**مقاله مروري**

**الگوريتم‌هاي رمزگذاري چندلايه بر روي داده‌هاي مراقبت‌هاي بهداشتي**

سميه كرباسي1

1دانشگاه پيام‌نور تهران پست الكترونيكي: [Somayeh.Karbasy@gmail.com](mailto:Somayeh.Karbasy@gmail.com)

**چکیده**

در مورد محرمانگی داده‌های مراقبت‌های بهداشتی ( PHI ) هنگامی که در محیط ابر ذخیره می‌شوند، سیاست‌های درستی باید اعمال شود. این اطلاعات می‌تواند به دلیل ذخیره‌سازی در قالب ساده یا با استفاده از الگوریتم‌های رمزگذاری ضعیف، به خطر بیفتد. بعضی از اطلاعات مربوط به بیمار ضرورت دارد که محافظت شده باشد و توسط افراد غیرمجاز دیده نشده یا تغییر داده نشوند. هدف اصلی این گزارش ارائه یک الگو و روش مطمئن برای حفظ محرمانگی داده‌های بیماران است. چون داده‌ها، به صورت همیشگی در محیط ابری در دسترس هستند. این امر با رمزگذاری و رمزگشایی داده‌ها به صورت چند لایه به دست می‌آید. الگوریتم‌هایی که برای رمزگذاری استفاده خواهیم کرد؛ الگوریتم‌های استاندارد هستند که توسط NIST توصیه می‌شوند. در این‌جا هدف استفاده ار الگوریتم‌های چندگانه برای حفظ محرمانگی داده‌ها است. در پایان‌نامه مورد بررسي، برای اطمینان از محرمانه بودن اطلاعات ذخیره شده در محیط ابر، یک روش رمزگذاری چند لایه را پیشنهاد شده است. این تکنیک پیشنهادی در صورت استفاده در قالب چند لایه، امنیت تکنیک های رمزنگاری را بهبود می‌بخشد. یک سیستم محلی برای پژوهش تنظیم کرده‌ است. از پایگاه داده رابطه‌ای و فریم‌ورک 4.5 استفاده کرده است. مجموعه‌ای از 500 پرونده ساختگی بیمار برای استفاده از روش‌های پیشنهادی استفاده می‌شود. اين پژوهش برای بررسی محرمانگي روش‌های پیشنهادی انجام شده است. اين پژوهش به ما نشان می‌دهد که وقتی داده‌ها در محیط ابری هستند، تکنیک‌های رمزگذاری چند لایه برای بخش‌های بهداشت عمومی مناسب‌ترند.[4]

**کلمات کليدي: رايانش ابري ، داده‌ هاي مراقيت‌هاي بهداشتي ، رمزگذاري، كليد**

**1. مقدمه**

رایانش ابري، سرويس محاسباتی مورد تقاضا است.(منابع محاسباتی در صورت تقاضا و در حد نیاز در دسترس هستند.) كه بيشترين امكانات را در اختيار بخش‌هاي مراقبت‌هاي بهداشتي مورد نياز بيماران قرار مي‌دهد. داده‌ها به ساده‌ترين صورت و حتي از راه دور ذخيره و بازيابي مي‌شوند و امکان تغییر دارند. در واقع بیمارستان‌ها نیازی به ذخیره‌ه‌سازي محلي داده‌ها ندارند و فقط كافي است سرور مورد نياز جهت دسترسي به اطلاعات را بخرند. هدف اصلی رایانش ابری، به اشتراک گذاری منابع و دسترسي بهينه به آن‌ها است.

**2. پیشینه تحقیق**

در اوایل دهه 1960 معماری سرور مشتری فقط برای رایانه‌های اصلی و کلاینت مورد استفاده قرار گرفت. در آن زمان ذخیره اطلاعات بسیار گران بود. هزینه CPU نیز بسیار زیاد بود. به همین دلیل از Mainframe برای ذخیره سازی و پردازش استفاده مي‌شد. برای دسترسی به داده‌ها و پردازش، از ترمینال‌های تخلیه استفاده مي‌شد.

در سال 2006 آمازون شروع به فعالیت خود در زیر شاخه‌ای به نام خدمات وب آمازون کرد.

گوگل نسخه آزمایشی Google App Engine را در آوریل 2008 منتشر کرد. در همان سال ناسا OpenNebula را نیز معرفی کرد. این اولین پروژه منبع آزاد بود که برای خصوصیات ابرهای ترکیبی به کار گرفته شد.

در سال 2010 مایکروسافت Azure توسط مایکروسافت منتشر شد.

در سال 2012، موتور محاسبه Google قبل از اینکه در دسامبر 2013 در دسترس عمومی قرار بگیرد، در حالت پیش‌نمایش منتشر شد

در سال 2011 دكتر سلیمان و همكاران در مقاله‌اي، روش چندلایه‌ای را برای خدمات سلامت الکترونیکی مطابق با سند ISO 17799 تعریف کرده و اطلاعات را به سه دسته اطلاعات سری، بسیار محرمانه و خصوصی تقسیم کرده؛ الگوریتم‌های رمزگذاری متقارن، 3DES و تابع مقدار هش را معرفی کرده‌ اند. نویسندگان از اندازه کلید 193 بیت برای لایه 1 و 129 بیت تا 192 بیت برای لایه 2 و 112 تا 128 برای لایه 3 و 80 تا 111 بیت برای لایه 4 استفاده کرده‌اند. کار اصلی نویسندگان روی الگوریتم 3DES است. و از يك الگوریتم برای رمزگذاری و رمزگشایی استفاده می‌شود.[6]

در سال 2013 کیا و همکاران در مقاله‌ای با استفاده از SOAP / XML داده‌ها را با AES رمزگذاری کرده اند.[2]

در سال 2016 ژو و همکاران نویسندگان به خوبی مدل مراقبت‌های بهداشتی جدیدی را برای ذخیره داده‌های ابری در نظر گرفته‌اند. آن‌ها RBE (رمزنگاری مبتنی بر نقش) را اعمال کرده‌اند. ابتدا، آن‌ها مدل PCEHR (سوابق الکترونیکی کنترل الکترونیکی شخصی) را که توسط دولت استرالیا معرفی شده شرح داده‌اند. سپس PCEHR در RBE برای امنیت داده استفاده می‌شود. آن‌ها ساختار آرم داده‌ها و ویژگی‌هایش را بر اساس رمزگذاری طراحی می‌کنند و ادعا كردند كه رویكرد آنها كنترل انعطاف‌پذیری در ذخیره‌سازی داده‌ها را فراهم می‌كند.[8]

در سال 2019 سودهیپ و همکار در مقاله‌ای رمزگذاری مبتنی بر ویژگی سیاست رمزگذاری (CP-ABE) را معرفی کرده‌اند. کلید رمزگذاری شامل خط‌مشی‌هایی است و آن‌ها می‌گویند اگر کلید هک شده‌باشد، آندسته از سوابق رمزگشایی می‌شوند که کلید آن‌ها هک می‌شود اما بقیه موارد همچنان محافظت می‌شوند.[5]

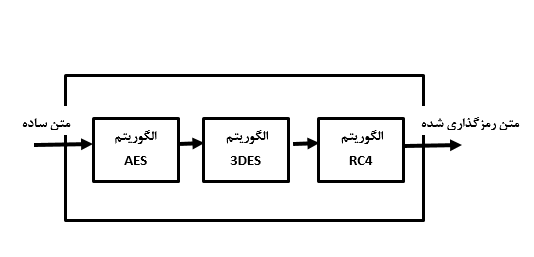
در سال 2019 هما و همکار ، درباره روش رمزنگاری منحنی بیضوی بحث کردند و روش‌های تولید کلید اصلی شخص ثالث را معرفی کردند. مالک داده را برای درخواست کلید و رمزگذاری سند به صورت آنلاین به بخش دیگر ارسال می‌کند. شخص ثالث رمز را رمزگذاری و به صاحب داده ارسال و مالک تاریخ را در سرور ابری بارگذاری می‌کند و کلید را برای استفاده در آینده نگه می‌دارد.[1]

در سال 2019 پارا و همکاران از تکنیک‌هایی استفاده کردند که در آن، آرم داده‌ها با استفاده از درون‌یابی خطی ایجاد شده و سپس مستطیل جادویی با استفاده از الگوریتم LSB ایجاد و با استگانوگرافی، داده‌ها را رمزگذاری کردند.[3]

در سال 2019 وزيد و همكاران نویسندگان در مورد مدل تهدید و احراز هویت برای دستگاه های مبتنی بر Iot در محیط ابر بحث کرده‌اند و سعی کرده‌اند چالش‌های فعلی امنیت و داده‌‍‌های مبتنی بر اینترنت اشیا در ابر را بررسی کنند. تمرکز اصلی آنها در تحقیق، سازوکار احراز هویت است و مفهوم مجازی تکنیک جدید را ارائه داده‌اند. در مقاله خود یک مطالعه تطبیقی در مورد هزینه‌های ارتباطی و فنی و حرفه ای انجام داده‌اند. محاسن و معایب تکنیک‌های احراز هویت موجود نیز در دست بررسی است اما راه‌حل مشخصی پیشنهاد نمی‌شود.[7]

3**. راه‌اندازی آزمایشی طرح پیشنهادی**

ابتدا به تکنیک چندلایه رمزگذاری ( شکل 1) توجه کنید؛ در این حالت متنی که باید محافظت شود؛ وارد سیستم الگوریتم چندگانه می‌شود. داخل سیستم الگوریتم چندگانه در این مورد خاص، 3 الگوریتم AES و DES3 و RC4 وجود دارد. خروجی هر الگوریتم، به صورت رمزگذاری شده و دوباره توسط الگوریتم بعدی طبق شکل، رمزگذاری می‌شود و خروجی نهایی با رمزگذاری چندلایه و ایمنی بالا ایجاد می‌شود.



شكل 1 : تکنیک محافظت از چند لایه

برای توسعه طرح یک مجموعه داده ساختگی( برای ایمنی بیمار) از حدود 500 بیمار انتخاب کرد؛ روی داده‌ها، الگوریتم‌های رمزگذاری موجود در RDBMS اعمال می‌شوند.و داده‌ها در محیط ابری ذخیره می‌شوند.

در آغاز ثبت نام بیماران، شماره پرونده پزشكي با با رمز عبور پیچیده‌ای که به طور تصادفی ایجاد شده است، برای اطلاعات بیمار اختصاص می‌یابد. برای دسترسی در وب سايت، بیمار شماره پرونده پزشکی(MR No) را به عنوان نام کاربری و رمز ورود وارد می‌کند و روی Login کلیک می‌کند. اگر نام کاربری معتبر باشد و رمز عبور آن درست باشد، پس از رمزگشایی نسخه پزشک برای وی نمایش داده می‌شود. الگوریتم رمزگذاری متقارن AES را با ترکیب کلیدهای مختلف و DES3 بر روی داده‌ها اعمال مي‌كنيم زیرا کلید در RDBMS ذخیره می‌شود و توسط سرور Microsoft SQL محافظت می‌شود و از رمز عبور محافظت می‌کند.

**4. فرآیند رمزگذاری و رمزگشایی در RDBMS**

فرایند رمزگذاری کلی با استفاده از SQL Server بر روی يك ستون مطابق مراحل زير است. کلید اصلی در پایگاه‌داده، براساس روش متقارن محافظت می‌شود.

مرحله 1 :  ایجاد کلید اصلی

ابتدا باید کلید اصلی با رمز عبور مناسب ایجاد شود و سپس گواهینامه بر اساس کلید اصلی تولید می‌شود.

مرحله 2 : ایجاد گواهی

گواهینامه دیجیتالی جهت محافظت از کلید اصلی پایگاه‌داده ایجاد می‌شود.

مرحله 3 : کلید متقارن

یک کلید متقارن برای رمزگذاری و رمزگشایی بر اساس الگوریتم‌های رمزگذاری در سرور sql ، ساخته می‌شود؛ به عنوان مثال AES128 ، AES192 و AES256.

مرحله 4 : رمزگذاری ستون‌ها

شمای جدول و فیلدهای را رمزگذاری می‌کنیم.

**5. تجزیه و تحلیل طرح پیشنهادی**

*مجموعه داده ساختگی از 500 بیمار را برای هدف‌ آزمایش آماده شده است. برخی از ویژگی‌ها با در نظر گرفتن GDPR و HIPAA (‌قانون حفاظت اطلاعات آمريكا و اروپا )گرفته شده است. به عنوان مثال MR No ( شماره پرونده پزشکی)، نام، نام نسبی، جنسیت، آدرس، تاریخ تولد، تاریخ ثبت، NIC ، شماره تلفن همراه و شماره حساب/اطلاعات کارت اعتباری. این ویژگی‌ها به ویژه هنگامی که داده ها در فضای ابری قرار دارند، نیاز به مراقبت بیشتری دارند. برای افزایش سطح محرمانگي، خصوصیات ویژه  PHI را برای رمزگذاری و رمزگشایی در نظر گرفته شده است.*

**6. نصب پیکربندی سخت‌افزار و نرم‌افزار**

**سخت‌افزار مورد نياز**

* *پردازنده Intel Core i7-6500U Processor*
* *Ram 8 گیگابایتی*
* *هارد دیسک 500 گیگابایتی*

**سیستم عامل و نرم‌افزار مورد نیاز**

* *ویندوز 10 یا بالاتر*
* *Visual Studio 12 یا 15*
* *SQL Server 2014 یا بالاتر*
* *Framework 4.5*

**7. ایجاد کلیدها و گواهینامه‌ها و رمزگذاری داده‌ها**

ایجاد کلید و گواهینامه‌ها با دستورات SQL انجام می‌شود. داده‌های مربوط به بیمار که باید روی ابر بارگذاری شوند؛ تهیه شده و فرآیند رمزگذاری روی آن اعمال می‌شود. داده‌ها در جدول پایگاه‌داده با فرمت رمزگذاري‌شده، ذخیره می‌شوند.

**8. رمزگشایی داده‌ها**

*بیمار وارد سایت مورد نظر می‌شود که در برگه ثبت نام چاپ شده است و از شماره پرونده پزشکی به عنوان نام کاربری و رمز عبور استفاده می‌کند و بر روی ورود کلیک می‌کند. جزئیات پرونده پزشکی بیمار، نشان داده شده است.*

**9. تحليل نتايج**

• اگر الگوریتم رمزگذاری منفرد AES با اندازه کلید 128 بیتی اعمال شود، کل زمان سپری شده 250 میلی‌ثانیه خواهدبود.

• اگر AES با اندازه کلید 192 بیتی اعمال شود، کل زمان سپری شده 21 میلی‌ثانیه خواهد ‌بود.

• اگر AES با اندازه کلید 218 بیتی اعمال شود، کل زمان سپری شده 321 میلی‌ثانیه خواهد بود.

• اگر 3DES به تنهایی اعمال شود، کل زمان سپری شده 260 میلی‌ثانیه خواهد بود.

نتایج حاصل از ترکیب چند الگوریتم با مجموعه داده‌های مشابه نیز در این شکل نشان داده شده است.

• اگر ترکیبی از AES128 و 192 استفاده شود؛ زمان سپری شده 521 میلی‌ثانیه خواهد بود.

• اگر ترکیبی از AES128 و 256 استفاده شود؛ زمان سپری شده 474 میلی‌ثانیه خواهد بود.

• اگر ترکیبی از AES128 و 3DES استفاده شود، زمان سپری شده 29 میلی‌ثانیه خواهد بود.

• اگر ترکیبی از AES192 و AES256 استفاده شود، مدت زمان سپری شده 35 میلی ثانیه خواهد بود.

• اگر ترکیبی از AES192 و 3DES استفاده شود، مدت زمان سپری شده 86 میلی‌ثانیه خواهد بود.

• اگر ترکیبی از AES256 و 3DES استفاده شود، مدت زمان سپری شده 163 میلی ثانیه خواهدبود.

زمان پردازنده را در میلی‌ثانیه برای 500 رکورد با الگوریتم‌های رمزگذاری منفرد مقایسه می‌کنیم.

o AES128 زمان پردازنده 203 میلی ثانیه را می‌گیرد.

o AES192 زمان پردازنده 78 میلی‌ثانیه است.

o AES256 ، 72میلی‌ثانیه طول می‌کشد.

o 3DES، 78 میلی‌ثانیه طول می‌کشد.

نتایج زمان پردازنده برای چندین ترکیب الگوریتم با مجموعه داده‌های مشابه نیز نشان داده شده است.

o AES128 و 192، 141 میلی‌ثانیه طول می‌کشد.

o AES128 و AES256 ، 94 میلی‌ثانیه طول می‌کشد.

o AES192 و AES256 31 میلی‌ثانیه طول می‌کشد.

o AES192 و 3DES ، 15 میلی‌ثانیه طول می‌کشد.

o AES256 و 3DES ، 110 میلی‌ثانیه طول می‌کشد.

اگرچه زمان پردازنده با AES256 و 3DES به زمان CPU بیشتری نیاز دارد اما زمان سپری شده AES256 و 3DES طرح بهتری را برای رویکردهای چندلایه ارائه می‌دهد زیرا رمزگذاری فقط بارگذاری اطلاعات را انجام می‌دهد. برای بهترین سطح محرمانگی AES256 با 3DES مناسب است.

**10. دستورالعمل‌های موجود**

**قانون HIPAA و GDPR**

HIPAA يك كلمه اختصاري به مفهوم " قابلیت حمل و پاسخگویی بیمه درمانی است". این مصوبه قوانين مختلفي را درباره حفاظت از داده‌هاي بيمار ارائه مي‌دهد.

18 ویژگی زیر اعمالي كه بايد محافظت شوند را مشخص مي‌كند:

• نام و نام خانوادگی بیمار

• آدرس شامل کد پستی، شهر، کشور

• همه تاریخ‌ها

• شماره تلفن

• نمابر

• شناسه ایمیل

• شماره بيمه

• سوابق پزشکی شماره

• اطلاعات کارت سلامت

• حساب بانکی بدون/ اطلاعات کارت اعتباری

• گواهینامه یا گواهینامه رانندگی

• شماره خودرو

• شناسه دستگاه و شماره سریال

• آدرس وب

• آدرس پروتکل اینترنت

• بیومتریک

• هر نوع تصویری

• هر مشخصه دیگری که بتواند منحصراً فرد را شناسایی کند.

GDPR (مقررات عمومی حفاظت از داده ها) مقررات اتحادیه اروپا است که در سال 2016 پذیرفته شده است. پس از سال 2018 این قانون برای کلیه سازمان های کشورهای اتحادیه اروپا اجباری شده است که ذخيره اطلاعات شخصی فرد را باید مطابق با GDPR باشد.

**11. پیشنهادها**

زماني كه به عنوان سمينار دانشجويي، كار بر روي اين پايان‌نامه را شروع كردم؛ جذب موضوع آن شدم. امنيت داده‌هاي مربوط به بيمار و حفظ و نگه‌داري اطلاعات براي استفاده مجدد بيمار و پزشك. دانشجويان ارشد الگوريتم‌هاي رمزگذاري را به خوبي مي‌دانند اما تركيب آن‌ها و رسيدن به حالت ايده‌آل كاري است كه راستاي فكري اين پايان‌نامه بوده است. طراحي نرم‌افزار به كاررفته در اين سيستم، تقريبا راحت بوده و نوشتن برنامه رمزنگاري به توجه به تركيب الگوريتم‌هاي راحت است. موردي كه نياز به دقت دارد و در واقع نيرو محركه كار و عامل برتري طرح مي‌باشد؛ ژيدا كردن بهترين تركيب‌هاي الگوريتم‌هاي رمزگذاري است كه بتوان به صورت چند لايه استفاده كرد.

در مورد مشخصات سخت‌افزاری مورد نیاز طرح، اکثر سيستم‌های موجود شرایط لازم را دارند و نیاز به توسعه خاصی نیست ولی مشخصات نرم‌افزاری ممکن است مشکلاتی از لحاظ هزینه برای توسعه وجود آورد؛ به طور مثال ویندوز 10 ممکن است روی بعضی سیستم‌ها قابل نصب نباشد. لذا یکی از پیشنهادهای من تبدیل دستورات به صورت است که روی مشخصات پایین‌تر نرم‌افزاری قابل نصب و اجرا باشد. یک حالت موثر می‌تواند وجود چند نسخه با تاکید بر روی مشخصات بالاتر باشد که احیانا در صورت وجود مشکلات زیر ساختی قابل اجرا باشد. موردی که جای کار بیشتر دارد و مورد نیاز است توجه به داده‌های غیرمتنی بیمار است که با تکنیک‌های بروز رمزگذاری، ایمن‌تر باشند.

پیشنهاد دیگری که مربوط به نگارش پایان‌نامه است؛ استفاده از شیوه ارجاع به منابع می‌باشد. به نظر بنده، شیوه ارجاع بهتر است مطابق راهنماری نگارش پایان‌نامه معاونت آموزشی و تحصیلات تکمیلی دانشگاه پیام‌نور باشد. شیوه ارجاع در این پایان‌نامه به صورت لینک به منابع بود و شخصا کار مشکلی در درک مفاهیم آن داشتم.

**12. ارائه ایده برای پایان‌نامه‌های جدید تکمیلی**

- بررسی و تست بهترین ترکیب الگوریتم‌های رمزگذاری از لحاظ سرعت،هزینه،کارایی و ... روی داده‌های مراقبت‌های بهداشتی برای رسیدن به مطلوب‌ترین نتیجه

- پیاده‌سازی الگوریتم‌های رمزگذاری بومی ایران روی داده‌های مراقبت‌های بهداشتی

- رمزگذاری چندلایه کارا روی داده‌های تصویری مراقبت‌های بهداشتی

- ساخت برنامه امنیتی Open Source رمزگذاری چند لایه روی انواع سیستم ها

**13. نتيجه­گيري**

در این مقاله به موضوع اجرای رمزگذاری چند لایه داده‌های مراقبت‌های بهداشتی پرداخته شد؛ انواع ترکیب‌ها تست شد و با ذکر سخت‌افزار و نرم‌افزار مورد نیاز، طرح پیاده‌سازی شده؛ بررسی شد. در ادامه پیشنهادات جهت ادامه طرح داشتم و موضوعات پایان‌نامه‌ها و سمینار‌های بعدی در راستای این مقاله مطرح شد.

**مراجع**

1. V. S. V. Hema and R. Kesavan, “Ecc based secure sharing of healthcare data in the health cloud environment,” Wireless Personal Communications, vol. 108, no. 2, pp. 1021–1035, 2019.
2. M. M. Kiah, M. S. Nabi, B. Zaidan, and A. Zaidan, “An enhanced security solution for electronic medical records based on aes hybrid technique with soap/xml and sha-1,” Journal of medical systems, vol. 37, no. 5, p. 9971, 2013.
3. S. A. Parah, A. Bashir, M. Manzoor, A. Gulzar, M. Firdous, N. A. Loan, and J. A. Sheikh, “Secure and reversible data hiding scheme for healthcare system using magic rectangle and a new interpolation technique,” in Healthcare Data Analytics and Management. Elsevier, 2019, pp. 267–309
4. H.A.Shah. (2020). “A Multilayer Encryption Model To Protect Healthcare Data in Cloud Environment”. (Unpublished master’s thesis). University of Islamabad
5. K. Sudheep and S. Joseph, “Review on securing medical big data in healthcare cloud,” in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*. IEEE, 2019, pp. 212–215
6. R. Sulaiman, D. Sharma, W. Ma, and D. Tran, “A new security model using multilayer approach for e-health services,” Journal of Computer Science, vol. 7, no. 11, pp. 1691–1703, 2011.
7. M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. Rodrigues, “Authentication in cloud-driven iot-based big data environment: Survey and outlook,” Journal of Systems Architecture, vol. 97, pp. 185-196, 2019.
8. L. Zhou, V. Varadharajan, and K. Gopinath, “A secure role-based cloud storage system for encrypted patient-centric health records,” *The Computer Journal*, vol. 59, no. 11, pp. 1593–1611, 2016.