives en tant que documents : « Les archives sont l'ensemble des documents de toute nature, produits ou

[2] https://www.piaf-archives.org/sites/default/files/bulk_media/m09s2/section2_papier.pdf (visité le 11/03/2021)

reçus par une personne physique ou morale, par un organisme public ou privé, résultat de son activité, organisé en conséquence de celle-ci et conservés en vue d'une utilisation éventuelle»[3].

1.2.2 Les différentes types de l'archives

Les archives se différencient par rapport à leur degré d'utilisation et de manipulation par les structures émettrices. Elles sont, généralement de trois types.

1.2.2.1 Les archives courantes

Sont appelées « **archives courantes** » les documents qui sont d'utilisation habituelle pour l'activité des services qui les ont produits ou reçus. Ces documents sont conservés dans les services.

1.2.2.2 Les archives intermédiaires

Sont considérées comme « **archives intermédiaires** » les documents qui ne sont plus des documents courants et ne peuvent pas encore faire l'objet d'éliminations en raison de leur intérêt administratif et légal.

1.2.2.3 Les archives définitives

Sont considérées comme « **archives définitives** » les documents qui sont à conserver sans limitation de durée, après les opérations de tri et élimination (conservation obligatoire de documents publics).

[3] https://www.arcalys.com/archivage/les-archives-tentative-de-definition/ (visité le 20/02/2021)

1.3 Archivage

1.3.1 Définition de l'archivage

L'archivage est l'action d'archiver des documents. C'est l'ensemble des techniques et moyens employés pour recueillir, classer, conserver et exploiter des documents jusqu'à leur destruction éventuelle.

1.3.2 Les différente types d'archivages

Il existe en général deux types d'archivage: l'archive physique et l'archive numérique.

1.3.2.1 L'archivage physique

L'archivage physique est ce qu'on peut qualifier de solution traditionnelle. La technique consiste à faire le tri des pièces qui doivent être stockées, à les classer et à les ranger d'une manière structurée pour qu'il soit possible de les retrouver aisément en cas de besoins. Les documents classés peuvent alors être conservés au sein de la société ou au sein d'un site de conservation extérieur.

C'est pour cela qu'il est conseillé de s'adresser à des archivistes qualifiées pour vous aider à organiser et à structurer votre gestion documentaire pour vous permettre de gagner du temps et de l'espace pour augmenter votre efficacité tout en sécurisant vos informations au maximum[4].

1.3.2.2 L'archivage numérique

Les documents numériques ayant désormais la même valeur que les documents papiers, l'archivage numérique est venu concurrencer l'archivage physique. Cette technique est davantage pratique pour les moyennes et grandes entreprises qui ont un flux de documents plus important. Il s'agit en effet d'un stockage à long terme **des documents numérisés**

[4] https://lejournaldeleco.fr/news_abonnes/archivage-numerique-ou-archivage-physique-que-choisir (visité le 23/02/2021)

(images des archives physiques) ou **documents électroniques**[5] sur un support sécurisé. Si cette technique a de nombreux avantages dont le gain de temps, elle nécessite cependant l'élaboration d'une bonne stratégie en amont et une expertise qui tient compte entre autres de l'ensemble des normes à respecter[6].

1.4 Numérisation

1.4.1 Définition de la numérisation des archives

La numérisation d'archive consiste à convertir les archives papier en fichiers numériques; elle permet ainsi la dématérialisation des archives. La numérisation des documents d'archives permet de faciliter leur accessibilité, tout en évitant la détérioration, la dégradation ou la perte accidentelle des originaux.

1.4.2 Pourquoi numériser ?

La numérisation de documents permet de simplifier les échanges de fichiers, et les collaborateurs peuvent travailler ensemble sans tenir compte des distances physiques.

Alors les objectifs de numérisation des documents peuvent être de quatre **ordres**[7], soit :

1.4.2.1 La préservation des documents

La numérisation à des fins de préservation vise les documents dont le support est obsolète, qui présentent des altérations ou dont la manipulation peut causer une détérioration irréversible. Les documents originaux seront conservés, à moins qu'ils ne soient complètement irrécupérables. La copie numérisée constitue la copie de consultation privilégiée auprès des utilisateurs.

---

[5] Tout contenu conservé sous forme électronique, notamment un texte ou un enregistrement sonore, visuel ou audiovisuel.

[6] https://lejournaldeleco.fr/news_abonnes/archivage-numerique-ou-archivage-physique-que-choisir/ (visité le 23/02/2021)

[7] https://www.enssib.fr/bibliotheque-numerique/documents/64628-guide-de-gestion-d-un-projet-de-numerisation.pdf (visité le 25/02/2021)

1.4.2.2 La diffusion des documents

La numérisation à des fins de diffusion vise les documents qui seront utilisés dans le cadre d'un projet de diffusion telle une exposition ou pour rendre accessibles des documents aux utilisateurs sur place ou à distance. Les documents originaux seront conservés, mais, comme dans le cas précédent, la consultation se fera à partir de la copie numérisée.

1.4.2.3 La sauvegarde des documents

La numérisation à des fins de sauvegarde de documents vise essentiellement des documents d'une importance vitale pour les institutions (documents essentiels) et qui nécessitent la conservation d'un deuxième exemplaire, par mesure de précaution (copie de sécurité). Habituellement, cette copie de sécurité sera effectuée sur un support différent et, de préférence, conservée dans un autre lieu que les originaux. Les documents originaux seront conservés, mais la consultation se fera à partir de la copie numérisée.

1.4.2.4 La substitution des documents

La numérisation à des fins de substitution vise à rationaliser les coûts de conservation liés aux espaces et aux ressources matérielles nécessaires pour l'entreposage des documents. Elle vise également à faciliter l'accès et la consultation des documents. Les documents originaux seront éliminés une fois que ceux-ci auront été numérisés et qu'un contrôle de qualité en ait validé l'intégrité. Le recours à ce type de numérisation se répand de plus en plus dans les établissements universitaires, étant donné les problèmes de pénurie d'espace physique pour l'entreposage des documents dans les bureaux ou dans les dépôts de documents semi-actifs. Toutefois, la réalisation de ces projets doit être rigoureusement encadrée par des lois, des règlements et des normes afin de garantir la valeur de preuve des documents et leur pérennité.

1.4.3 Les étapes de la numérisation[8]

1.4.3.1 L'acquisition

Permettant la conversion du document papier sous la forme d'une image numérique (bitmap). Cette étape est importante car elle se préoccupe de la préparation des documents à saisir, du choix et du paramétrage du matériel de saisie (scanner), ainsi que du format de stockage des images.

1.4.3.2 Le prétraitement

Dont le rôle est de préparer l'image du document au traitement. Les opérations de prétraitement sont relatives au redressement de l'image, à la suppression du bruit et de l'information redondante, et enfin à la sélection des zones de traitement utiles.

1.4.3.3 La reconnaissance du contenu

Qui conduit le plus souvent à la reconnaissance du texte et à l'extraction de la structure logique. Ces traitements s'accompagnent le plus souvent d'opérations préparatoires de segmentation en blocs et de classification des médias (graphiques, tableaux, images, etc.).

1.4.3.4 La correction des résultats

Cette opération peut se faire soit automatiquement par l'utilisation de dictionnaires et de méthodes de correction linguistiques, ou manuellement au travers d'interfaces dédiées de la reconnaissance en vue de valider l'opération de numérisation.

1.5 Archive de l'université de Mostaganem

1.5.1 Présentation du siège

Le département des archives est situé au sous-sol de la Bibliothèque Centrale de l'Université de Mostaganem « **Site 3** » de l'ancien Institut d'agriculture (**ITA**).

[8] https://perso.esiee.fr/~najmanl/papers/numerisation.pdf (visité le 27/02/2021)

Il dispose de 03 bureaux et d'un entrepôt de grande capacité qui contienne l'archive, l'archive de l'université se compose d'un ensemble de documents produits par les sous-directions de la présidence de l'université et les dossiers des anciens étudiants diplômés, ainsi qu'aux journaux officiels.

1.5.2 Taille du bâtiment

La superficie totale du bâtiment d'archivage est de **10.318 m^2**, où le couloir a une longueur de 134 m ou une largeur de 77 m.

- L'entrepôt a une superficie de 68%.
- La salle de soins a une superficie de 12%.
- Bureau d'érudition a une superficie de 10%.
- Bureau d'arrangement d'équilibre a une superficie de 10%.

1.5.3 Les ressources matérielles de l'archive

matérielle	Nombre
Étagères en métal	48
Étagères mobiles	30
Boîtiers d'archives	4800
Bureau	03
Imprimante	01
Armoire	01
Ordinateur	06
Photocopieuse	01

Tableau 1 : Ressources Matérielles

1.5.4 Plan administratif du service de l'archives

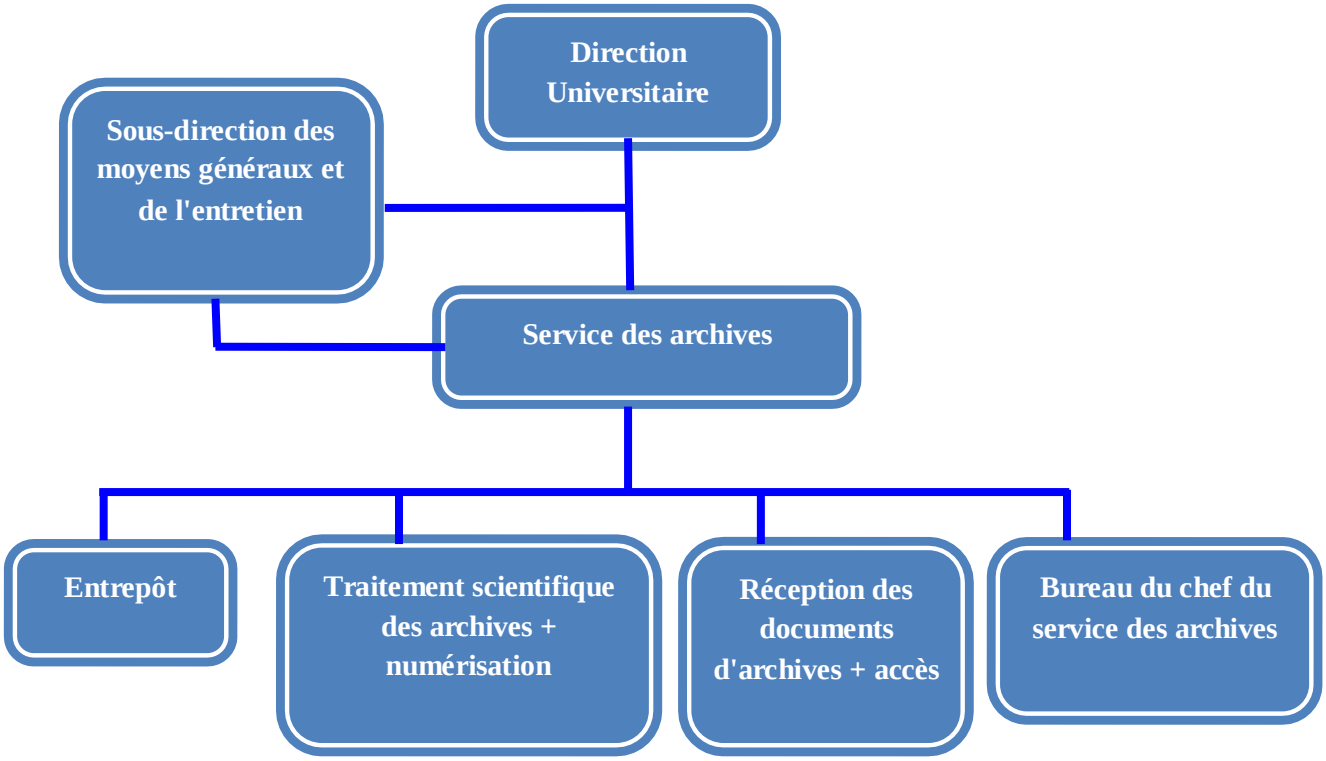

Figure 1 : Plan administratif de l'Autorité des archives

1.6 Conclusion

Dans ce chapitre, nous avons présenté les aspects théoriques des archives par la définition, les différents types d'archive et d'archivage par son définition, les types d'archivages. Après, nous avons entamé la numérisation des archives, ses objectifs et

les étapes de la numérisation. En dernière section du chapitre, nous avons donné un aperçu sur l'archive de l'université de Mostaganem par la présentation du siège et la taille du bâtiment, ressources matérielles de l'archive et le plan administratif du service de l'archive.

Chapitre 2

Sécurité des Archives Numériques

2.1 Introduction

Aujourd'hui, pour sécuriser son information, il faut certes raisonner en cycle de vie de l'information, document vital et preuve, mais aussi en métadonnées ou journal transactionnel. Records management[9] et archives ont pris acte de l'entrée de l'information dans l'ère de la trace. Il s'agit d'appréhender de nouveaux développements (blockchain[10], cryptographie) et défis (lutte contre la fraude documentaire, anonymisation des données personnelles, archivage dans le cloud[11]). L'archivage numérique, pour le privé comme pour le public, doit pouvoir évoluer sans risque[12].

2.2 Qu'est-ce qu'un archivage sécurisé ?

La sécurité du système d'archivage a pour objectif de protéger et valoriser l'information stockée. Cette dernière doit être sécurisée dès sa création ainsi qu'à travers les autres étapes du processus de conservation que sont le versement, l'enregistrement, la gestion et la restitution des documents.

---

[9] Un système de gestion de l'information consignée et organique documents ou données prouvant une activité, sous n'importe quel format.

[10] La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle

[11] Le cloud computing ou informatique en nuage est une infrastructure dans laquelle la puissance de calcul et le stockage sont gérés par des serveurs distants auxquels les usagers se connectent via une liaison Internet sécurisée

[12] https://www.archimag.com/le-kiosque/guides-pratiques/pdf/gp-57-58/securite-information-archivage-electronique (visité le 13/03/2021)

L'ensemble des modalités de conservation et de gestion des archives électroniques destinées à garantir leur valeur, notamment juridique, pendant toute la durée nécessaire. Le but de l'archivage sécurisé est de garantir et d'assurer l'intégrité, la pérennité, la sécurité et la confidentialité des documents

2.3 Pourquoi assurer un archivage sécurisé ?

L'évolution des technologies et des avantages liés aux nouveaux moyens de communication fait que les échanges électroniques et l'utilisation des nouvelles technologies prennent une place de plus en plus importante au sein de la société. Dès lors que les éléments concernés dans le cadre de la dématérialisation présentent une valeur juridique, une utilité pour la bonne gestion à long terme ou encore un intérêt historique, il y a une nécessité d'archiver. En particulier, seul un archivage électronique sécurisé permettra au juge d'apprécier la valeur juridique du document présenté, la conservation réalisée devant répondre aux exigences légales ou jurisprudentielles.

2.4 Risques et défis de l'archivage numérique[13]

Lorsqu'il est question de l'archivage des documents numériques, les archivistes ont souvent tendance à être négligents, ou à prendre pour acquis que les technologies sont infaillibles. En y ajoutant la relative nouveauté de la pratique, cela engendre de nombreux risques et défis dont il convient de tenir compte au moment de se lancer dans un processus d'archivage de nos fichiers. Alors nous avons recensés plusieurs risques qui guettent nos archives numériques :

2.4.1 Perte ponctuelle de fichiers :

Il peut nous arriver d'en effacer suite à une erreur de manipulation. Une mauvaise classification ou un oubli, par exemple du titre du fichier recherché, peut nous faire perdre la

[13] https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/11361/Dimitri-J-archives-perso.pdf (visité le 13/03/2021)

trace d'un document. Enfin, si un service en ligne que nous utilisons fait défaut, nous pouvons perdre les fichiers que nous y avions stockés.

2.4.2 Problèmes logiciels : Une panne ou un bogue d'un logiciel ou du système d'exploitation peuvent mettre en péril nos documents.

2.4.3 Problèmes matériels : Nos fichiers peuvent être corrompus suite à un crash de disque dur ou d'une altération de leur support ou nous égarons le support sur lequel sont stockés nos documents.

2.4.4 Sinistres : Nos fichiers peuvent disparaître à la suite d'un vol matériel, d'un incendie, d'une inondation ou d'un tremblement de terre.

2.4.5 Dégradations volontaires de la part d'un tiers : Un virus informatique, une dégradation intentionnelle ou une interception de notre mot de passe peuvent affecter nos fichiers.

2.4.6 Obsolescence : Les supports et les formats de fichiers peuvent ne plus être supportés par les technologies futures, ce qui rendrait impossible la lecture de nos documents.

2.4.7 Défection de services de sauvegarde sur Internet : La fermeture d'un fournisseur de services peut entraîner la perte des fichiers que nous y avions stockés.

2.4.8 Défaillances de confidentialité de services du Web : Nos documents laissés sur le Web peuvent être espionnés, et les mots de passe les protégeant peuvent être dérobés.

2.4.9 Changements liés à la santé des personnes : Un accident, une maladie ou un décès peuvent empêcher l'accès à nos fichiers ou nous empêcher de les transmettre à d'autres personne

2.5 Comment sécuriser un archive ?

L'archive numérique doit être sécurisé par un ensemble des techniques permettant de se prémunir contre les attaques et piraterie informatique, en interdisant la copie de contenus d'un support (logiciel) ou en rendant inutilisable toute intrusion dans le système de numérisation des archives physiques ou les archives numériques. Les systèmes de protection informatique les plus connus sont l'antivirus, le mot de passe, …etc.

2.5.1 Les anti-virus

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus informatiques ne sont qu'une catégorie). Ces derniers peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de logiciels modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur stockés sur l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur (le plus souvent ceux du système d'exploitation).

En effet, un virus est programmé de telle sorte qu'il signe le fichier dès qu'il est contaminé. Cette signature consiste en une suite de bits apposée au fichier. Cette suite, une fois décelée, permettra de reconnaitre le virus. Lorsque le virus est détecté par l'antivirus, plusieurs possibilités sont offertes pour l'éradiquer :

- Supprimer le fichier infecté ;
- Supprimer le code malicieux du fichier infecté ;
- Placer le ou les fichiers infectés en "quarantaine" pour un traitement futur.

Voici des exemples des anti-virus les plus populaires des PC and Serveurs : Avast Antivirus, AVG, Avira AntiVirus, NOD32, Kaspersky AntiVirus, Kaspersky Internet Security, etc.

2.5.2 Le mot de passe

Un mot de passe est un mot ou une série de caractères utilisés comme moyen d'authentification pour prouver son identité lorsque l'on désire accéder à un lieu protégé, à une ressource (**notamment informatique**) ou à un service dont l'accès est limité et protégé.

Le mot de passe doit être tenu secret pour éviter qu'un tiers non autorisé puisse accéder à la ressource ou au service. C'est une méthode parmi d'autres pour vérifier qu'une personne correspond bien à l'identité déclarée. Il s'agit d'une preuve que l'on possède et que l'on communique au service chargé d'autoriser l'accès. Quand il s'agit d'un code personnel, il vaut mieux utilisé l'expression « code confidentiel » pour mettre en évidence le caractère secret du code et responsabiliser son détenteur.

2.5.3 Les systèmes de détection d'intrusion[14]

Un système de détection d'intrusion (ou IDS : Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions. Les IDS, les plus connus selon leurs différentes catégories sont :

- **Les NIDS** (Network Based Intrusion Detection System), qui surveillent l'état de la sécurité au niveau du réseau ;
- **Les HIDS** (HostBased Intrusion Detection System), qui surveillent l'état de la sécurité au niveau des hôtes. Les HIDS sont particulièrement efficaces pour déterminer si un hôte est contaminé et les NIDS permettent de surveiller l'ensemble d'un réseau contrairement à un HIDS qui est restreint à un hôte.
- **Les IDS hybrides**, qui utilisent les NIDS et HIDS pour avoir des alertes plus pertinentes.

2.5.4 Pare-feu

Un pare-feu est un système ou un groupe de systèmes qui gère les contrôles d'accès entre deux réseaux. Ces dispositifs filtrent les trames des différentes couches du modèle

[14] https://hal.archives-ouvertes.fr/cel-01965300/document (visité le 04/03/2021)

TCP/IP[15] afin de contrôler leur flux et de les bloquer en cas d'attaques, celles-ci pouvant prendre plusieurs formes. Le filtrage réalisé par le pare-feu constitue la première défense de la protection du système d'information. Il peut être composé de périphériques comportant des filtres intégrés dont la fonction principale est de limiter et de contrôler le flux de trafic entre les différentes parties des réseaux.

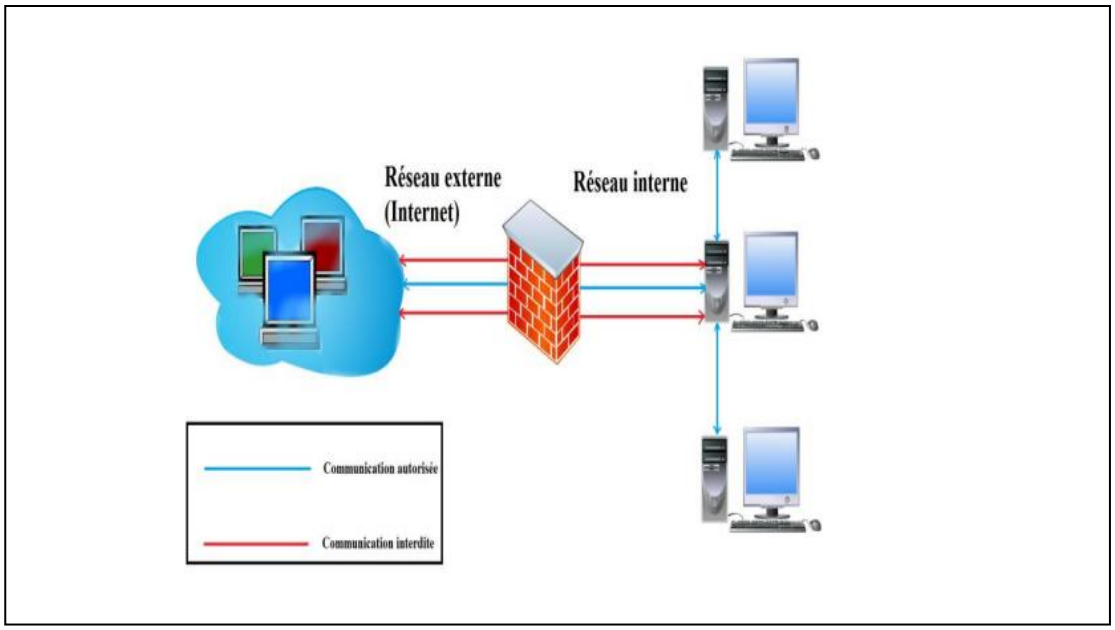

Figure 2 : Pare-feu

[15] Le **protocole TCP/IP est** un standard de communication entre deux processus. Il détermine et fixe les règles inhérentes à l'émission et à la réception de données sur un réseau

2.5.5 La cryptographie

2.5.5.1 Définition

Le terme cryptographie provient des deux mots grecs anciens « **Kruptos** » qui signifie « **cacher** » et « **graphein** » qui signifie « **écrire** »[16] (4). Ce qui signifie littéralement, « cacher l'écriture ». Le Petit Larousse donne la définition suivante : « Ensemble des techniques de chiffrement qui assurent l'inviolabilité de textes et, en informatique, de données»[17].

2.5.5.2 Cryptographie symétrique

La cryptographie symétrique (ou cryptographie à clé secrète) est la forme la plus ancienne de cryptographie. Ce chiffrement fonctionne en principe avec une clé secrète, bien qu'il existe certains chiffrements symétriques qui n'utilisent pas de clé, comme par exemple le chiffre de **César**[18].

Dans le cas des chiffrements avec clé, le principe est le suivant : L'émetteur du message chiffre les données grâce à une clé. Cette clé est généralement une chaîne de caractères. Le message est chiffré et sans la clé il est quasi impossible (le niveau d'impossibilité dépend du niveau de protection du chiffrement utilisé ainsi que de la complexité de la clé utilisée) de retrouver le message d'origine. L'émetteur doit donc transmettre la clé aux personnes à qui il désire transmettre le message s'il veut que son message puisse être lu.

[16] https://core.ac.uk/download/pdf/43671478.pdf (visité le 04/03/2021)
[17] https://www.larousse.fr/dictionnaires/francais/cryptographie/20864
[18] https://www.cryptage.org/outil-crypto-cesar.html (visité le04/03/2021)

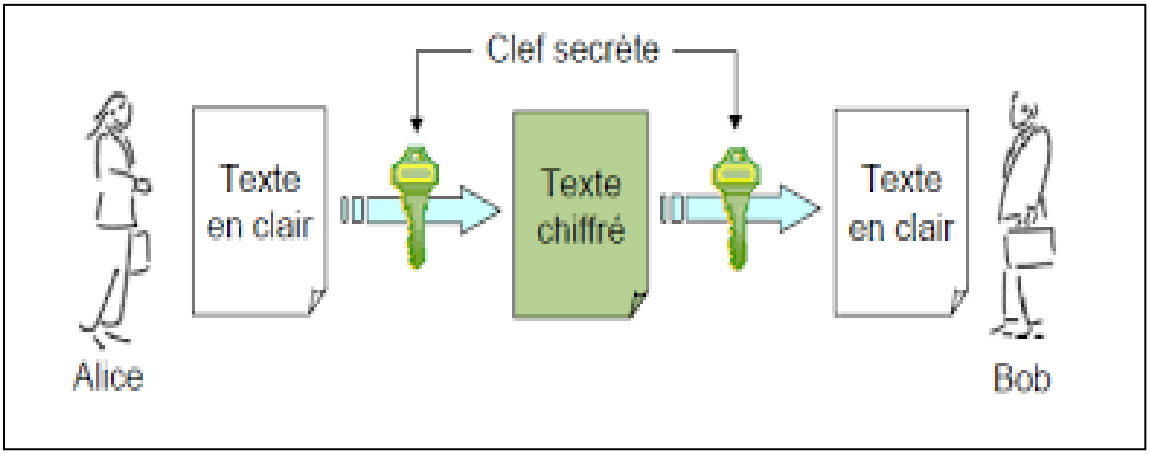

Figure 3 : Schéma de fonctionnement de la cryptographie symétrique

2.5.5.3 Cryptographie asymétrique[19]

La cryptographie asymétrique ou cryptographie à clé publique fonctionne de façon totalement différente à la cryptographie symétrique. Si l'on peut comparer la cryptographie symétrique à un coffre-fort auquel seules les personnes possédant la clé peuvent accéder, la cryptographie asymétrique pourrait être comparée à une boite aux lettres dans laquelle on peut déposer des informations, et seule la personne possédant la clé peut accéder au contenu de la boîte. La boite aux lettres serait la clé publique (donc accessible à tout le monde), alors que la clé pour ouvrir la boite serait la clé privée. En effet, dans la cryptographie asymétrique, il y a une clé publique et une clé privée.

Les nombres premiers sont l'élément clé pour rendre les algorithmes de cryptographie asymétrique indéchiffrables (ou presque). En prenant comme exemple la multiplication de 5 x 7, il est assez facile de répondre instantanément 35.

L'opération inverse, à savoir, retrouver 35 à partir de facteurs premiers est assez facile. Cependant, factoriser 1591 par exemple, est beaucoup plus compliqué, alors que

[19] https://core.ac.uk/download/pdf/43671478.pdf (visité le 04/03/2021)

calculer 37 x 43 se fait très facilement. C'est sur cette difficulté de factorisation que se reposent les algorithmes asymétriques[20].

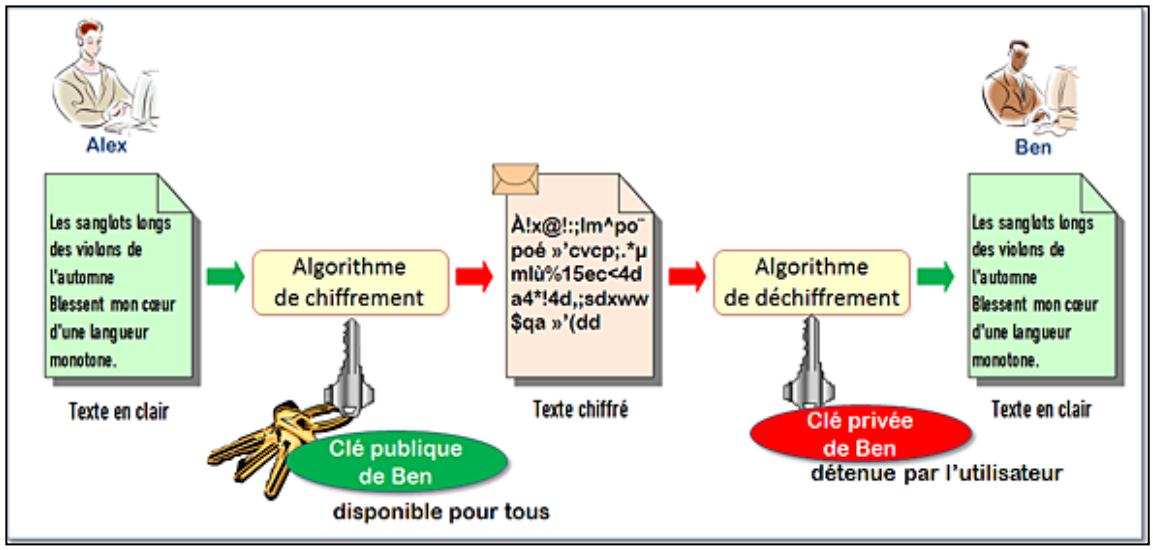

Figure 4 : Schéma de fonctionnement de la cryptographie asymétrique

2.5.5.4 Hachage[21]

Les fonctions de hachage permettent de chiffrer un message sous la forme d'une chaîne de caractères de taille fixe, peu importe la taille du message d'origine, généralement entre 128 et 512 bits. Elles sont comparables à une empreinte, car un message aura toujours la même empreinte en appliquant une fonction de hachage. Elles sont à sens unique, ce qui signifie qu'il est facile de hacher un message, mais qu'il n'est en principe pas possible de calculer son inverse, à moins d'utiliser une méthode de force brute. Pour qu'une fonction de hachage soit sûre, elle doit être résistante aux collisions. En partant du principe qu'il y a une infinité de messages possibles pouvant être chiffrés, il est évident que plusieurs messages

[20] https://core.ac.uk/download/pdf/43671478.pdf (visité le 04/03/2021)
[21] https://core.ac.uk/download/pdf/43671478.pdf (visité le 04/03/2021)

vont donner le même résultat une fois hachés. La résistance est le fait que les collisions ne puissent pas être retrouvées.

2.5.5.5 Cryptographie quantique

La cryptographie quantique se base sur les propriétés de la mécanique quantique. Plutôt que d'essayer de chiffrer des données afin qu'elles soient incompréhensibles, la communication est arrêtée si un message a été intercepté. C'est donc de cette façon que fonctionne la cryptographie quantique. Selon le principe d'incertitude d'Heisenberg[22], si un objet quantique (dans ce cas, un photon circulant dans une fibre optique) a été observé alors il a été modifié et donc la communication est coupée. Le papier « La cryptographie quantique en bref » résume ce type de cryptage avec un exemple : Un joueur de tennis lance avec sa raquette, des balles contenant chacune un message. Si une personne souhaite intercepter les balles, elle pourrait le faire. Mais si au lieu de lancer des balles, le joueur de tennis lançait des bulles en savon ? Dans ce cas-là, si quelqu'un tente de les intercepter, elles exploseraient sur le coup car elles sont fragiles[23].

[22] https://fr.wikipedia.org/wiki/Principe_d%27incertitude (visité le 04/03/2021)
[23] https://core.ac.uk/download/pdf/43671478.pdf (visité le 04/03/2021)

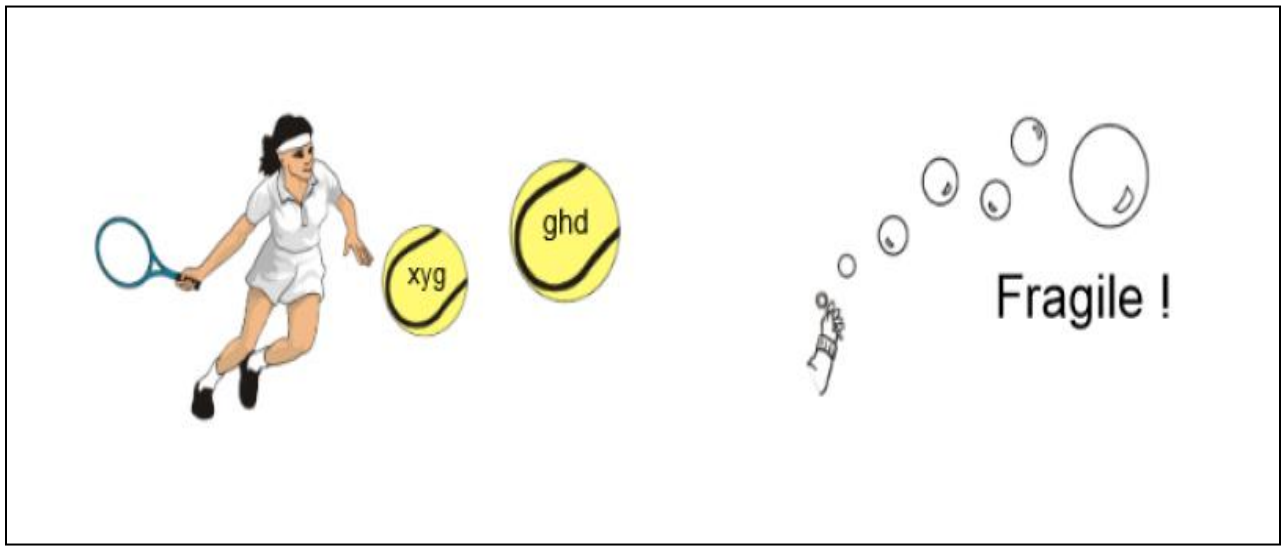

Figure 5 : Illustration du fonctionnement de la cryptographie quantique

2.6 Conclusion

Dans ce chapitre, nous a permis en premier lieu de découvrir la sécurité des archives numérique par définition, objectives de la sécurité , les risques et les déférentes technique proposées pour la sécurité des archives numérique comme les anti-virus, le mot de passe, les systèmes de détection d'intrusion, Pare-feu, et la cryptographie.

Chapitre 3

Conception et Réalisation

de l'Application

3.1 Introduction

Dans ce chapitre, nous aborderons les outils et le langage utilisé pour la réalisation de ce projet et nous allons présenter les différentes étapes, à savoir la conception et la réalisation de notre application en passant des diagrammes UML à la programmation avec PHP et Mysql.

3.2 Présentation de l'application

Cette application, que nous avons développé pour la numérisation des archives de l'Université de Mostaganem, est un logiciel de suivi complet de document archivé de l'administration universitaire jusqu'au la numérisation de ces papiers qui peut durer une langue temps. Le but principal étant de faciliter la recherche de l'information spécifique à chaque étudiant ou enseignant afin de prendre leurs documents administratifs.

3.3 Présentation des outils utilisés

3.3.1 Pour la conception

- **UML** (Unified Modeling Langage) **:** Durant de la phase d'analyse, on suivi comme processus de démarche orienté objet.

- **ArgoUML** : est un logiciel de création de diagrammes UML sous licence libre et programmé en Java et donc multi-systèmes. Nous utilisons la version on ligne (Free Online UML Tools)

3.3.2 Pour la programmation

- **PHP**[24] **:** Le PHP, pour Hypertext Preprocessor, désigne un langage informatique, ou un langage de script, utilisé principalement pour la conception de sites web dynamiques. Il s'agit d'un langage de programmation sous licence libre qui peut donc être utilisé par n'importe qui de façon totalement gratuite. Créé au début des années 1990 par le Canadien et Groenlandais Rasmus Lerdorf, le langage PHP est souvent associé au serveur de base de données MySQL et au serveur Apache. Avec le système d'exploitation Windows, il fait partie intégrante de la suite des logiciels libres XAMPP.

- **MySQL**[25] : est un système de gestion de bases de données relationnelles (SGBDR) . Il fait partie des logiciels de gestion de base de données les plus utilisés au monde, autant par le grand public (application web principalement) que par des professionnels, en concurrence avec Oracle, et PHP MySQL. MySQL est capable, depuis la version3.1.3 d'utiliser un système de réplication à sens unique relativement simple à mettre en place : un serveur maitre qui contient la base de données source et va recevoir l'ensemble des modifications, et un serveur esclave qui contient une base

[24] https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203597-php-hypertext-preprocessor-definition/ (visité le 31/08/2021)
[25] http://dspace.univ-tlemcen.dz/bitstream/112/13167/1/Ms.GBM.Marouf%2BMahamdaoui.pdf (visité le 31/08/2021)

à structure identique et qui va se connecter au serveur maitre pour aller chercher les nouvelles modifications et mettre à jour ses bases. Un maitre peut avoir plusieurs esclaves, et un esclave peut devenir à son tour maitre pour un autre serveur esclave, réalisant ainsi une chaine de réplication. Toutes les modifications (UPDATE, DELETE, INSERT. . .)doivent être envoyées au serveur maitre et seront automatiquement répercutées sur ses esclaves, mais les requêtes de recherche (SELECT), souvent plus nombreuse et plus gourmand en pourront être effectuées sur un ou plusieurs esclaves. Comme les requêtes de modification doivent être redirigées sur le serveur maitre, La conception de l'application doit s'adapter à l'architecture : le programmeur va ouvrir deux connexions dans son programme, une sur le serveur maitre, sur lequel il exécutera toutes ses recherches.

3.4 Analyse des besoins

3.4.1 Identification des acteurs

La numérisation des archives est l'une des méthodes scientifique les plus innovantes dans le domaine d'archivage. Un acteur représente un rôle joué par une personne externe ou par un processus qui interagit avec le système. Dans notre système les acteurs principaux est :

- **Chef service:** est un professionnel de l'archive titulaire d'un diplôme d'archive **(Master)** avec la fonction **chef de service.** C'est la personne qui s'occupe de la gestion administrative de l'archive.

- **L'archiviste :** est un professionnel de l'archive titulaire d'un diplôme d'archive. C'est la personne qui s'occupe du traitement et la numérisation des archives.

3.4.2 Les besoins fonctionnels

Ce sont les exigences de l'archiviste spécifiant un comportement d'entrée et sortie du système. Les besoins fonctionnels des différents acteurs peuvent être résumés comme suit :

- L'assurance de la numérisation des archives des fiches administratives.

- Consulter les dossiers numériser des archivons.

3.4.3 Les besoins non fonctionnels

Ce sont des besoins relier avec la performance du système, la facilité d'utilisation, l'ergonomie des interfaces, la sécurité. Parmi ses besoins nous citons :

- Accès à l'application via l'authentification.
- Simplicité et ergonomie de l'interface graphique.
- Performance du système en temps de réponse : stockage mémoire, suppression.....
- La performance de la recherche des informations des archivons.

3.4.4 Identification des cas d'utilisation

Chaque service offre par le système est modélisé par cas d'utilisation qui exprime l'interaction acteurs/système. Pour chaque acteur identifié il convient de rechercher les différentes intentions (métier) selon lesquelles il utilise le système ce qui représente les cas d'utilisation.

Le tableau suivant illustre l'ensemble des cas d'utilisation nécessaires pour le bon fonctionnement du système.

N	Cas d'utilisation	Affichage de l'interface principale
01	Authentification	Chef de service archive, Archiviste,
02	Crée des comptes **Utilisateur**	Chef de service archive
03	Ajouter, Supprimer, Modifier, Rechercher	Chef de service archive, Archiviste,

Tableau 2 : identification des cas d'utilisation

3.5 Les Diagrammes

3.5.1 Diagramme de cas d'utilisation

Le diagramme suivant résume les différentes interactions entre les utilisateurs (les acteurs) et les différentes parties du système.

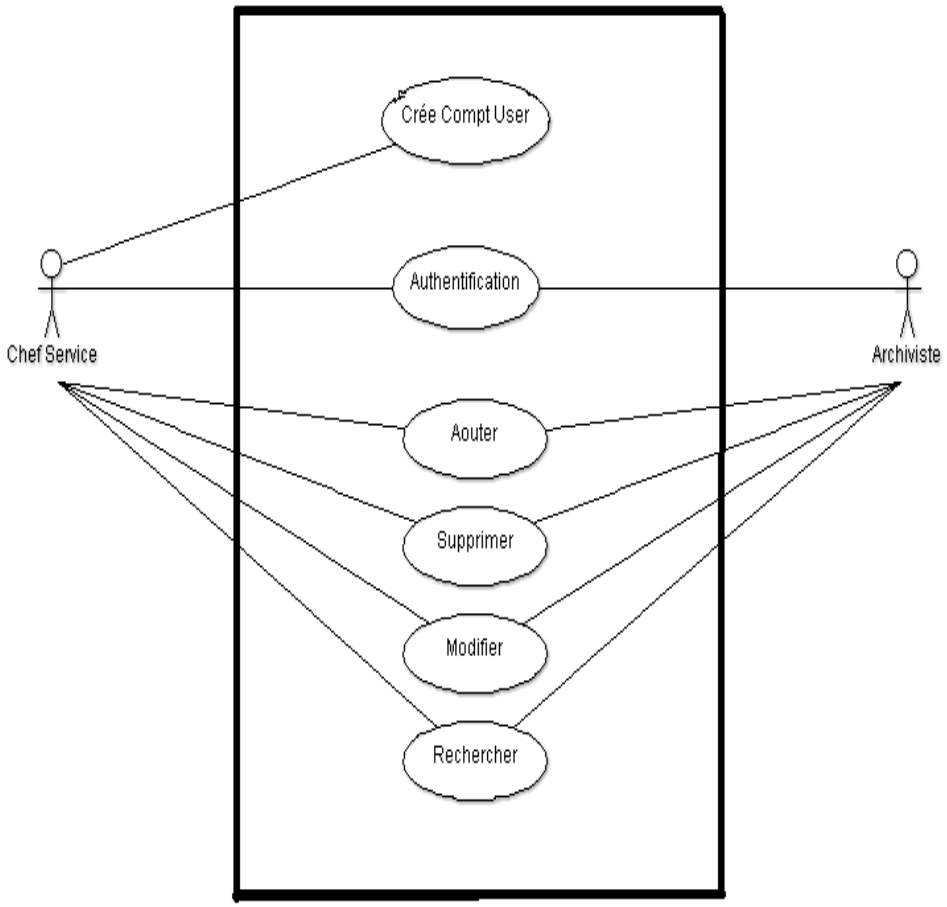

Figure 6 : Diagramme de cas d'utilisation

3.5.2 Diagramme de séquence

3.5.2.1 Diagramme de séquence du cas d'utilisation « Authentification »

Un utilisateur doit s'authentifier en saisissant ses propres coordonnées (Nom d'utilisateur et mot de passe), puis le système procède à la vérification des informations introduites pour les comparer avec les données stockées dans la base de données, si l'une des coordonnées est erronée, le système affiche un message d'erreur (Nom d'utilisateur et mot de passe Incorrect) sinon l'accès est autorisé.

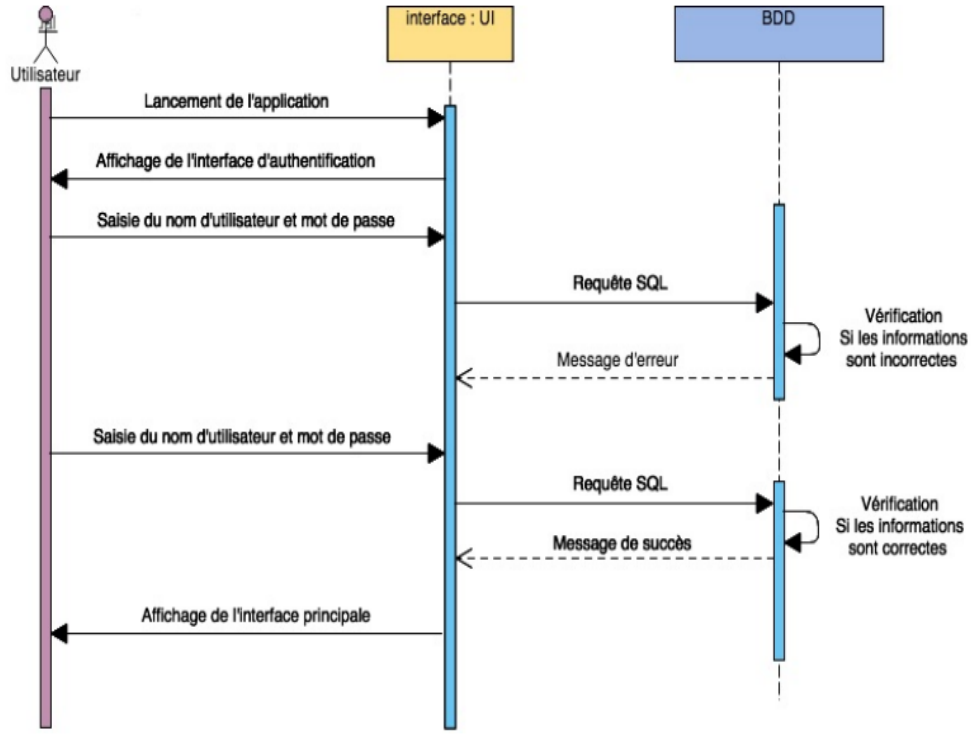

Figure 7 : Diagramme de séquence « Authentification »

3.5.2.2 Diagramme de séquence du cas d'utilisation « Crée Compte User »

Après que le chef de service soit authentifié et accédé à l'application, il remplit le formulaire en ajoutant un Compte User pour l'Archiviste **(Nom de Compte et Mots de Passe)**, le système doit vérifier si le compte existe, le système affiche Message d'erreur **(Compte existe déjà)** si nom le système enregistre **Compte User.** Le diagramme de séquence trouvé dans la figure suivante résume les étapes nécessaires pour de la création d'un compte User.

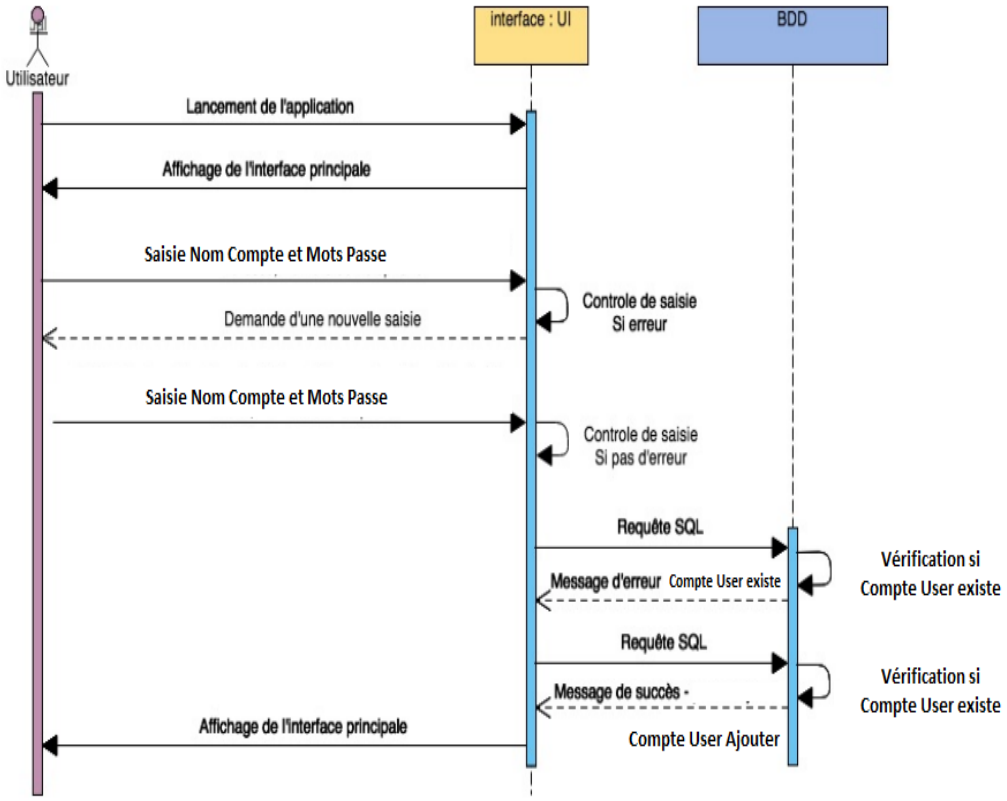

Figure 8 : Diagramme de séquence de cas d'utilisation Crée Compte User

3.5.2.3 Diagramme de séquence du cas d'utilisation « Ajouter Archivons »

La figure 9 présente le diagramme de séquence pour l'ajout un archivons. Après que l'Archiviste soit connecté, il remplit le formulaire en ajoutant un Archivons, le système doit vérifier la saisie ainsi que l'existence de l'Archivons.

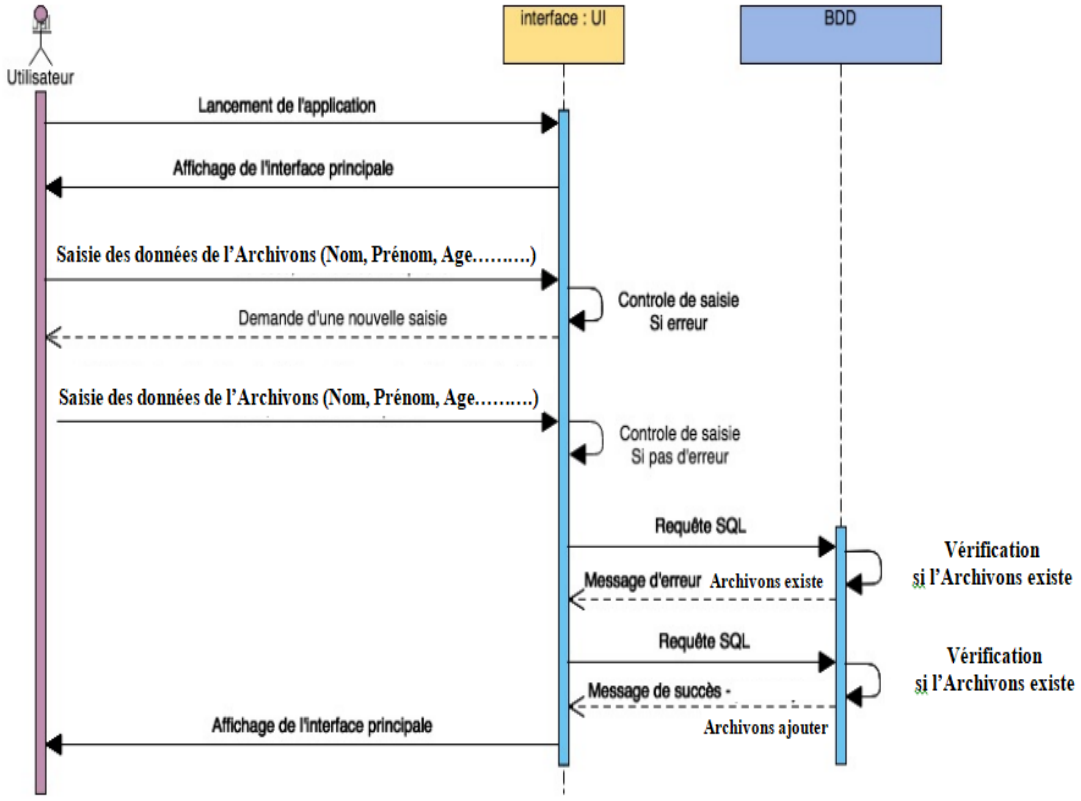

Figure 9 : Diagramme de séquence de cas d'utilisation « ajouter Archivons »

3.5.2.4 Diagramme de séquence du cas d'utilisation « Recherche Archivons»

Afin d'accéder au dossier l'Archiviste doit effectuer une recherche, remplir le champ de recherche en introduisant soit le nom, prénom ou ID et valide. Le système doit vérifier la saisie ainsi que l'existence de l'Archivons (voir le diagramme présenté dans la figure 10).

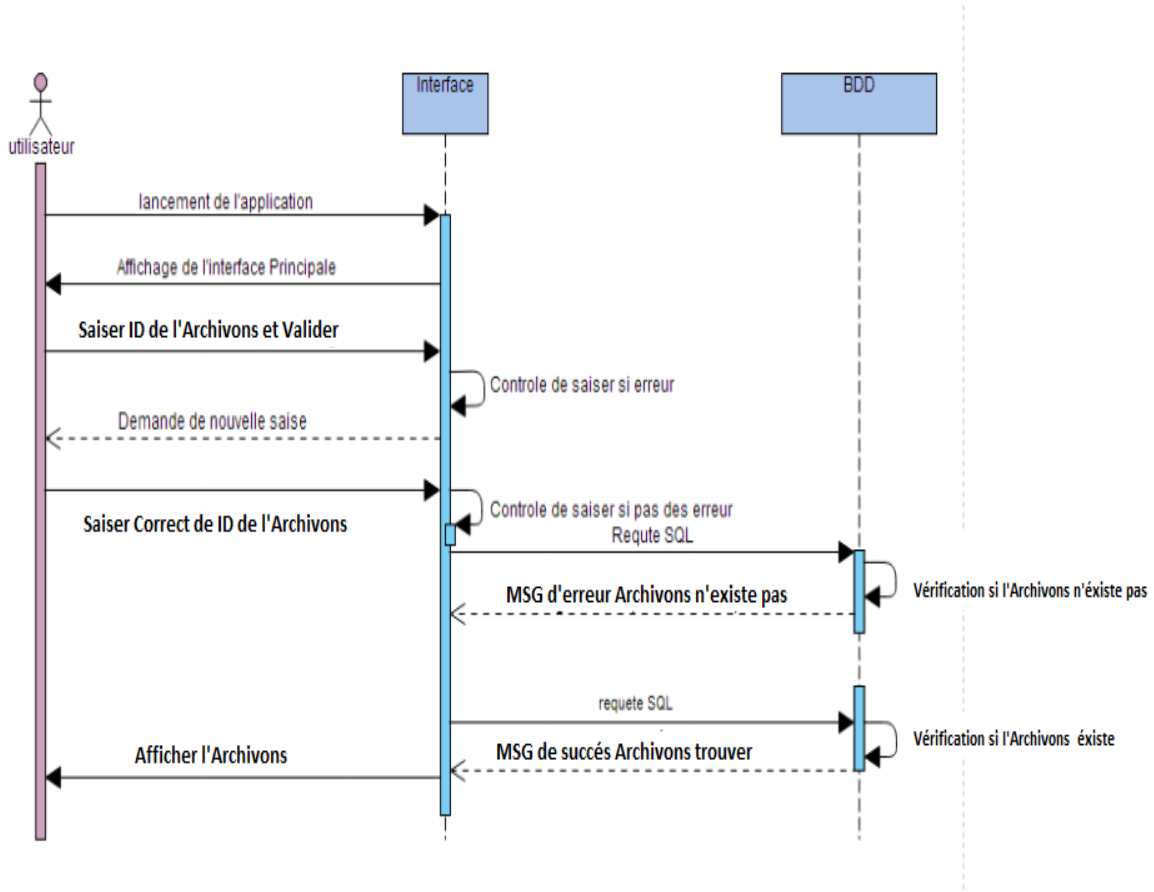

Figure 10 : Diagramme de séquence de cas d'utilisation « Recherche Archivons »

3.5.2.5 Diagramme de séquence du cas d'utilisation « Modifier Archivons»

La modification d'un Archivons se fait par l'Archiviste, sélectionne l'Archivons concerné et fait la modification. Le système doit afficher un message de confirmation de modification et fait la mise à jour comme montré dans la figure 11.

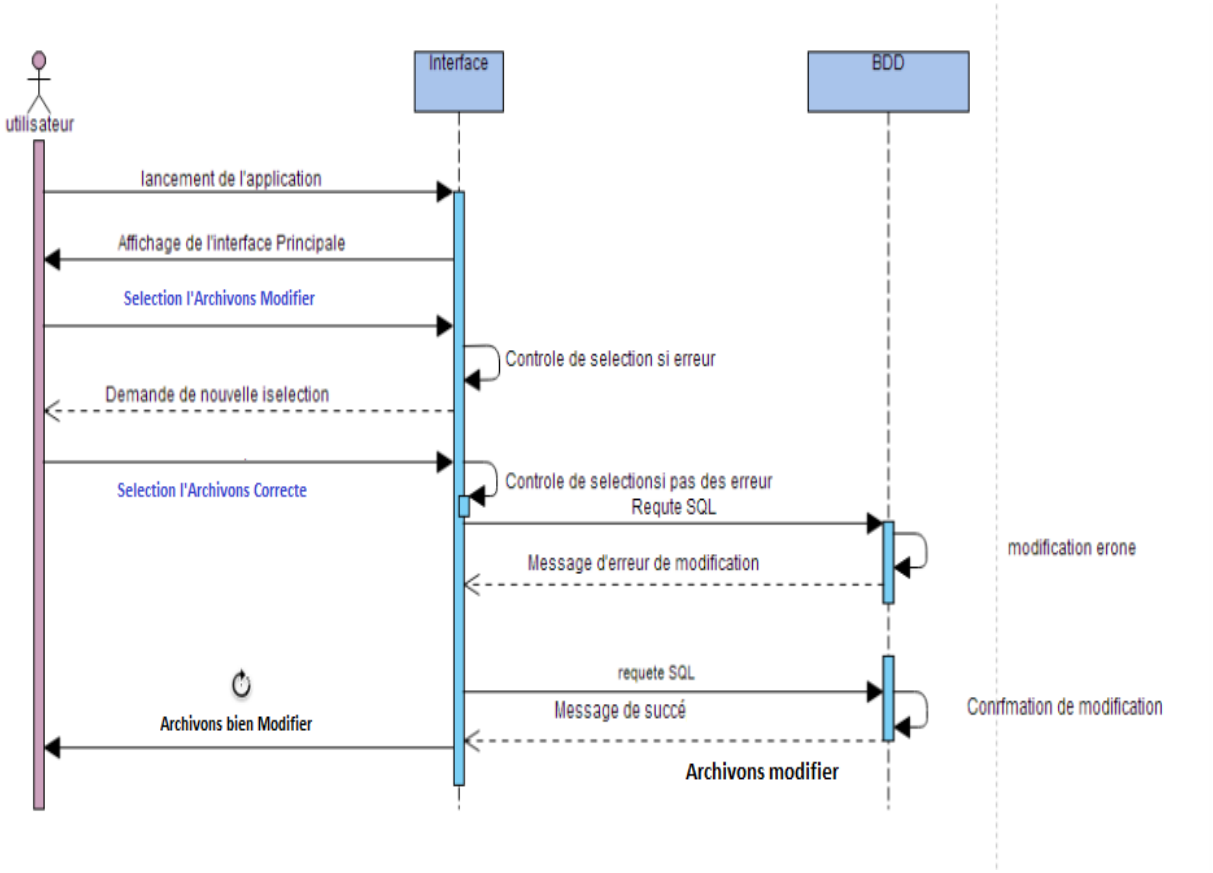

Figure 11 : Diagramme de séquence de cas d'utilisation « Modifier Archivons »

3.5.2.6 Diagramme de séquence du cas d'utilisation « Supprimer Archivons»

Pour supprimer un Archivons, il faut d'abord sélectionner l'Archivons et valider. Une Message sera afficher pour confirmer la suppression ou annuler, après la confirmation le système effectue une mise à jour.

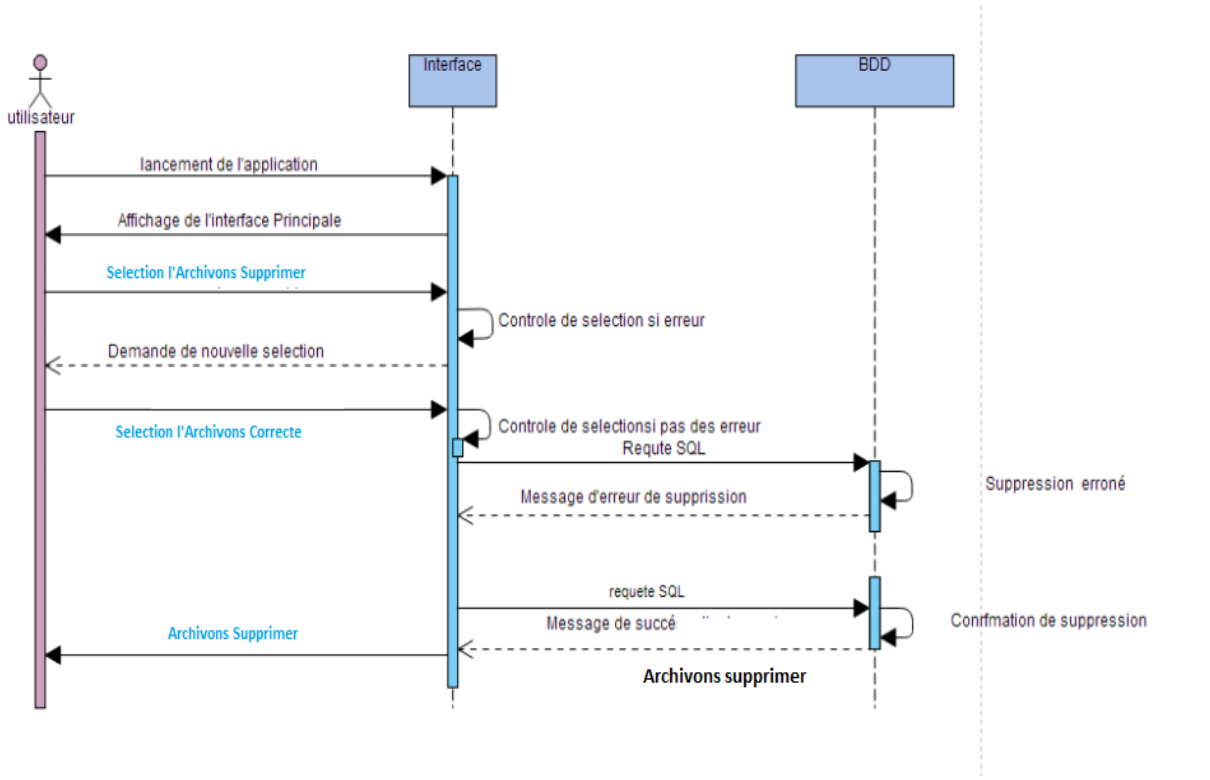

Figure 12 : Diagramme de séquence de cas d'utilisation « Supprimer Archivons »

3.5.3 Diagramme de classe

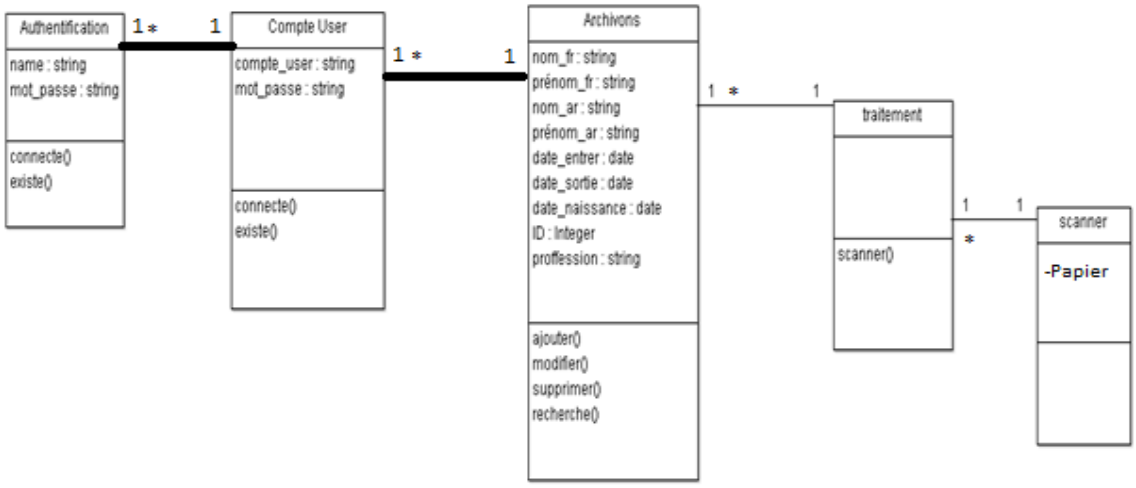

Figure 13 : Diagramme de classe

3.6 La sécurisation de l'application par Chiffrement

Pour sécuriser notre application, nous proposons le chiffrement de la base des données, par la sécurité des colonnes spécifiques dans la base de données. Par exemple, les mots de passes de compte utilisateur on pourrait vouloir chiffrer et on peut aussi chiffrer une colonne contenant les noms et les prénoms des archivons tout en laissant les autres données en claire

3.6.1 Présentation de openSSL[26]

- **Protocole SSL**

Le protocole SSL (Secure Socket Layer) a été développé par la société Netscape Communications Corporation pour permettre aux applications client/serveur de communiquer de façon sécurisée. TLS (Transport Layer Security) est une évolution de SSL réalisée par l'IETF[27].

La version 3 de SSL est utilisée par les navigateurs tels Netscape et Microsoft Internet Explorer depuis leur version 4.

SSL est un protocole qui s'intercale entre TCP/IP et les applications qui s'appuient sur TCP. Une session SSL se déroule en deux temps

1. une phase de poignée de mains (handshake) durant laquelle le client et le serveur s'identifient, conviennent du système de chiffrement et d'une clé qu'ils utiliseront par la suite.

2. la phase de communication proprement dite durant laquelle les données échangées sont compressées, chiffrées et signées.

L'identification durant la poignée de mains est assurée à l'aide de certificats X509[28].

- **openSSL**

openSSL est une boîte à outils cryptographiques implémentant les protocoles SSL et TLS qui offre

[26] https://lig-membres.imag.fr/prost/M1_MEEF_NSI/openssl.html visité le 13/09/2021

[27] **L'Internet Engineering Task Force**, élabore et promeut des standards Internet, en particulier les standards qui composent la suite des protocoles Internet. **L'IETF** produit la plupart des nouveaux standards d'Internet.

[28] est un fichier numérique qui est utilisé pour Secure Sockets Layer (SSL) ou Transport Layer Security (TLS)

1. une bibliothèque de programmation en C permettant de réaliser des applications client/serveur sécurisées s'appuyant sur SSL/TLS.

2. une commande en ligne (openssl) permettant

- la création de clés RSA, DSA (signature)
- la création de certificats X509
- le calcul d'empreintes (MD5, SHA, RIPEMD160, ...)
- le chiffrement et déchiffrement (DES, IDEA, RC2, RC4, Blowsh, ...)
- la réalisation de tests de clients et serveurs SSL/TLS
- la signature et le chiffrement de courriers (S/MIME)

3.6.2 Advanced Encryption Standard (AES[29])

Le chiffrement AES (Advanced Encryption Standard) est l'algorithme de chiffrement le plus utilisé et le plus sûr disponible aujourd'hui. Ouvert au public, **la NSA** l'utilise pour chiffrer ses documents qui portent le sceau **"secret défense."**

L'histoire de l'AES a débuté en 1997 lorsque le **NIST (National Institue of Standards and Technology)** décide de trouver un successeur à un algorithme plus ancien, le **DES (Data Encryption Standard)**. Ce nouvel algorithme se nomme **Rijndael** en l'honneur de ses créateurs, les chercheurs Belges **Daemen et Rijmen**. L'AES est beaucoup plus sûr et flexible que son prédécesseur.

Cet algorithme est officiellement devenu la norme de cryptage AES après sa victoire sur ses concurrents lors d'une compétition internationale organisée en 2001. Fondé sur des entrées permutées selon une table définie au préalable, l'algorithme offre des tailles de blocs et de clés qui sont des multiples de 32 (compris entre 128 et 256 bits).

Ces différentes opérations sont répétées plusieurs fois et définissent un «tour». A chaque tour, une clé unique est calculée à partir de la clé de cryptage et incorporée dans les

[29] https://www.boxcryptor.com/fr/encryption/ (visité le 13/09/2021)

calculs. L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait donc entre 128, 192 ou 256 bits.

De ce fait, l'AES remplace l'algorithme DES qui utilisait des clés de 56 bits seulement. Craquer une clé AES de 128 bits avec un ordinateur prendrait plus de temps que l'âge présumé de l'univers. **Boxcryptor** n'utilise que des clés de 256 bits. L'algorithme AES reste la norme de cryptage préférée pour les gouvernements, les banques et de nombreux systèmes de sécurité dans le monde.

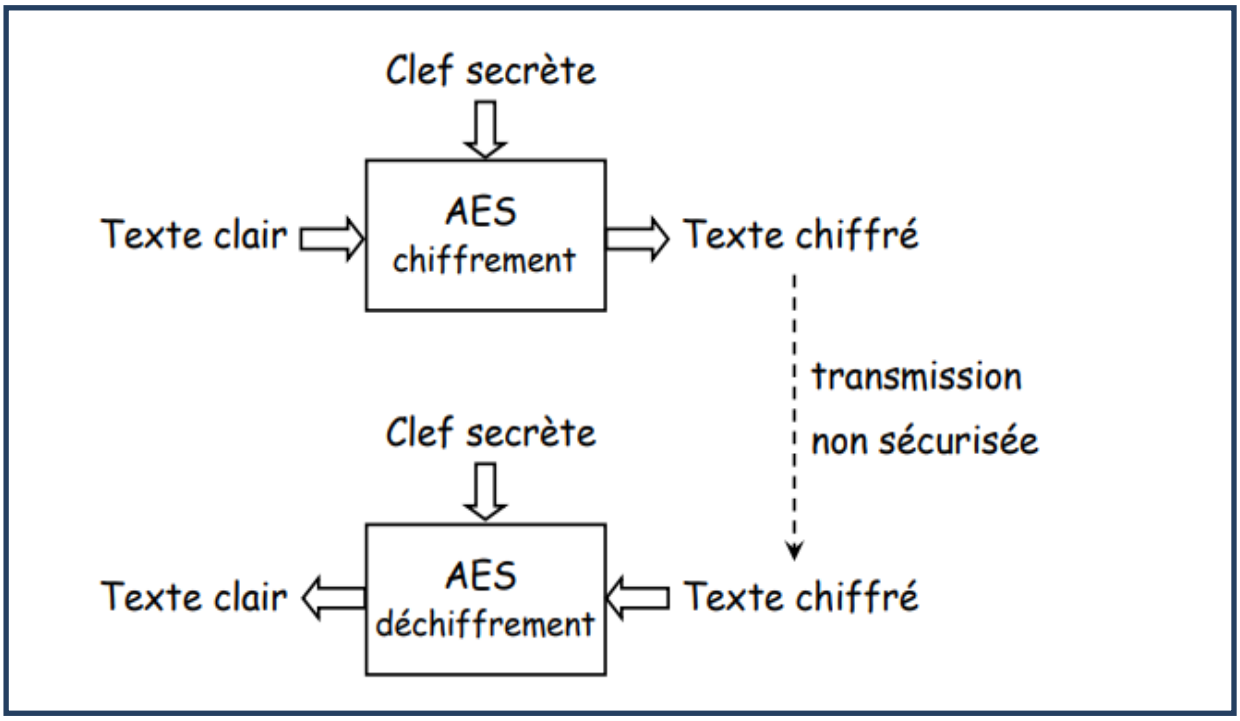

Figure 14: schéma de l'algorithme AES

[https://www.emse.fr/~dutertre/documents/synth_AES128.pdf]

3.7 Contribution

Dans le cadre de ce projet, nous proposons une méthode permettant de renforcer la sécurité des informations qui sont destinées à être enregistrer dans la base de données par l'utilisation du **(openssl)** la boite à outils cryptographiques implémentant les protocoles SSL et TLS pour sécuriser le transfert des données et le cryptage des données au niveau de la base de données avec la fonction de cryptage symétrique **AES** de type **« AES-128-ECB »** avec une clef secrète **« hello ».**

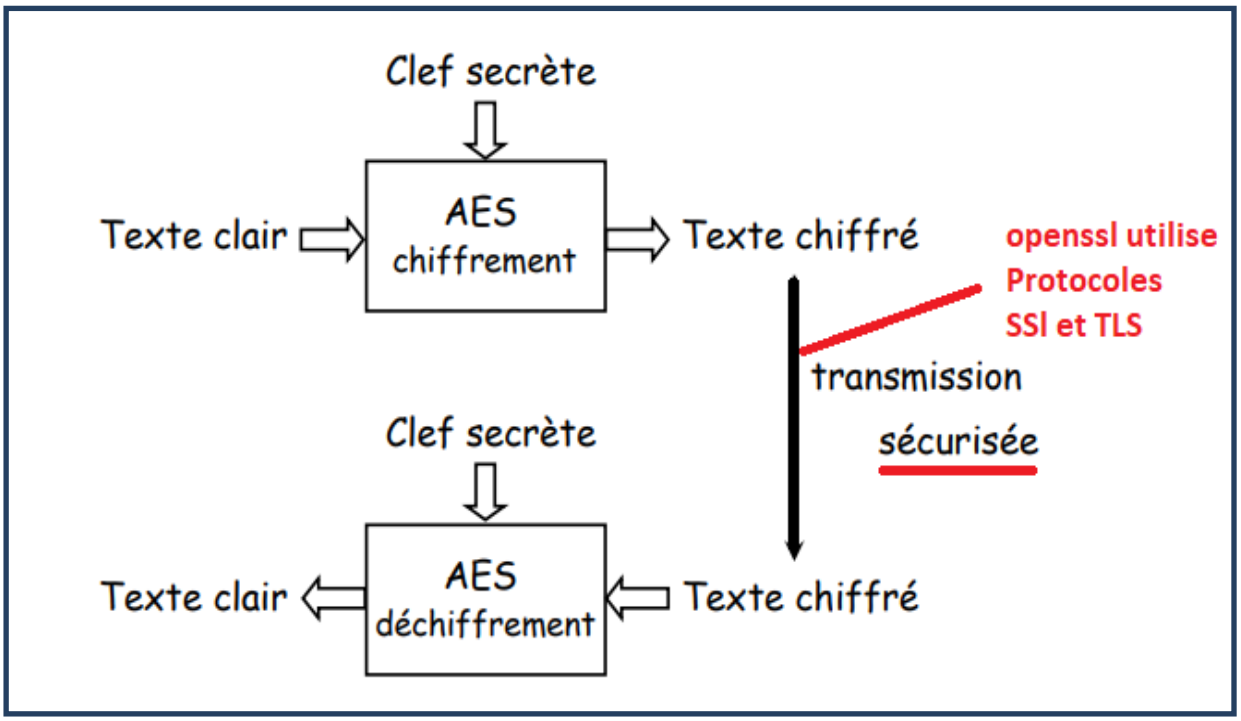

Figure 15 : Schéma de notre contribution

Exemple : (https://encode-decode.com/aes-128-ecb-encrypt-online/) **Cryptage+Décryptage**

Mots : admin **- Clef secrète :** hello **- Résultat :** zZFHsM1KmVD6YtCjHm8tUw==

3.8 Cryptanalyse de la solution :

La fonction de cryptage **AES « AES-128-ECB »** n'est pas déchiffré jusqu'à maintenant et utilisé par les gouvernements du monde et les Bancs.

Mais si en pirate le contenue des fichiers de programmation au niveau **du Serveur**. Alor en peut déchiffrer les données de la base de données par **la clef secrète**.

Donc il faut sécuriser les Serveur avec des bonnes techniques de sécurité.

3.9 Implémentation et réalisation de l'application

3.9.1 Interface de l'authentification Login (Administrateur)

Voici l'interface de l'authentification permettant au chef de service d'avoir accès au contenu de l'application.

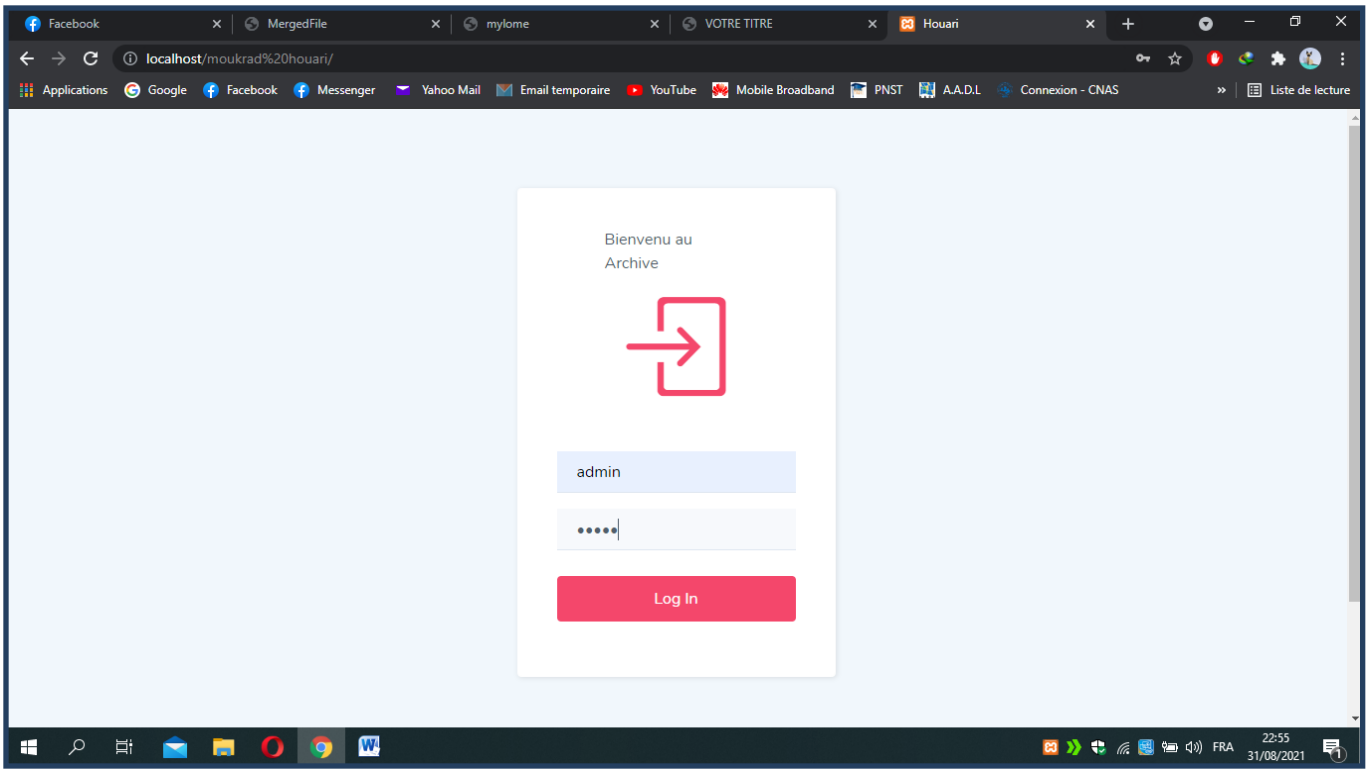

Figure 16: Interface Login

3.9.2 Interface Accueil chef de service

3.9.2.1 Interface Ajouter Agent

La figure suivante présente l'interface qui permet au chef de service de créer un nouveau compte (Username, Password)) pour un agent de saisie des archivons.

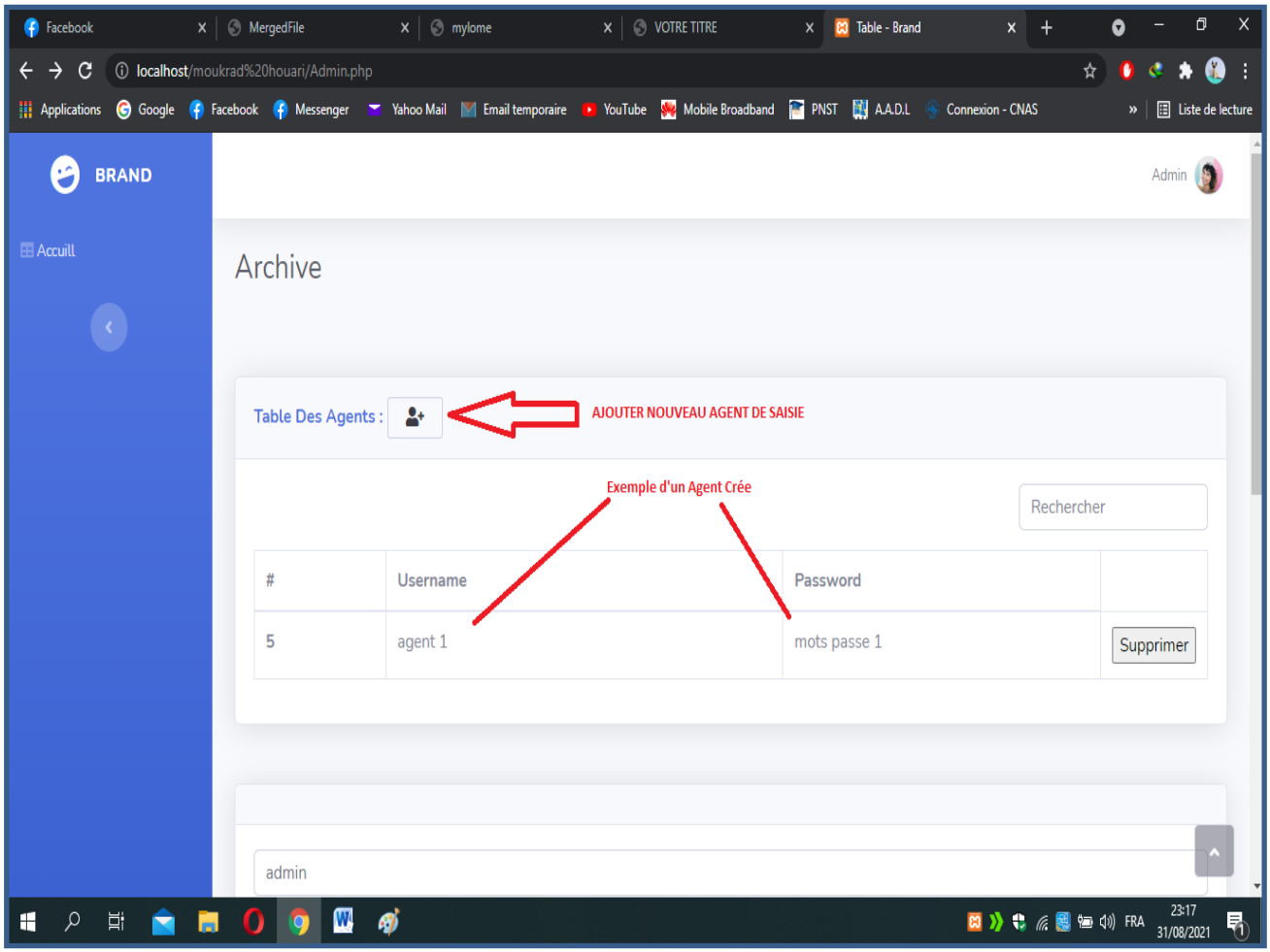

Figure 17 : Interface « Ajout d'un Agent de saisie »

3.9.2.2 Interface de modifier Login cher de service et la saisie de l'agent

Travers de cette interface, l'administrateur peut changer son nom d'utilisateur et son mot de passe qui sont par défaut : Admin ; Admin

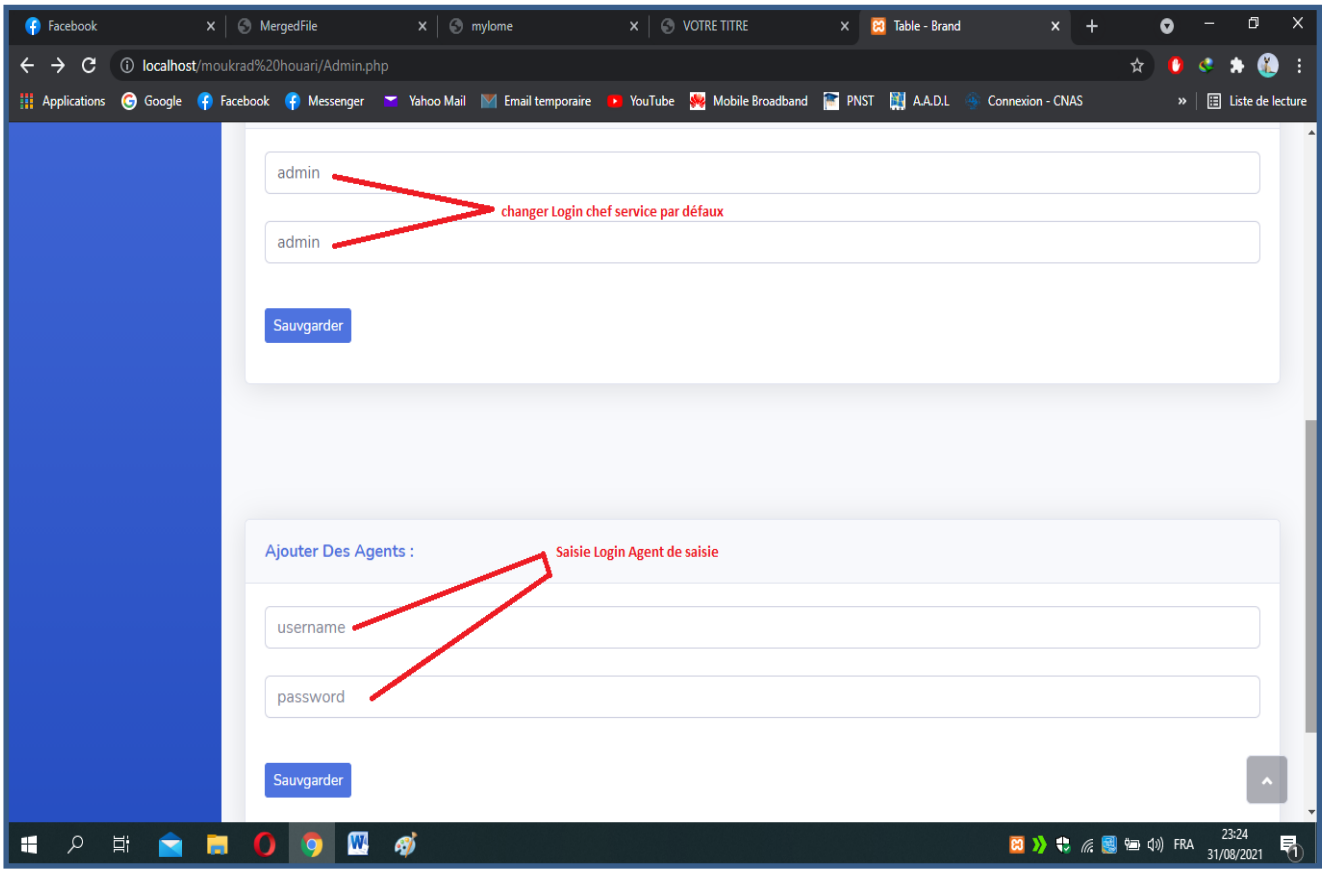

Figure 18 : Interface Changer Login Chef de Service et Saisie ajouter des Agents

3.9.2.3 Interface Ajouter Archivons

Dans cette interface on peut ajouter un Archivons par la saisie de ces informations.

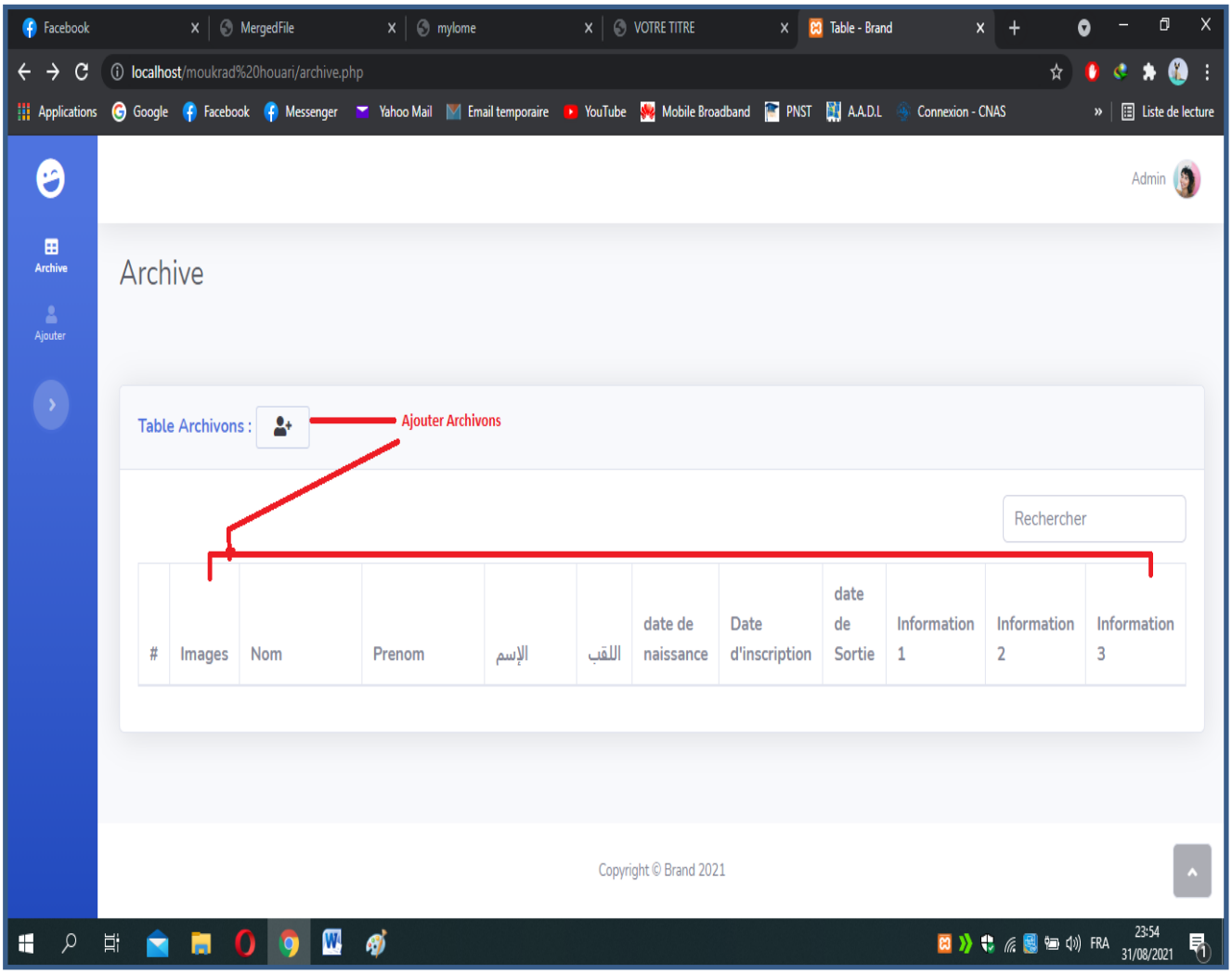

Figure 19 : Interface Ajouter Archivons

3.9.2.4 Interface Saisie Information Archivons

Dans cette interface on peut saisie les informations ; l'image et les fichiers scannés de l'archivons.

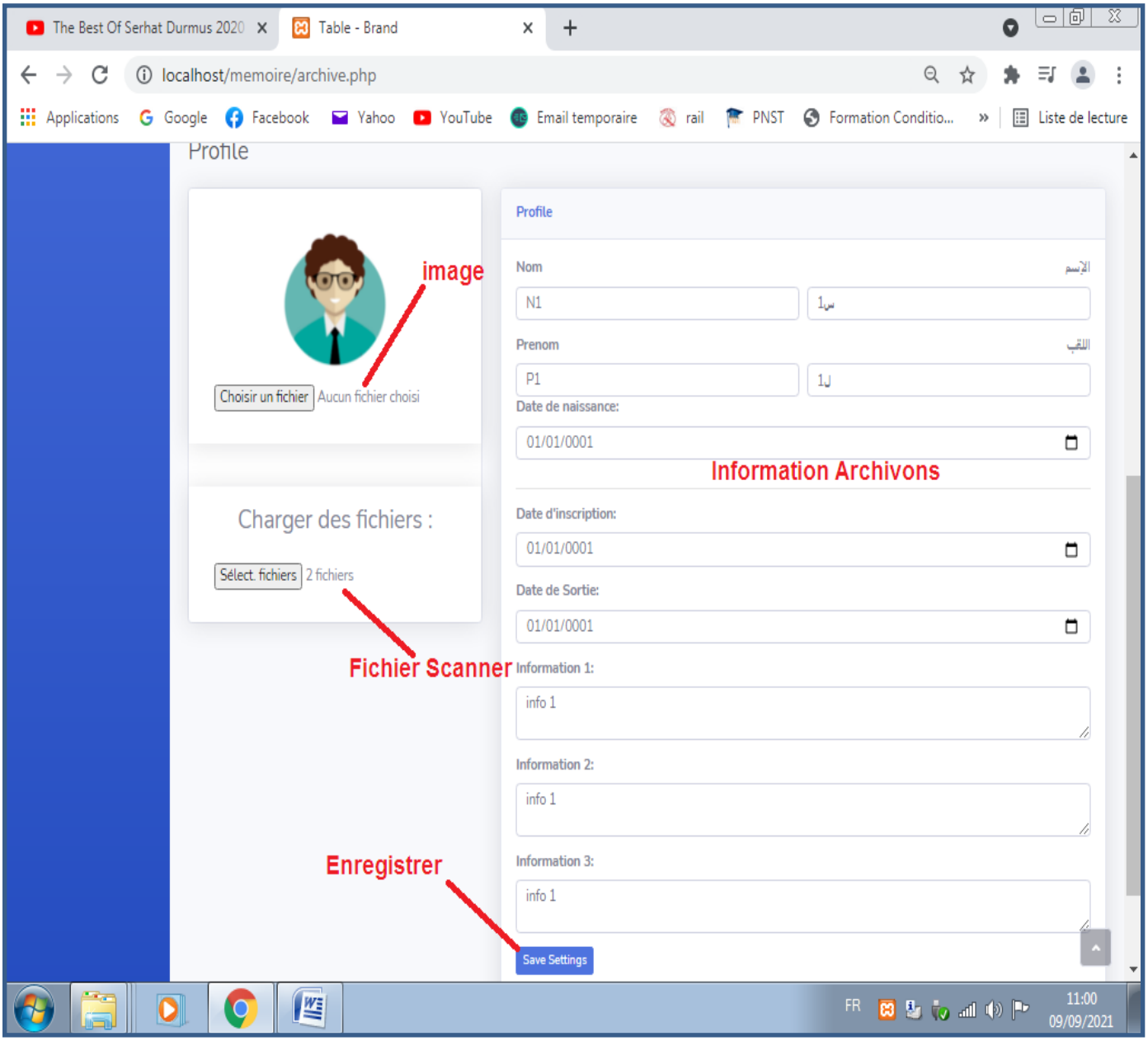

Figure 20 : Interface Saisie Archivons

3.9.2.5 Interface (Recherche ; Modifier ; Supprimer) Archivons

Dans cette interface on peut Rechercher ; Supprimer ou Modifier un Archivons.

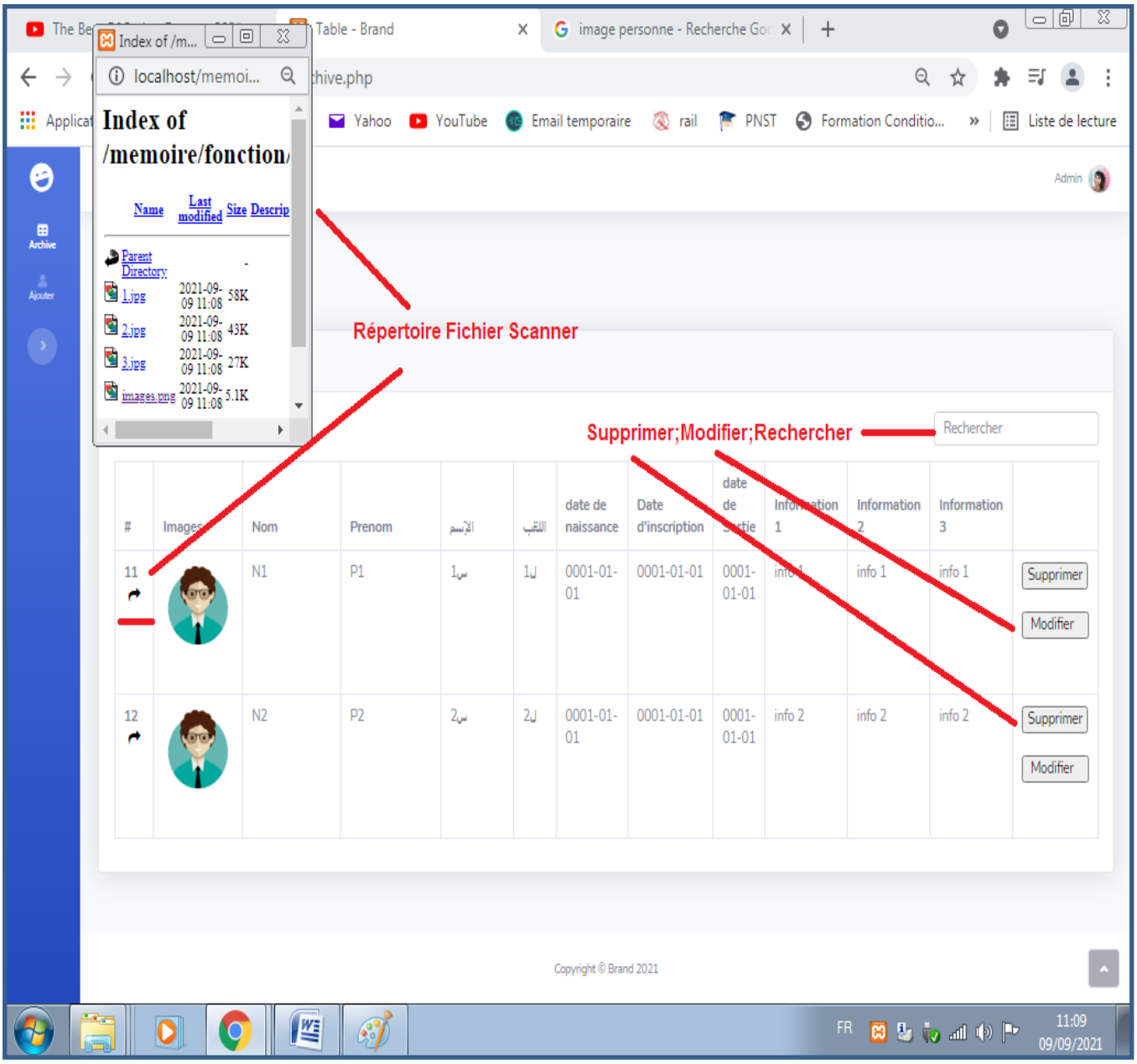

Figure 21 : Interface Recherche ; Modifier ; Supprimer Archivons

3.9.3 Le Cryptage de la Base des Données

Dans ces interfaces, on peut voir les informations stockée au niveau de la base de données sont Cryptées.

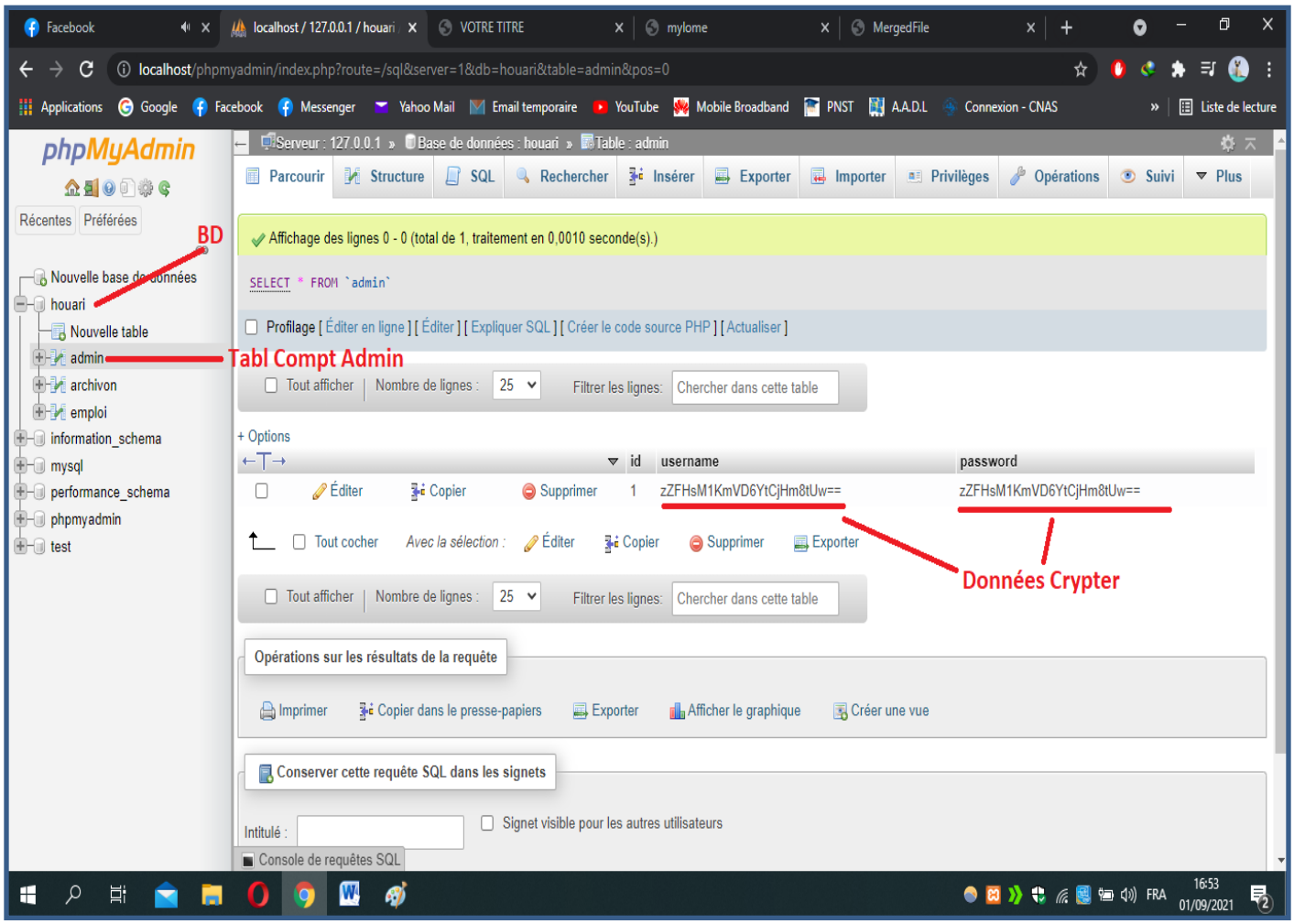

Figure 22 : BD + Table de l'Administrateur Crypter

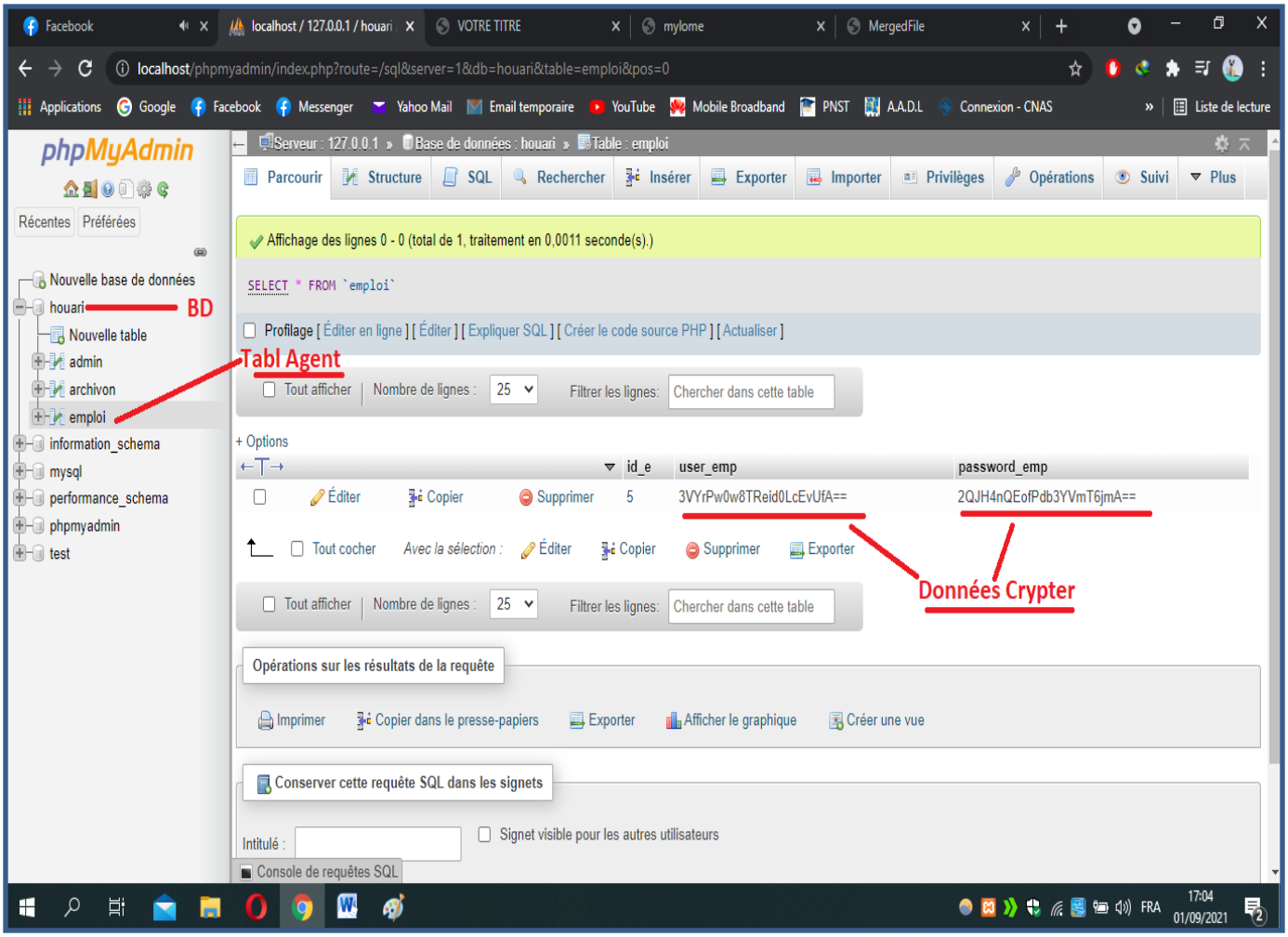

Figure 23 : BD + Table des Agents Crypter

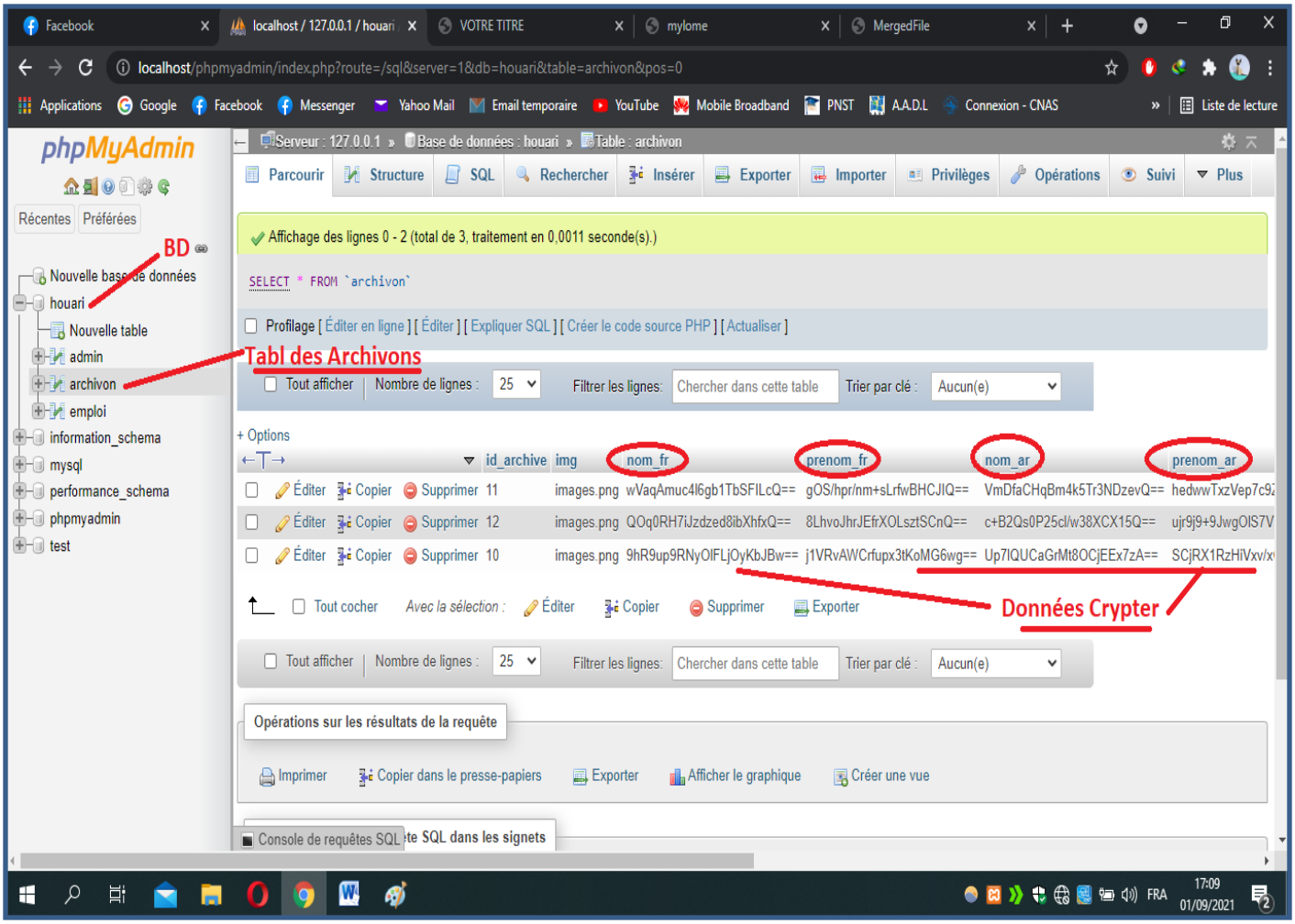

Figure 24 : BD + Table des Archivons crypter

3.10 Conclusion

Dans ce chapitre ; nous avons mentionné l'environnement de développement pour réaliser de l'application **(PHP ; MYSQL)**. Et nous avons exposé la phase de conception de l'application, qui nous a permis de maîtriser les différents diagrammes **UML** avec lesquels nous avons pu exprimer les objectifs attendus dans le système à réaliser.

Aussi nous avons proposé notre contribution par Cryptage de la base de données pour répondre aux besoins de la sécurité de l'application. Et on termine par la présentation des différents aspects et fonctionnalité de notre application ainsi que quelques interfaces des cas d'utilisation cités à la conception.

Conclusion Générale

Dans cette mémoire, nous avons présenté les différentes étapes de la conception et la réalisation de notre application pour la numérisation des archives de l'université de Mostaganem.

L'objectif majeur de notre projet consiste à faciliter le travail de l'archivage, gagner du temps et surtout le point le plus important qui est de garder la trace de chaque dossier au service et saisir dans la base de donnée, pour d'éventuelles mises à jour, ou impression des différents rapports.

Afin de satisfaire les besoins des utilisateurs, nous avons commencé la conception en utilisant le langage UML et la mise en œuvre des bases de données avec le SQL (XAMPP) et enfin la Concrétisation de l'application avec langage PHP.

Pour la sécurité des données, nous avons proposés notre approche permettant de renforcer la sécurité des informations qui sont destinées à être enregistrer dans la base de donnée par (openssl) la boite à outils cryptographiques implémentant les protocoles SSL et TLS pour sécuriser le transfert des données et le cryptage des données au niveau de la base de données avec la fonction de cryptage symétrique **AES** de type **« AES-128-ECB »** avec une clef secrète**.**

Avec le temps, les techniques de cryptage vont être améliorées. Donc, on peut sécuriser plus de données mais les ordinateurs sont devenus plus puissants en termes de temps de calcul surtout avec les ordinateurs quantiques. Ceci rend le crypto-analyse de la plus part des algorithmes en temps réel. Cette guerre reste contre les gens de la sécurité informatique et les Hackers. **Au futur travail**, nous proposons de crypter la base de données avec l'algorithme **MD5** en y ajoutant une donnée supplémentaire **(SALT)** au résultat de

hachage et le faire hachée **une deuxième** fois avec **MD5** afin de renfoncer la sécurité des informations enregistrées dans la base de données.

Bibliographie

Livre, monographie

[1] G.DESGEORGE. La sécurité des réseaux ,3 eme édition Dunod ,2012

[2] JA. BUCHMANN, introduction à la cryptographie, 2eme édition Dunod ,2006.

[3] Sécurité informatique Principes et méthode à l'usage des DSI, RSSI et administrateurs Laurent Bloch , Christophe Wolfhugel

[4] S. GHERNAOUTI-HELIE, Sécurité informatique et réseaux, DUNOD, Paris, 2011.

Articles de revue

[5] Revue maghrébine de documentation et d'information, n°27, 2018
les Archives en Algérie : génération d'archivistes, mêmes lieux mais autres temps et autres enjeux
http://www.revue-uma.rnu.tn/index.php/RMDI/article/download/174/146/

[6] Charte d'archivage Chapitre I : Concepts et définitions page 02
http://www.meer.gov.dz/a/wp-content/uploads/2019/07/charte-darchivage-MEER.pdf

Documents web

[7] https://www.enssib.fr/bibliotheque-numerique/documents/64628-guide-de-gestion-d-un-projet-de-numerisation.pdf . Consulté le : 25/02/2021

[8] https://www.commentcamarche.net/contents/1033-introduction-a-la-securite-informatique#les-causes-de-l-insecurite Consulté le : 25/02/2021

[9] Object Management Group: Unified Modeling Language: Superstructure v. 2.1.1, http://www.omg.org/cgi-bin/apps/doc?formal/07-02-03.pdf Consulté le : 06/03/2021

[10] http://dspace.univ-tlemcen.dz/bitstream/112/1297/1/Securite-d-une-application-Web.pdf Consulté le: 12/03/2021

[11] https://core.ac.uk/download/pdf/43671478.pdf Consulté le: 12/03/2021

[12] https://hal.archives-ouvertes.fr/cel-01965300/document Consulté le: 05/04/2021

[13] http://www.amue.fr/fileadmin/amue/documents-publications/amue/Gestion_archives_web.pdf Consulté le: 06/04/2021

[14] http://www.revue-uma.rnu.tn/index.php/RMDI/article/download/174/146/ Consulté le : 12/04/2021

[15] http://www.meer.gov.dz/a/wp-content/uploads/2019/07/charte-darchivage-MEER.pdf Consulté le : 12/04/2021

[16] http://www.mathdoc.fr/publis/falavard_numerisation_31mars2005_web.pdf Consulté le : 15/05/2021