



دانشکده فنی و مهندسی
گروه مهندسی کامپیوتر و فناوری اطلاعات

گزارش سمینار کارشناسی ارشد رشته مهندسی کامپیوتر نرم افزار (M.Sc)

عنوان سمینار:

مدل رمزگذاری چند لایه برای محافظت از داده‌های مراقبت‌های
بهداشتی در محیط ابری (بررسی و مرور)

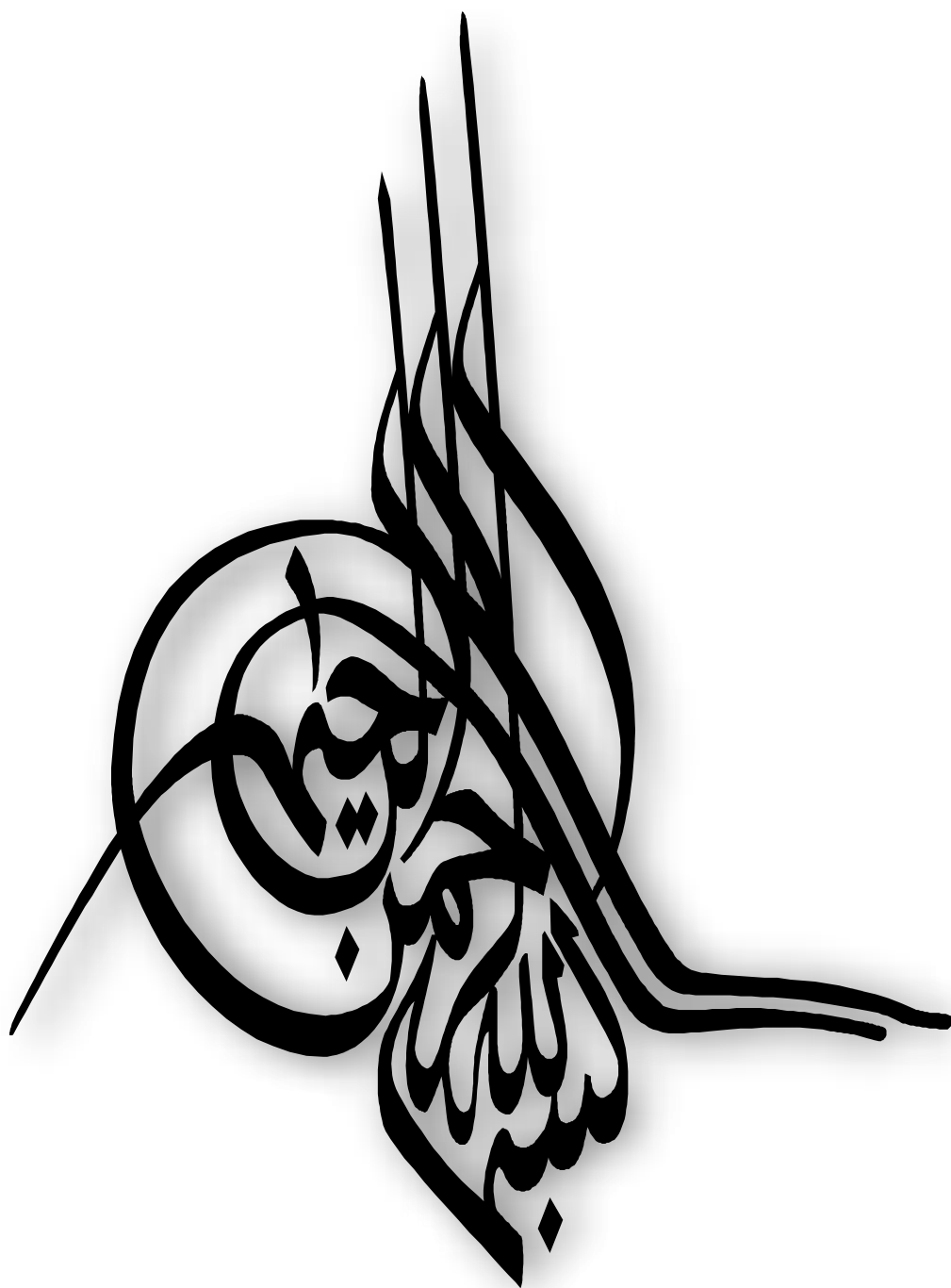
استاد راهنما:

دکتر سیدعلی رضوی

نگارنده:

سمیه کرباسی راوری

مرداد ۱۴۰۰



فهرست مطالب

چکیده	۱
کلمات کلیدی	۱
۱. مقدمه	۲
۱-۱ تعریف مسئله و بیان سؤال‌های اصلی تحقیق	۵
۱-۲ ضرورت تحقیق	۵
۱-۳ هدف‌ها	۵
۱-۴ چه کاربردهایی از انجام این تحقیق متصور است؟	۶
۱-۵ روش و مراحل انجام تحقیق	۶
۱-۶ سازمان پایان‌نامه مورد بررسی	۶
۱-۷ ساختار گزارش تحقیق	۶
۲. مفاهیم عمومی رمزگذاری و پیشینه تحقیق	۷
۲-۱ انواع طرح‌های رمزنگاری	۷
۲-۱-۱ رمزگذاری متقارن	۷
۲-۱-۲ رمزگذاری نامتقارن	۷
۲-۲ سرویس امنیتی برای رمزنگاری برای مراقبت‌های بهداشتی	۸
۲-۳ رمزگذاری چند لایه	۹
۲-۴ کار الگوریتم‌های مورد استفاده در طرح پیشنهادی	۹
۲-۵ پیشینه تحقیق	۱۴
۳. مروری بر کارهای انجام‌شده	۱۷
۳-۱ مقدمه	۱۷
۳-۲ راه‌اندازی آزمایشی طرح پیشنهادی	۱۷
۳-۲-۱ فرآیند رمزگذاری و رمزگشایی در RDBMS	۱۹
۳-۳ تجزیه و تحلیل طرح پیشنهادی	۱۹
۳-۴ نصب پیکربندی سخت‌افزار و نرم‌افزار	۲۰

۲۰	۳-۱ سخت افزار مورد نیاز
۲۰	۳-۲ سیستم عامل و نرم افزار مورد نیاز
۲۰	۳-۵ ایجاد کلیدها و گواهینامه ها و رمز گذاری داده ها
۲۲	۳-۶ رمز گشایی داده ها
۲۳	۳-۷ تحلیل نتایج
۲۶	۴. کاربرد الگوریتم های چند گانه رمز گذاری روی داده های مراقبت بهداشتی-مزایا و معایب
۲۶	۴-۱ مقدمه
۲۶	۴-۲ دستورالعمل های موجود
۲۷	۴-۳ آینده کار
۲۷	۴-۴ مزایا و معایب استفاده از تکنیک های پیشنهادی
۲۷	۴-۴-۱ مزایا
۲۸	۴-۴-۲ معایب
۲۸	۴-۵ پاسخ به سوالات تحقیق
۲۹	۴-۶ جمع بندی
۳۰	۵. جمع بندی و پیشنهادها
۳۰	۵-۱ مقدمه
۳۰	۵-۲ نتایج حاصل از تحقیق
۳۱	۵-۳ پیشنهادها
۳۱	۵-۴ ارائه ایده برای پایان نامه های جدید تکمیلی
۳۲	۵-۵ جمع بندی و نتیجه گیری
۳۳	مراجع
۳۴	واژه نامه
۳۶	Abstract

فهرست اشکال

شکل ۱-۱: رایانش ابری	۳
شکل ۲-۱: رمزنگاری استگانوگرافی (Shah,2020)	۴
شکل ۱-۲: رمزگذاری نامتقارن کلید	۸
شکل ۲-۲: روش رمزگذاری چند لایه (Shah,2020)	۹
شکل ۳-۲: جایگزینی اولیه (Shah,2020)	۱۰
شکل ۴-۲: تابع Round (Shah,2020)	۱۰
شکل ۵-۲: گسترش جعبه جایگزینی	۱۰
شکل ۶-۲: تولید کلید	۱۱
شکل ۷-۲: نمودار معماری ۳DES	۱۲
شکل ۸-۲: معماری الگوریتم AES (Shah,2020)	۱۴
شکل ۱-۳: تکنیک محافظت از چند لایه (Shah,2020)	۱۷
شکل ۲-۳: نمودار معماری روش شناسی (Shah,2020)	۱۸
شکل ۳-۳: فیش ورود به سیستم برای بیمار (Shah,2020)	۱۸
شکل ۴-۳: فرآیند رمزگذاری کلی (Shah,2020)	۱۹
شکل ۵-۳: نمونه مجموعه داده‌های ساختگی (Shah,2020)	۲۰
شکل ۶-۳: ایجاد کلیدها و گواهینامه‌ها (Shah,2020)	۲۱
شکل ۷-۳: فرم رمزگذاری شده داده‌ها (Shah,2020)	۲۱
شکل ۸-۳: صفحه ورود به سیستم برای ورود بیمار (Shah,2020)	۲۲
شکل ۹-۳: جزئیات پرونده پزشکی یک بیمار (Shah,2020)	۲۲
شکل ۱۰-۳: نمای گرافیکی زمان سپری شده الگو (Shah,2020)	۲۳
شکل ۱۱-۳: نمای گرافیکی زمان CPU زمان الگوریتم رمزگذاری چندلایه و منفرد (Shah,2020)	۲۳
شکل ۱۲-۳: نمای گرافیکی اندازه جدول پایگاه داده بعد از ذخیره‌سازی (Shah,2020)	۲۴

فهرست جداول

- جدول ۱-۱: مقایسه بین رمزنگاری کلاسیک و مدرن (Shah,2020) ۴
- جدول ۱-۴: مقایسه الگوریتم‌های منفرد و ترکیبی DES^۳ و AES256 (Shah,2020) ۲۸

فهرست علائم اختصاری

<i>ABE</i>	<i>Attribute Based Encryption</i>	رمزگذاری مبتنی بر خصوصیات
<i>AES</i>	<i>Advance Encryption Standard</i>	استاندارد رمزگذاری پیشرفته
<i>DES</i>	<i>Data Encryption Standard</i>	استاندارد رمزگذاری داده
<i>GDPR</i>	<i>General Data Protection Regulation</i>	مقررات عمومی حفاظت اطلاعات
<i>HIPAA</i>	<i>Health Insurance Portability and Accountability Act</i>	قانون قابلیت انتقال و مسئولیت بیمه سلامت
<i>IFHDS</i>	<i>Intelligent Framework for Healthcare Data Security</i>	چارچوب هوشمند برای امنیت داده های مراقبت های بهداشتی
<i>LSB</i>	<i>Least Significant Bit</i>	جز کم اهمیت
<i>MSD</i>	<i>Mass storage Device</i>	دستگاه ذخیره سازی انبوه
<i>MR No</i>	<i>Medical Record No</i>	شماره پرونده پزشکی
<i>PHI</i>	<i>Protected Health Information</i>	داده های مراقبت بهداشتی محافظت شده
<i>RDBMS</i>	<i>Relational Database Management System</i>	سیستم مدیریت داده های رابطه ای
<i>RSA</i>	<i>Rivest, Shamir, and Adelman</i>	ریوست، شمیر و عادل من
<i>SHA</i>	<i>Secure Hash Algorithm</i>	الگوریتم هش امنیتی
<i>SNAP</i>	<i>Subnetwork Access Protocol</i>	پروتکل دسترسی زیر شبکه
<i>Three DES</i>	<i>Triple Data Encryption Standard</i>	استاندارد رمزگذاری داده سه گانه

چکیده

اکنون عصر محاسبات ابری است و این موضوع برای هر سازمانی به بخشی جدایی ناپذیر تبدیل شده است و برای کلیه سازمان‌ها مانند آموزش، دولت، بخش عمومی، بخش بهداشت و درمان به همان اندازه اهمیت دارد. ویژگی‌های اصلی رایانش ابری؛ شبکه گسترده، منابع مشترک، کشش سریع و پرداخت به ازای هر استفاده می‌باشد. رایانش ابری همچنین خدمات بسیار بالقوه‌ای را به بخش مراقبت‌های بهداشتی مبتنی بر فناوری اطلاعات ارائه می‌دهد. در مدل رایانش ابری بیمار می‌تواند از هر پزشکی در هر جای دنیا مشاوره بگیرد. دو نوع اطلاعات بیمار وجود دارد: ۱- اطلاعات سلامت محافظت شده / حساس ۲- اطلاعات عمومی. اطلاعات محافظت شده (شماره تلفن، ای تی ام، شماره امنیتی و غیره) در مقایسه با اطلاعات عمومی به محرمانگی بیشتری نیاز دارد. بنابراین برخی از اطلاعات بهداشتی محافظت شده بدون اجتماع بیمار (نام عمومی بیماری، علائم) برای آزمایش‌های تجربی بسیار مفید خواهد بود. وقتی داده‌ها در فضای ابری ذخیره می‌شوند، به وسیله رازداری، یکپارچگی و در دسترس بودن، از اطلاعات بهداشتی محافظت می‌شود. انواع مختلف حملات ممکن است به اطلاعات بهداشتی محافظت شده در ابر وجود داشته باشد. به عنوان مثال اگر اطلاعات کارت بیمار توسط هکر هک شود؛ ممکن است تمام پول خود را از دست بدهد. به همین ترتیب، اگر اطلاعات بیماری یک فرد مشهور به بیرون درز کند، ممکن است حرفه خود را از دست بدهد. به همین دلیل اطلاعات محافظت شده و حساس، به حفاظت از محیط ابر احتیاج دارند. روش‌های رمزنگاری تکنیک‌های مختلفی را برای محافظت از داده‌های ذخیره شده در محیط ابر ارائه می‌دهند. در این پایان‌نامه، ما برای اطمینان از محرمانه بودن اطلاعات ذخیره شده در محیط ابر، یک روش رمزگذاری چند لایه را پیشنهاد کرده ایم. این تکنیک پیشنهادی در صورت استفاده در قالب چند لایه، امنیت تکنیک‌های رمزنگاری را بهبود می‌بخشد. یک سیستم محلی برای آزمایش تنظیم کرده ایم. از پایگاه داده رابطه‌ای و فریم‌ورک ۴٫۵ استفاده کرده ایم. مجموعه‌ای از ۵۰۰ پرونده ساختگی بیمار برای استفاده از روش‌های پیشنهادی استفاده می‌شود. این آزمایش برای بررسی محرمانگی روش‌های پیشنهادی انجام شده است. این آزمایش به ما نشان می‌دهد که وقتی داده‌ها در محیط ابری هستند، تکنیک‌های رمزگذاری چند لایه برای بخش‌های بهداشت عمومی مناسب‌ترند. (Shah, ۲۰۲۰)

کلمات کلیدی: رایانش ابری^۱، داده‌های مراقبت‌های بهداشتی^۲، رمزگذاری، کلید

^۱ Cloud computing

^۲ healthcare

فصل اول

۱. مقدمه

محیط مبتنی بر ابر روز به روز در حال پیشرفت است و بسیاری از سازمان‌ها به سمت محیط ابر تغییر مسیر می‌دهند. به همین ترتیب، بخش مراقبت‌های بهداشتی مبتنی بر فناوری اطلاعات به دلیل مزایایی که دارد، به عنوان مثال در دسترس بودن در هر مکان، هر زمان و منابع اندازه گیری شده، به سمت محیط ابر در حال حرکت است. داده‌های بیمار در قالب الکترونیکی در فضای ابری ذخیره می‌شود. برای مشاوره و درمان بیشتر می‌توان از طریق اینترنت در دسترس بود. بیمار می‌تواند از هر دکتری که در اینترنت در دسترس است؛ از هر نقطه از جهان، مشاور بگیرد. داده‌های دیجیتال بستری را برای پزشکان فراهم می‌کنند که بتوانند بیماران خود را تحت نظر بگیرند. بنابراین با اختراع اینترنت و رایانش ابری، کیفیت خدمات بخش بهداشت و درمان مبتنی بر فناوری اطلاعات نیز روز به روز بهبود می‌یابد. اما حملاتی مانند سرقت اطلاعات محافظت شده/ حساس، DoS، DDoS و غیره در محیط رایانش ابری وجود دارد. به همین دلیل محرمانگی و حریم خصوصی داده‌های بیمار در فضای ابری بیشتر مورد توجه قرار می‌گیرد زیرا به طور عمومی در دسترس است. اگر اطلاعات محرمانه بیمار نقض شود، ممکن است بیمار دچار مشکلات زیادی شود، به عنوان مثال اگر شناسه ایمیل شخصی افراد مشهور هک شود، ممکن است شهرت خود را از دست بدهد و غیره. به همین ترتیب، اگر اطلاعات کارت اعتباری یا اطلاعات حساب به بیرون درز کند، ممکن است بیمار تمام دارایی خود را از دست بدهد. این‌ها دلایلی است که نیاز به افزایش امنیت و حفاظت از داده‌ها دارد و به همین دلیل HIPAA و GDPR برای محافظت از صفات PHI نقش دارند. (Shah, ۲۰۲۰)

رایانش ابری، سرویس محاسباتی مورد تقاضا است. (منابع محاسباتی در صورت تقاضا و در حد نیاز در دسترس هستند.) که بیشترین امکانات را در اختیار بخش‌های مراقبت‌های بهداشتی مورد نیاز بیماران قرار می‌دهد. داده‌ها به ساده‌ترین صورت و حتی از راه دور ذخیره و بازیابی می‌شوند و امکان تغییر دارند. در واقع بیمارستان‌ها نیازی به ذخیره‌سازی محلی داده‌ها ندارند و فقط کافی است سرور مورد نیاز جهت دسترسی به اطلاعات را بخرند. هدف اصلی رایانش ابری، به اشتراک گذاری منابع و دسترسی بهینه به آن‌ها است.

خدمات محاسبات ابری برای بخش بهداشت و درمان به دلایل زیر مفید است:

- خدمات رایانش ابری در دسترس هستند و از هر مکانی که سرویس اینترنت در دسترس باشد، می‌توان به داده‌های بیمار دسترسی داشت.
- پرداخت با توجه به نیاز ذخیره‌سازی و استفاده از داده‌های بیمار انجام می‌شود.
- هیچ هزینه نگهداری، پرداخت اضافی و هزینه مدیریت، مدیر شبکه، اتاق، برق به بخش بهداشت الکترونیکی مورد نیاز نیست.

- اشتراک منابع به این معنی است که ممکن است یک سرور بین چندین سازمان بهداشتی به اشتراک گذاشته شود. از این طریق حداکثر استفاده از منابع حاصل خواهد شد.
 - عملکرد سرورها توسط پرسنل با کیفیت فنی اندازه‌گیری می‌شود. (Shah, ۲۰۲۰)
- برای درک مفهوم رایانش ابری شکل ۱-۱ بسیار مفید است که منبع اصلی شکل را در پاورقی ذکر کرده‌ام.



شکل ۱-۱: رایانش ابری^۳

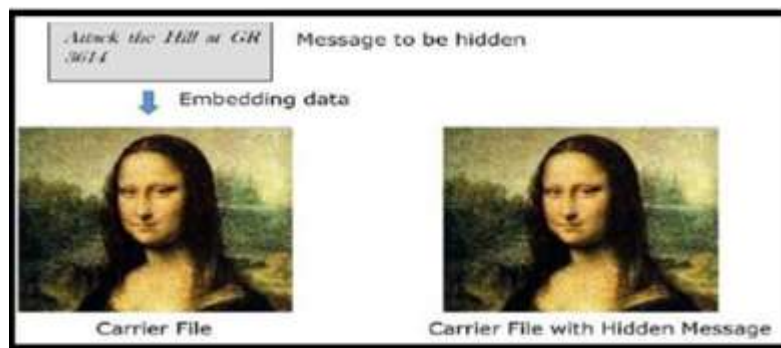
- NIST (موسسه بین‌المللی استانداردها و تکنولوژی) پنج مزیت رایانش ابری را به شرح زیر بیان می‌کند:
- در صورت تقاضا و سلف سرویس، خدمات در صورت تقاضا در دسترس است.
 - کشش سریع به این معنی است که نیازهای سخت‌افزاری و نرم‌افزاری بدون تلاش زیاد قابل ارتقا است.
 - قابلیت‌های دسترسی به شبکه گسترده در اینترنت موجود است و روش‌های دستیابی استاندارد است.
 - منبع تجمع به معنای به اشتراک‌گذاری منابع است.
 - هزینه خدمات اندازه‌گیری مانند استفاده از اینترنت یا خدمات اتومبیل است.^۴
- رایانش ابری به دلیل زیرساخت‌هایش، سرعت و بودجه انعطاف‌پذیری، به مورد حیاتی فناوری اطلاعات تبدیل شده است. با استفاده از ویژگی‌های سلف سرویس، هر کاربر می‌تواند از ویژگی‌های مقیاس‌پذیر استفاده کند و بسته به نیاز، استفاده را ارتقا دهد. این فناوری انواع خاصی از خدمات ذکر شده زیر را ارائه می‌دهد که کاربر می‌تواند از سیستم عامل ابری بدست آورد. (Gao, Thiebes, Sunyaev, ۲۰۱۸)
- این خدمات شامل نرم‌افزار به عنوان سرویس، بسترهای نرم‌افزاری به عنوان سرویس، زیرساخت به عنوان سرویس می‌شود که در مقاله اصلی به آن پرداخته شده است و در این پایان‌نامه هرکدام مختصراً توضیح داده شده‌اند.

^۳ <https://medium.com/@outrightsystems/cloud-computing-in-business-ab۱۹f۳۰۸۲۲۱d>

^۴ <https://timesofcloud.com/cloud-tutorial/characteristics-of-cloud-computing-as-per-nist>

رمزنگاری، رمزگذاری تبدیل متن ساده به متن مخفی برای ایجاد امنیت بیشتر است. داده‌های ذخیره‌شده بیمار در ابر به حفاظت نیاز دارند و لذا می‌توان با تکنیک‌های رمزگذاری، سطح محرمانگی داده‌های مربوط به بیمار را بهبود بخشید. رمزنگاری از تکنیک‌های ریاضی استفاده می‌کند که مقاله "تاریخچه مختصری از رمزگذاری"^۵ به آن پرداخته است؛ این تکنیک‌های بر مبنای کلید است.

استگانوگرافی نوعی دیگر از رمزنگاری است. شکل ۱-۲ را ببینید؛ در این فرم رمزنگاری، اطلاعات علاوه بر محافظت به گونه‌ای محرمانه می‌مانند که فرد غیرمجاز نتواند یک نشانه از پنهان‌نگاری نامرئی اطلاعات بدست آورد. در استگانوگراف، یک متجاوز یا یک گیرنده ناخواسته نمی‌داند که اطلاعاتی که در مقابل او قرار دارد؛ حاوی اطلاعات مخفی است.



شکل ۱-۲: رمزنگاری استگانوگرافی (Shah, ۲۰۲۰)

مقایسه مختصری بین رمزنگاری کلاسیک و مدرن در جدول ۱-۱ نشان داده شده است.

جدول ۱-۱: مقایسه بین رمزنگاری کلاسیک و مدرن (Shah, ۲۰۲۰)

نوین	کلاسیک
با داده‌های باینری کار می‌کند	با حروف و ارقام کار می‌کند
در تکنیک‌های مدرن الگوریتم‌ها به طور عمومی شناخته می‌شوند و کلیدها از داده‌ها محافظت می‌کنند.	در تکنیک‌های کلاسیک فقط فرستنده و گیرنده با یکدیگر در ارتباط هستند.
اما در تکنیک‌های مدرن فقط کلید مخفی، مورد نیاز است نه کل رمزنگاری	در تکنیک‌های کلاسیک، برای ارتباطات ایمن کل رمزنگاری مورد نیاز است.

^۵ T. M. Damico, "A brief history of cryptography," *Inquiries Journal*, vol. 1, no. 11, 2009.

۱-۱ تعریف مسئله و بیان سؤال‌های اصلی تحقیق

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. در این گزارش، براساس پایان‌نامه انتخابی و منابع مرجع، پس از طرح مباحث، در فصل چهار به سوالات زیر پاسخ داده می‌شود:

۱. چه نوع تکنیک‌های محرمانگی داده برای محیط مبتنی بر ابر در دسترس است؟
۲. عمده‌ترین ایرادات و نقایص موجود در این تکنیک‌ها چیست؟
۳. رویکردهای پذیرفته شده در ادبیات کدام است؟
۴. چگونه می‌توان از روش‌های رمزگذاری مبتنی بر چند لایه برای حفظ محرمانه بودن داده‌های مراقبت‌های بهداشتی استفاده کرد؟

۲-۱ ضرورت تحقیق

بعضی از اطلاعات مربوط به بیمار ضرورت دارد که محافظت شده باشد و توسط افراد غیرمجاز دیده نشده یا تغییر داده نشوند. اگر اطلاعات بیمار و داده‌های مراقبت‌های بهداشتی دسترسی غیرمجاز پیدا کند؛ دو نوع خطر وجود دارد:

- ۱- ضرر مالی و از دست دادن اطلاعات بیمار، مثلاً در مورد بیمار ممکن است با سرقت رفتن کارت اعتباری و رمزهای وارد شده در سیستم، پول خود را از دست بدهد.
 - ۲- در صورت شکایت بیمار، اعتبار سازمان خدشه دار می‌شود.
- پس موضوع این تحقیق برای مدیریت و پیشگیری از بروز خطرات فوق ضروری است.

۱-۳ هدف‌ها

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 این جا هدف استفاده از الگوریتم‌های چندگانه برای حفظ محرمانگی داده‌ها است.

۱-۴ چه کاربردهایی از انجام این تحقیق متصور است؟

- بالا رفتن سطح امنیت و محرمانگی داده‌ها با الگوریتم‌های رمز گذاری چندلایه
- در بهبود وضعیت امنیتی و اعتماد به بیمارستان‌ها، بیمه، سازمان‌های مربوطه
- در حفظ و نگهداری دائمی اطلاعات مربوط به بیمار و پرسنل در محیط رایانش ابری

۱-۵ روش و مراحل انجام تحقیق

روش انجام این تحقیق به صورت کتابخانه‌ای است. منابع مورد استفاده شامل پایان نامه، مقالات، تحقیقات علمی و پژوهشی، کتب و جستجوهای اینترنتی در زمینه‌ی الگوریتم‌های رمز گذاری و حفظ امنیت داده‌های مراقبت بهداشتی است. در این راستا یک پایان‌نامه انتخاب شد (Shah, ۲۰۲۰) و با بررسی ساختار پایان نامه و منابع مرجع، توانستم موضوع درک و تجزیه و تحلیل و بیان کنم.

۱-۶ سازمان پایان‌نامه مورد بررسی

فصل‌های این پایان‌نامه به صورت ذیل مرتب شده است:

- فصل ۲ درباره مرور ادبیات است که در آن ما تکنیک‌های مختلف پیشنهادی را شرح داده‌ایم و یک تحلیل مقایسه‌ای درباره این تکنیک‌ها انجام داده‌ایم.
- فصل ۳ مربوط به تنظیمات آزمایشی طرح پیشنهادی است که در آن ما نحوه تهیه مجموعه داده، نحوه رمزگذاری در RDBMS و نحوه عملکرد ما را شرح داده‌ایم.
- در فصل ۴، نیازهای سخت افزاری و نرم افزاری برای نصب آزمایشی، نحوه انجام آزمایشی و بحث درباره نتایج، ارائه شده است.
- فصل ۵ درباره نتیجه‌گیری و کارهای آینده است. (Shah, ۲۰۲۰)

۱-۷ ساختار گزارش تحقیق

فصل اول به تعریف و مقدمه و دلایل نیاز به طرح ارائه شده پرداخته می‌شود. فصل دوم به مفاهیم عمومی رمزگذاری پرداخته می‌شود. فصل سوم مروری است بر کارهای انجام شده طرح پیشنهادی پایان‌نامه فصل چهارم به کاربردها و مزایا و معایب الگوریتم‌های رمزگذاری پرداخته می‌شود. فصل پنجم نیز به جمع‌بندی و نتیجه‌گیری پرداخته می‌شود.

فصل دوم

۲. مفاهیم عمومی رمزگذاری و پیشینه تحقیق

۱-۲ انواع طرح‌های رمزنگاری

الگوریتم‌های رمزگذاری به دو دسته تقسیم می‌شوند:

- رمزگذاری کلید متقارن
- رمزگذاری کلید نامتقارن

۱-۱-۲ رمزگذاری متقارن

در این نوع رمزگذاری فقط یک کلید برای رمزگذاری و رمزگشایی استفاده می‌شود.

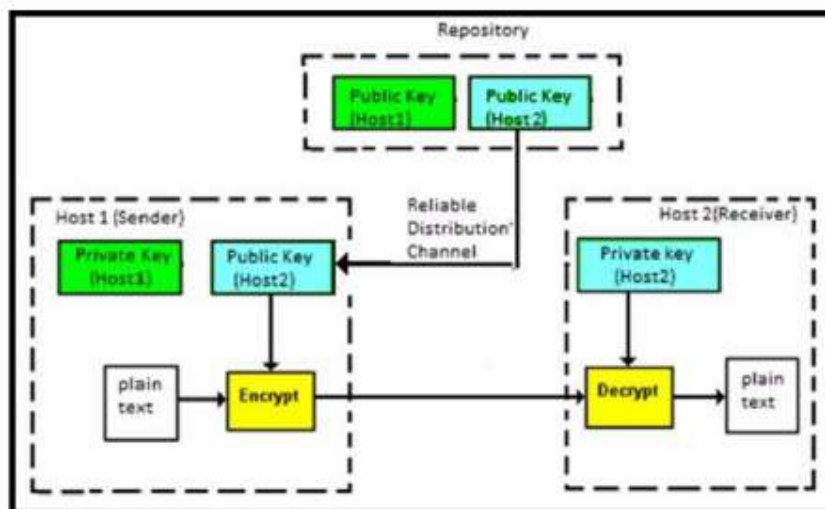
این کلید دارای ویژگی‌های زیر است:

- طول کلید روند رمزگذاری و رمزگشایی آن را سریع‌تر یا آهسته‌تر می‌کند.
- کمترین پردازش مصرف می‌شود.
- یک مکانیسم ارتباط سریع بین دو طرف برای برقراری ارتباط امن است.
- کلیدها می‌توانند بصورت دوره‌ای یا بر اساس نیاز تغییر کنند.
- قبل از شروع ارتباط بین طرفین، می‌توان کلید را به اشتراک گذاشت. (Yan, Deng, Varadharajan, 2017)

۲-۱-۲ رمزگذاری نامتقارن

در این حالت یک فرستنده و یک گیرنده داریم. کلید عمومی برای همه شناخته شده است ولی کلید خصوصی برای رمزگشایی استفاده می‌شود و دارای ویژگی‌های زیر است.

- از دو کلید خصوصی و عمومی برای رمزگذاری و رمزگشایی استفاده می‌شود.
- کلید عمومی در اینترنت است و هر کسی که بخواهد داده‌ها را رمزگذاری کند؛ می‌تواند آن را دریافت کند. این کلید از نظر ریاضی با کلید خصوصی پیوند خورده است و فقط شخص مجاز می‌تواند آن را رمزگشایی کند.
- هنگامی که شخص A نیاز به ارسال اطلاعات a به شخص B دارد، وی کلید عمومی شخص B را از مخزن به دست می‌آورد؛ داده‌ها را رمزگذاری می‌کند و انتقال می‌دهد.
- شخص B از کلید خصوصی خود برای استخراج متن ساده استفاده می‌کند.
- طول کلیدها بزرگ است و از این رو روند رمزگذاری-رمزگشایی کندتر است.
- پردازش پردازنده برای اجرای الگوریتم نامتقارن بالاتر است. (Yan, et. al., 2017)



شکل ۱-۲: رمزگذاری نامتقارن کلید^۶

۲-۲ سرویس امنیتی برای رمزنگاری داده‌های مراقبت‌های بهداشتی

ویژگی‌های زیر را می‌توان از رمزنگاری مربوط به داده‌های بیمار بدست آورد. (Babatunde, Taiwo, Dada, 2018)

محرمانه بودن

محرمانگی اساسی‌ترین سرویس امنیتی رمزنگاری است که اطلاعات پزشکی بیمار را از دسترسی غیرمجاز پنهان می‌کند. همچنین به عنوان راز و حریم خصوصی شناخته می‌شود که تضمین می‌کند به جز کاربران اصلی، شخصی نتواند پیام را بخواند. برای رمزگذاری داده‌ها از الگوریتم‌های مختلف ریاضی استفاده می‌شود. با استفاده از این الگوریتم‌ها می‌توان به سطحی از محرمانگی دست یافت.

جامعیت

جامعیت با اصلاح داده‌ها سروکار دارد. این سرویس، داده‌های بیمار را تأیید می‌کند و تضمین می‌کند توسط هیچ شخص غیر مجاز، آگاهانه یا ناآگاهانه داده‌ها اصلاح نمی‌شوند. همچنین از عدم تغییر داده‌ها پس از ایجاد آن اطمینان حاصل می‌کند. جامعیت نمی‌تواند تغییر در اطلاعات را متوقف کند. فقط شواهدی را برای شناسایی اطلاعات دستکاری شده فراهم می‌کند. این نکات امنیتی به ویژه هنگامی که داده‌ها در فضای ابری به کار می‌روند، نقش بسیار مهمی در امنیت بازی می‌کنند زیرا حفاظت بیشتری در ابر وجود دارد.

اعتبار

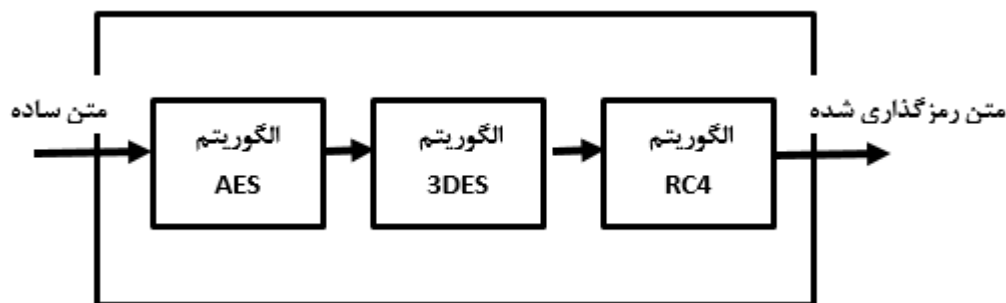
اصالت اطلاعات را از طرف فرستنده تضمین می‌دهد و به گیرنده اطمینان می‌دهد که اطلاعات دریافتی از کاربران واقعی است که شامل دو نوع است:

^۶ <https://www.tutorialspoint.com/cryptography/cryptosystems.htm/>

احراز هویت موجودیت: این اطمینان را به شما می‌دهد که پیام یا اطلاعات از یک نهاد خاص دریافت شده است. احراز هویت پیام: این اطلاعات بدون توصیف مسیر یا سیستمی که این اطلاعات را ارسال کرده است، اطلاعات مربوط به مبدع پیام را ارائه می‌دهد.

۳-۲ رمزگذاری چند لایه

متن ساده را به یک الگوریتم با کلید منتقل خواهیم کرد و خروجی آن الگوریتم با کلید متفاوت به الگوریتم دوم منتقل می‌شود. چنین لایه‌هایی می‌توانند شامل دو یا چند الگوریتم باشند. بنابراین، می‌توان به یک سطح محرمانگی دست یافت. شکل ۲-۲ روش رمزگذاری چندلایه را نشان می‌دهد.



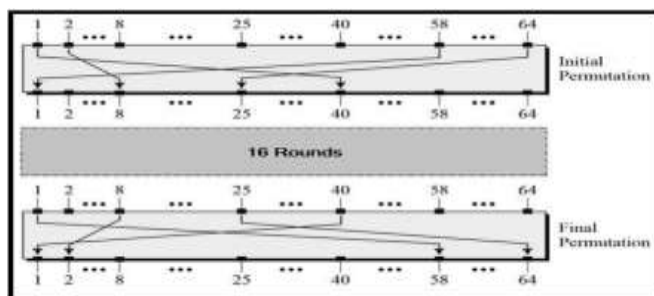
شکل ۲-۲: روش رمزگذاری چند لایه

۴-۲ کار الگوریتم‌های مورد استفاده در طرح پیشنهادی

اولین الگوریتمی که توسط *NIST* نیز مطرح است و در این جا به آن توجه شده است. استاندارد رمزگذاری داده‌ها (*DES*) یک الگوریتم متقارن است. پیاده‌سازی الگوریتم *DES* براساس رمزگذاری فایستل است که در ۱۶ دور انجام می‌شود. اندازه بلوک و اندازه کلید الگوریتم ۶۴ بیت است ۵۶ بیت برای رمزگذاری و ۸ بیت اضافه برای مصارف دیگر. از عملیات زیر در *DES* استفاده می‌شود:

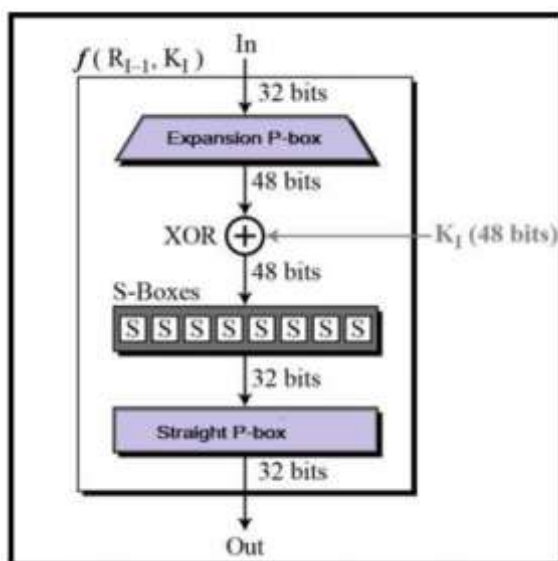
- جایگزینی اولیه
- عملکرد *Round*
- گسترش جعبه جایگشت
- تولید کلید

جایگشت اولیه: در شکل ۳-۲ این مفهوم نشان داده شده است:



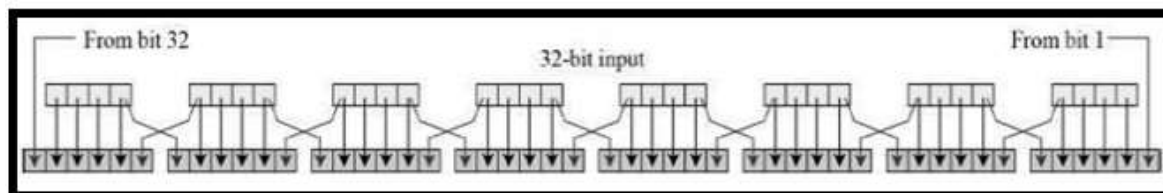
شکل ۳-۲: جایگزینی اولیه (Shah, ۲۰۲۰)

عملکرد *Round*: این عملکرد یک عملکرد مهم در دور هسته اصلی الگوریتم *DES* است. همان‌طور که در شکل ۲-۴ نمایش داده شده است کلاً ۴۸ بیت داریم که ۳۲ بیت آن در حالت درست هستند.



شکل ۴-۲: تابع Round (Shah, ۲۰۲۰)

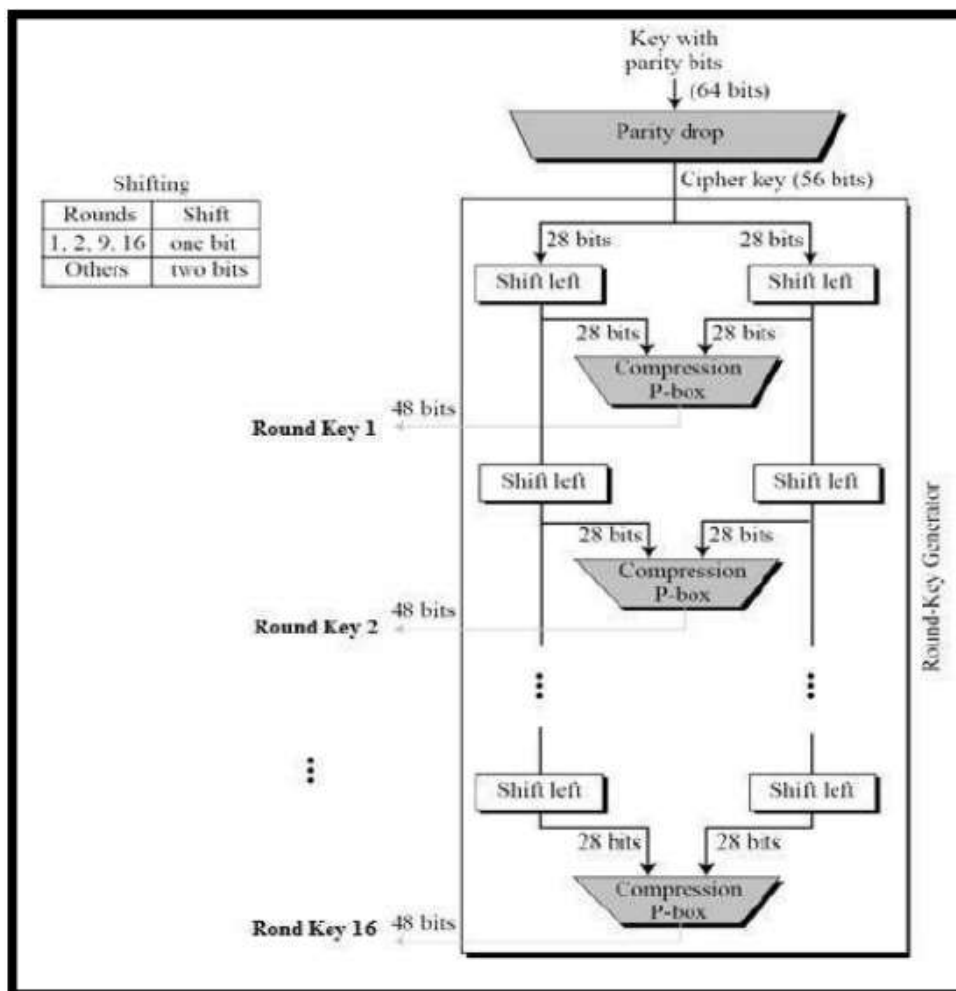
گسترش جعبه جایگشت: توجه داشته باشید که کلید دور ۴۸ بیت است و برای ایجاد ورودی ۳۲ بیت از سمت راست آن ۴۸ بیت استفاده می‌کنیم. در شکل ۲-۵ مفهوم گسترش نشان داده شده است.



شکل ۵-۲: گسترش جعبه جایگزینی^۷

تولید کلید: بخش نهایی و مهم این الگوریتم تولید کلید است. تابع *Round* که بالاتر مطرح شد؛ ۱۶ بیت کلید را ایجاد می‌کند که در پایان نامه با شکل ۲-۶ به وضوح نشان داده شده است.

^۷ <https://www.tutorialspoint.com/cryptography/cryptosystems.htm>

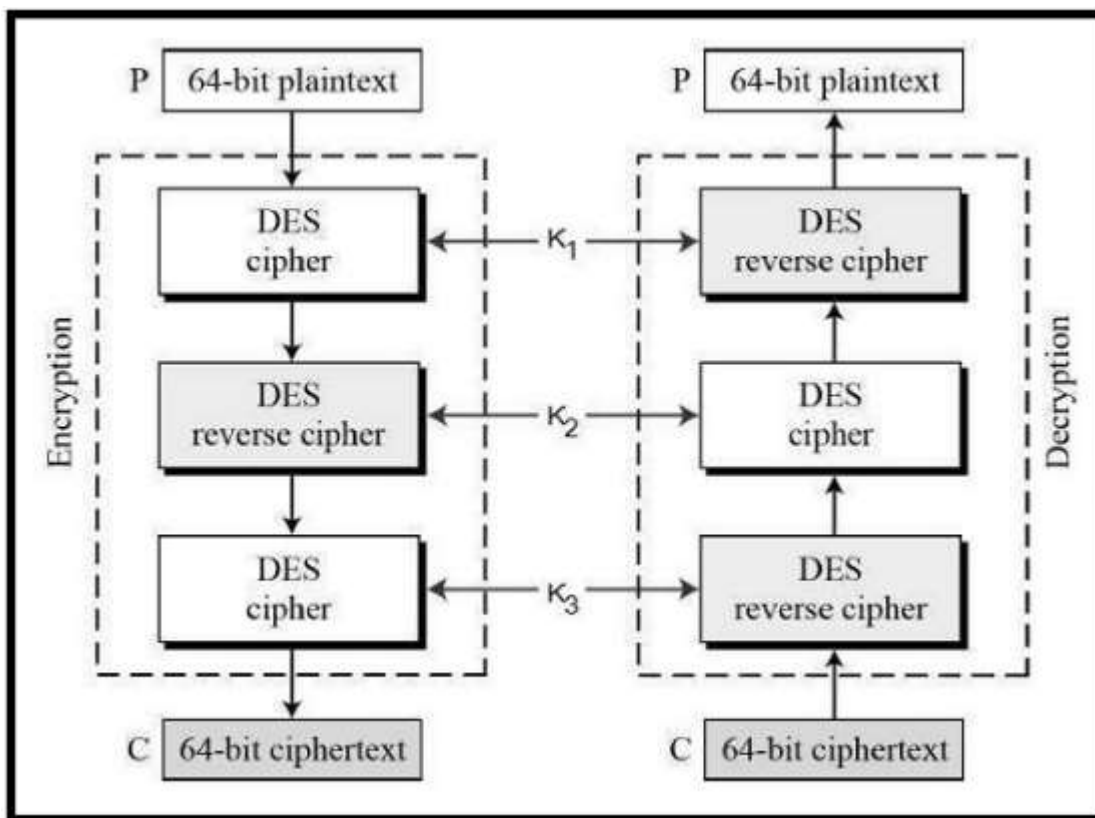


شکل ۲-۶: تولید کلید^۸

الگوریتم DES^۳: فرایند رمزگذاری و رمزگشایی به شرح زیر است:

- $K1$ متن ساده را رمزگذاری می‌کند.
 - خروجی اول توسط $K2$ رمزگشایی می‌شود.
 - و در آخرین مرحله خروجی بلوک دوم دوباره با $K3$ رمزگشایی می‌شود.
 - این متن رمز نهایی است.
 - رمزگشایی فرایند معکوس است.
- اگر کلیدهای $K1$ ، $K2$ ، $K3$ یکسان استفاده شود، مانند DES کار می‌کند. (Shah, 2020)
- این الگوریتم در نشان ۲-۷ نشان داده شده است.

^۸ <https://www.tutorialspoint.com/cryptography/cryptosystems.htm>



شکل ۷-۲: نمودار معماری DES^۹

استاندارد پیشرفته رمزگذاری *AES*: وینسنت ریچمن، جوآن دیمن این الگوریتم را در سال ۱۹۹۸ منتشر کردند. در آن از سه اندازه کلید ۱۲۸، ۱۹۲ و ۲۵۶ بیت و اندازه بلوک ۲۵۶ بیت استفاده می‌شود. ویژگی‌های اصلی *AES* به شرح زیر است:

- این رمزنگاری بلوکی است.
- الگوریتم کلید متقارن (رمزگذاری و رمزگشایی را می‌توان با تنها یک کلید انجام داد).
- اندازه‌های مختلف کلید را می‌توان با توجه به نیاز استفاده کرد. به عنوان مثال ۱۲۸ و ۱۹۲ و ۲۵۶ بیت اما اندازه کلید ۲۵۶ ایمن‌تر است.
- قدرت محاسبه سریع‌تر است.
- معماری باز است و می‌تواند به راحتی به هر زبان رایانه‌ای طراحی شود. (Shah, 2020)

کار الگوریتم *AES*

AES روی معماری فایستل کار نمی‌کند. در فایستل نیمی از بلوک داده برای اصلاح نیمی دیگر از داده‌ها استفاده می‌شود. *AES* روی کل بلوک به عنوان یک ماتریس واحد برای جایگشت و جایگزینی در هر دور کار می‌کند. برای درک بیشتر مطلب، از کتاب پایگاه داده پیشرفته دکتر احمدفراهی استفاده می‌کنم.

^۹ <https://www.tutorialspoint.com/cryptography/cryptosystems.htm>

این الگوریتم بایت به بایت کار می‌کند و ورودی اصلی را با کلید رمزنگاری در یک ماتریس 4×4 جفت می‌کند. کلید به طریقی تقسیم یا برنامه‌ریزی شده است که بتواند در مراحل مختلف تکرار به تدریج تزریق شود. اولین قسمت کلید قبل از شروع پروسه‌ی ۱۰ مرحله‌ای تزریق می‌شود. در هر کدام از این مراحل، بایت‌ها جابجا می‌شوند، ردیف‌ها نوبت پیدا می‌کنند و ستون‌ها ترکیب می‌شوند. (فراهی، ۱۳۹۸)

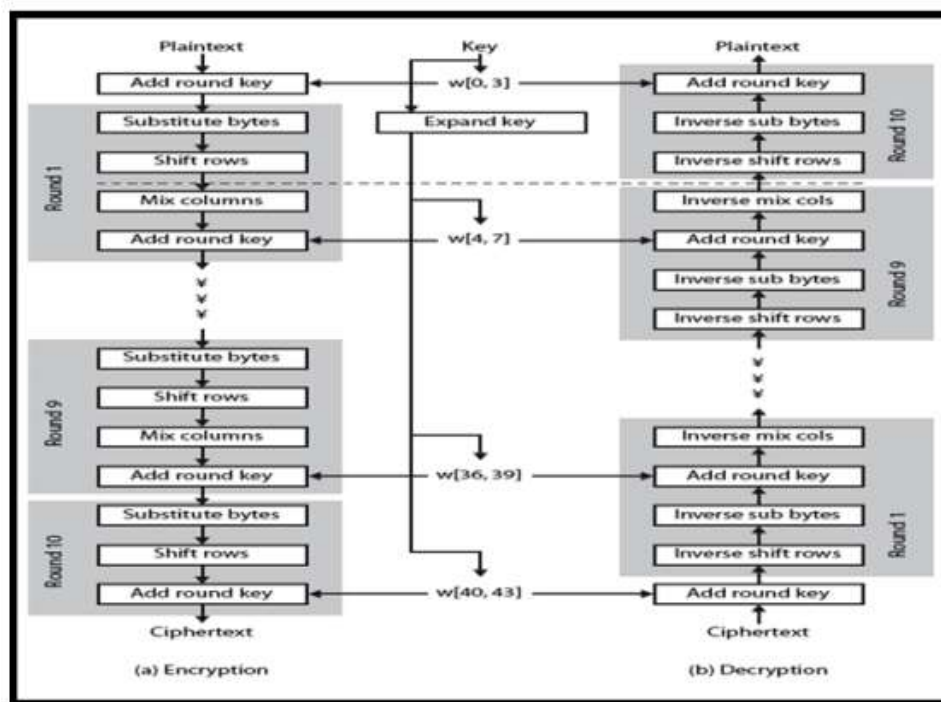
کلید اصلی به مجموعه‌ای از چهل و چهار ۳۲ بیت کلمه تقسیم شده است. چهار کلمه مشخص با اندازه ۱۲۸ بیت برای کلید *Round* در هر دور استفاده می‌شود.

در کل چهار مرحله در *AES* استفاده شده است، یکی برای جایگزینی و سه مرحله باقیمانده برای جایگشت است.

- **بایت های جایگزین:** از *s-box* برای اعمال بایت بایت و جایگشت روی بلوک استفاده می‌کند.
- *Shift Rows Operation*: این یک عملیات جایگزینی ساده است.
- *Mix Columns Operation*: در این عملیات از روش $GF(2^8)$ برای جایگزینی استفاده می‌شود.
- افزودن عملکرد کلید *Round*: بیتی که با بخشی از کلید منبسط شده در بلوک جاری *XOR* می‌شود.

- ساختار *AES* بسیار آسان است. در مرحله رمزگذاری و رمزگشایی، رمزگذاری با یک مرحله *AddRoundKey* با نه گام آغاز می‌شود، هر گام، چهار دور را تشکیل می‌دهد و به دنبال آن دهمین مرحله از سه گام تشکیل شده است.
- اضافه شدن *Round Key* از کلید استفاده می‌کند: رمزگذاری با یک مرحله *Add Round Key* شروع و پایان می‌یابد.
- اضافه کردن دورهای دور کلید مانند رمز ورنام انجام می‌شود و در صورت استفاده از سه دور باقیمانده برای سردرگمی، سر و صدا و غیرخطی بودن، مشکلی ندارد. اما نکته مهم این است که این مرحله امنیت را بدون استفاده از کلید تأمین می‌کند.
- برگشت هر مرحله بسیار آسان است. یک تابع معکوس در الگوریتم رمزگشایی در هر مرحله از جایگزینی بایت‌ها فعال می‌شود، ردیف‌های *Shift* و مخلوط می‌شوند. تابع معکوس می‌تواند با استفاده از *XOR* در همان دور کلید دور در بلوک به دست آید.
- به طور معمول الگوریتم‌های رمزنگاری بلوک هنگام انجام فرایند رمزگشایی، کلید خرج شده را به ترتیب معکوس استفاده می‌کنند. فرایند رمزگشایی مانند رمزگذاری نیست. اما *AES* به روشی متفاوت عمل می‌کند و رمزگذاری و رمزگشایی با سرعت یکسان انجام می‌شود.

- هنگامی که همه این چهار دور برگشت پذیر هستند، بررسی فرآیند رمزگشایی متن ساده و بازیابی آن، آسان است. شکل فرآیند رمزگذاری و رمزگشایی را در جهت های مخالف عمودی نشان می دهد. در هر نقطه افقی برای رمزگذاری و رمزگشایی یکسان است.
 - دور آخر هر دو فاز فقط شامل سه دور است. باز هم ، اهمیت یک طرح خاص الگوریتم AES است و نیاز است که قابل برگشت باشد. (Shah, 2020)
- ساختار الگوریتم AES در شکل ۸-۲ نشان داده شده است.



شکل ۸-۲: معماری الگوریتم AES (Shah, ۲۰۲۰)

۵-۲ پیشینه تحقیق

در اوایل دهه ۱۹۶۰ معماری سرور مشتری فقط برای رایانه های 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 می شد. برای دسترسی به داده ها و پردازش، از ترمینال های تخلیه استفاده می شد. در سال ۲۰۰۶ آمازون شروع به فعالیت خود در زیر شاخه ای به نام خدمات وب آمازون کرد. گوگل نسخه آزمایشی Google App Engine را در آوریل ۲۰۰۸ 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 ۲۰۱۰ مایکروسافت Azure توسط مایکروسافت منتشر شد.

در سال ۲۰۱۲، موتور محاسبه Google قبل از اینکه در دسامبر ۲۰۱۳ در دسترس عمومی قرار بگیرد، در حالت پیش‌نمایش منتشر شد

در سال ۲۰۱۱ دکتر سلیمان و همکاران^{۱۰} در مقاله‌ای، 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، *DES*^{۱۱} و تابع مقدار هش را معرفی کرده‌اند. نویسندگان از اندازه کلید ۱۹۳ بیت برای لایه ۱ و ۱۲۹ بیت تا ۱۹۲ بیت برای لایه ۲ و ۱۱۲ تا ۱۲۸ بیت برای لایه ۳ و ۸۰ تا ۱۱۱ بیت برای لایه ۴ استفاده کرده‌اند. کار اصلی نویسندگان روی الگوریتم *DES*^{۱۲} است. و از یک الگوریتم برای رمزگذاری و رمزگشایی استفاده می‌شود.

در سال ۲۰۱۳ کیا و همکاران^{۱۱} در مقاله‌ای با استفاده از *SOAP/XML* داده‌ها را با *AES* رمزگذاری کرده‌اند. در سال ۲۰۱۶ ژو و همکاران^{۱۲} 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 کردند که رویکرد آنها کنترل انعطاف‌پذیری در ذخیره‌سازی داده‌ها را فراهم می‌کند.

در سال ۲۰۱۹ سودهیپ و همکار^{۱۳} در مقاله‌ای رمزگذاری مبتنی بر ویژگی سیاست رمزگذاری (*CP-ABE*) را معرفی کرده‌اند. کلید رمزگذاری شامل خط‌مشی‌هایی است و آن‌ها می‌گویند اگر کلید هک شده باشد، آن دسته از سوابق رمزگشایی می‌شوند که کلید آن‌ها هک می‌شود اما بقیه موارد همچنان محافظت می‌شوند.

در سال ۲۰۱۹ هما و همکار^{۱۴}، 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.

در سال ۲۰۱۹ پارا و همکاران^{۱۵} 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.

^{۱۰} R.sulaiman.D.Sharma,W.Ma and D.Tran

^{۱۱} M.M.Kian,M.S.Nabi,B.Zaidan and A.Zaidan

^{۱۲} L. Zhou, V. Varadharajan, and K. Gopinath

^{۱۳} K.Sudheep and Joseph

^{۱۴} V.S.V Hema and R.Kesavan

^{۱۵} S. A. Parah, A. Bashir, M. Manzoor, A. Gulzar, M. Firdous, N. A. Loan, and J. A. Sheikh

در سال ۲۰۱۹ وزید و همکاران^{۱۶} نویسندگان در مورد مدل تهدید و احراز هویت برای دستگاه های مبتنی بر *Iot* در محیط ابر بحث کرده اند و سعی کرده اند چالش های فعلی امنیت و داده های 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 داده اند. در مقاله خود یک مطالعه تطبیقی در مورد هزینه های ارتباطی و فنی و حرفه ای انجام داده اند. محاسن و معایب تکنیک های احراز هویت موجود نیز در دست بررسی است اما راه حل مشخصی پیشنهاد نمی شود.

^{۱۶} M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. Rodrigues

فصل سوم

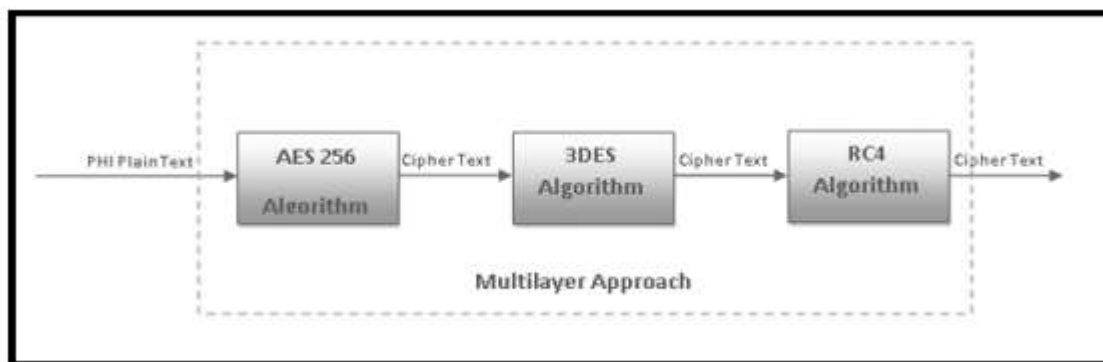
۳. مروری بر کارهای انجام شده

۳-۱ مقدمه

در فصل ۳ پایان نامه مورد بررسی راه اندازی آزمایشی طرح پیشنهادی مدنظر قرار گرفته شده؛ روش های پیشنهادی را تجزیه و تحلیل کرده؛ طرح اخیر بر مفاهیم و اصول رمزگذاری و رمز گشایی متمرکز است. طرح پیشنهادی با الگوریتم چندلایه رمزگذاری، داده های *PHI* را رمزگذاری و محافظت می کند. داده های رمزگذاری شده در سرور ابری قابل اعتماد که احتمالاً مورد نیاز بیمار در آینده، در دسترس خواهد بود. با استفاده از معماری کلاینت/ سرور و از طریق شبکه منتقل شود، طرح فوق توسعه داده شده است و در فصل ۴ پایان نامه مورد بررسی، طرح پیشنهادی تجزیه و تحلیل می شویم که در ادامه به تفکیک توضیح می دهیم.

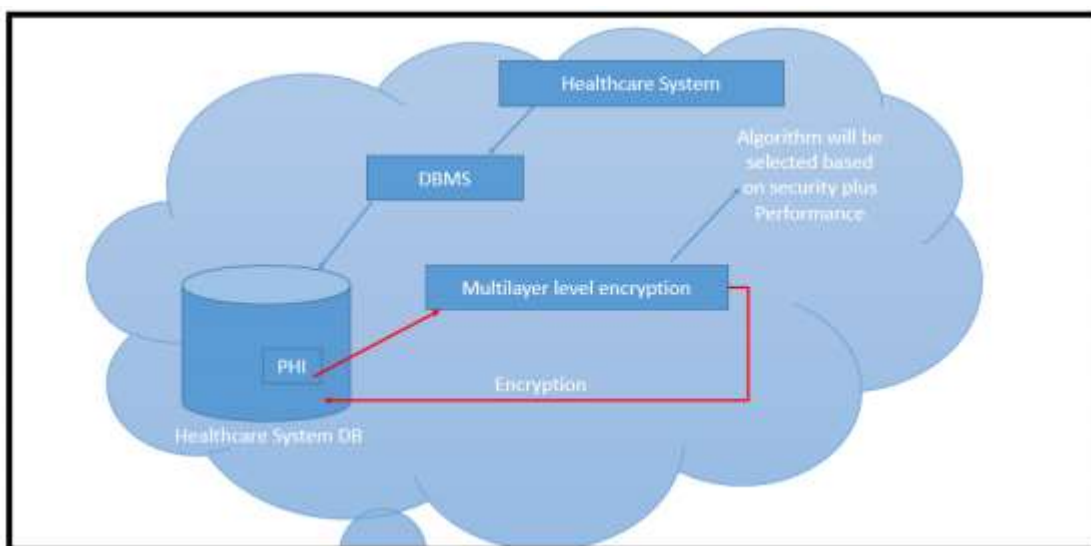
۳-۲ راه اندازی آزمایشی طرح پیشنهادی

ابتدا به تکنیک چندلایه رمزگذاری (شکل ۳-۱) توجه کنید؛ در این حالت متنی که باید محافظت شود؛ وارد سیستم الگوریتم چندگانه می شود. داخل سیستم الگوریتم چندگانه در این مورد خاص، ۳ الگوریتم *AES* و *DES* و *RC4* وجود دارد. خروجی هر الگوریتم، به صورت رمزگذاری شده و دوباره توسط الگوریتم بعدی طبق شکل، رمزگذاری می شود و خروجی نهایی با رمزگذاری چندلایه و ایمنی بالا ایجاد می شود.



شکل ۳-۱: تکنیک محافظت از چند لایه (Shah, ۲۰۲۰)

برای توسعه طرح یک مجموعه داده ساختگی (برای ایمنی بیمار) از حدود ۵۰۰ بیمار انتخاب کرده؛ شکل ۳-۲ یک سیستم مراقبت های بهداشتی به همراه سیستم مدیریت پایگاه داده را نشان می دهد. روی داده ها، الگوریتم های رمزگذاری موجود در *RDBMS* اعمال می شوند و داده ها در محیط ابری ذخیره می شوند.



شکل ۳-۲: نمودار معماری روش شناسی (Shah, ۲۰۲۰)

Receipt #: 1-2020-01-20390	Date: 28/01/2020	Visit: 8
MR No: 1-2018-23524	Name: MUSHTAQ AHMAD S/O MUHAMMAD MASKIN	Category: Free
CNIC: 3740616044471()		
Contact No: 03005049139	Clinic: GLAUCOMA CLINIC (G-8)	Age: 65 Yrs

Payment Mode :	Cash
Reg Fee :	0
Consultation :	200
Discount :	200
Payable Amount :	0

Next Follow-up: ____/____/____

For Web Access use MR No as Username and Password = Xt19&6P@

<https://www.alshifaeye.org/PatientModule/login>

sucoma Counter on 28/1/2020 @ 13:39:

شکل ۳-۳: فیش ورود به سیستم برای بیمار (Shah, ۲۰۲۰)

در آغاز ثبت نام بیماران، شماره *MR* با رمز عبور پیچیده‌ای که به طور تصادفی ایجاد شده است، برای اطلاعات بیمار اختصاص می‌یابد. برای دسترسی در وب سایت (شکل ۳-۳)، 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 *DES* بر روی داده‌ها اعمال می‌کنیم. کلید در *RDBMS* ذخیره می‌شود و توسط سرور *Microsoft SQL* محافظت می‌شود و از رمز عبور محافظت می‌کند. بنابراین برای رمزگذاری و رمزگشایی نیازی به ارائه رمز برای رمزگذاری و رمزگشایی بیمار نیست. (Shah, 2020)

۳-۲-۱ فرآیند رمزگذاری و رمزگشایی در RDBMS

فرایند رمزگذاری کلی با استفاده از *SQL Server* بر روی یک ستون از یک جدول در شکل ۳-۴ نشان داده شده است. کلید اصلی در پایگاه داده، براساس روش متقارن محافظت می شود.

مرحله ۱: ایجاد کلید اصلی

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

مرحله ۲: ایجاد گواهی

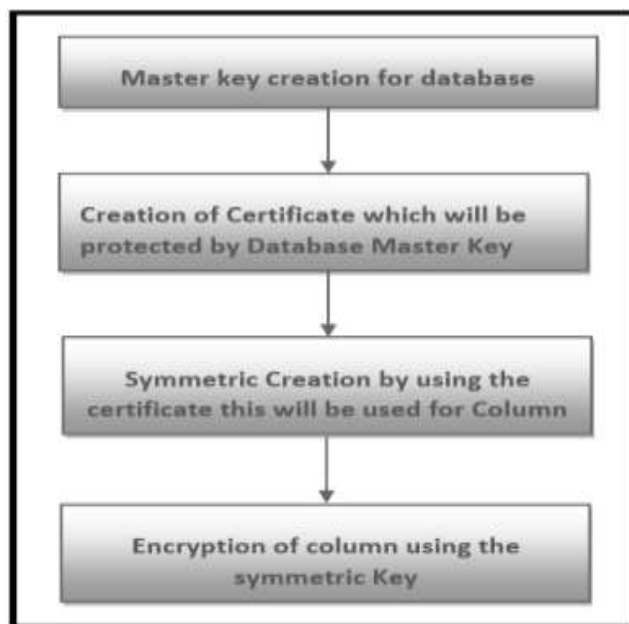
گواهینامه دیجیتالی جهت محافظت از کلید اصلی پایگاه داده ایجاد می شود.

مرحله ۳: ساخت کلید متقارن

یک کلید متقارن برای رمزگذاری و رمزگشایی بر اساس الگوریتم های رمزگذاری در سرور *sql*، ساخته می شود؛ به عنوان مثال *AES128*، *AES192* و *AES256*.

مرحله ۴: رمزگذاری ستون ها

شمای جدول و فیلدهای را رمزگذاری می کنیم.



شکل ۳-۴: فرآیند رمزگذاری کلی (Shah, ۲۰۲۰)

۳-۳ تجزیه و تحلیل طرح پیشنهادی

ما یک مجموعه داده ساختگی از ۵۰۰ بیمار را برای هدف آزمایش آماده کرده ایم. نمونه مجموعه داده در شکل ۳-۵ نشان داده شده است. برخی از ویژگی ها با در نظر گرفتن *GDPR* و *HIPAA* 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 ویژگی ها به ویژه هنگامی که داده ها در فضای ابری قرار

دارند، نیاز به مراقبت بیشتری دارند. برای افزایش سطح محرمانگی، ما خصوصیات ویژه PHI را برای رمزگذاری و رمزگشایی در نظر گرفته ایم. (Shah, 2020)

Patient no	first name	last name	relative name	sex	address	date of birth	date of registration	visit date time	NIC	Phone No
1-2018-10154	REHMAN	BI	MIBRAHIM	1	GILGIT	01/01/1973	08/02/2018	08/02/2018	7110347468740	3409557182
1-2018-10157	MUHAMMAD	NASEER	MUHAMMAD BASEER	0	BANNU	01/01/1970	08/02/2018	08/02/2018	1110154036677	3369115007
1-2018-10159	GHULAB	JAN	ABDUL GHAFOR	1	POONCH	01/01/1956	08/02/2018	08/02/2018	8230327053772	
1-2018-1016	MUHAMMAD	YOUSAF	MUHAMMAD KHAN	0	KOTLI	01/01/1957	04/01/2018	04/01/2018	8120253533745	3445216411
1-2018-1016	MUHAMMAD	YOUSAF	MUHAMMAD KHAN	0	KOTLI	01/01/1957	04/01/2018	04/01/2018	8120253533745	3445216411
1-2018-10162	GHULAM	NABI	MUHAMMAD AJAB KHAN	0	ABBOTABAD	01/01/1958	08/02/2018	08/02/2018	3429439488	3429439488
1-2018-1017	MALIK	ADNAN	MALIK PERVAIZ AKHTAR	0	RAWALPINDI	01/01/1981	04/01/2018	04/01/2018	3740517480127	3485613623
1-2018-10172	ABU	BAKAR	YASIR ALI	0	RWP	08/01/2018	08/02/2018	08/02/2018	1654564564565	3035197907
1-2018-1018	DUA	ZAINAB	M JUNAID	0	RAWALPINDI	01/01/2016	04/01/2018	04/01/2018	3740198364911	3425697212
1-2018-1018	DUA	ZAINAB	M JUNAID	0	RAWALPINDI	01/01/2016	04/01/2018	04/01/2018	3740198364911	3425697212
1-2018-10187	M	MAJID	JHANZAB	0	RWP	01/01/2014	08/02/2018	08/02/2018	4548978978987	3324888716
1-2018-1019	TAYYABA	NASIR	NASIR MEHMOOD	1	RAWALPINDI	01/01/2001	04/01/2018	04/01/2018	3720118671240	
1-2018-10191	RASHID	SOHAIL	M BASHIR	0	RWP	01/01/1989	08/02/2018	08/02/2018	1215648789789	3325576558
1-2018-102	MUHAMMAD	LIAQUAT	DOST MUHAMMAD	0	MURREE	01/01/1950	01/01/2018	01/01/2018	3740468232941	3445363872
1-2018-1020	KHURSHIDA	BIBI	IMTIAZ AHMED ABBASI	1	RAWALPINDI	01/01/1951	04/01/2018	04/01/2018	3740403786010	3165006762

شکل ۳-۵: نمونه مجموعه داده‌های ساختگی (Shah, ۲۰۲۰)

۳-۴ نصب پیکربندی سخت افزار و نرم افزار

۳-۴-۱ سخت افزار مورد نیاز

- پردازنده Intel Core i7-6500U Processor
- Ram ۸ گیگابایتی
- هارد دیسک ۵۰۰ گیگابایتی

۳-۴-۲ سیستم عامل و نرم افزار مورد نیاز

- ویندوز ۱۰ یا بالاتر
- Visual Studio ۱۲ یا ۱۵
- SQL Server 2014 یا بالاتر
- Framework ۴,۵

۳-۵ ایجاد کلیدها و گواهینامه‌ها و رمزگذاری داده‌ها

ایجاد کلید و گواهینامه‌ها با دستورات SQL و مطابق شکل ۳-۶ انجام می‌شود.



شکل ۳-۶: ایجاد کلیدها و گواهینامه‌ها (Shah, ۲۰۲۰)

داده‌های مربوط به بیمار که باید روی ابر بارگذاری شوند؛ تهیه شده و فرآیند رمزگذاری روی آن اعمال می‌شود. داده‌ها در جدول پایگاه داده با فرمت شکل ۳-۷، ذخیره می‌شوند.

```

OPEN SYMMETRIC KEY DProtect1
  DECRYPTION BY CERTIFICATE ThesisCertificate;
select * from patient_registration

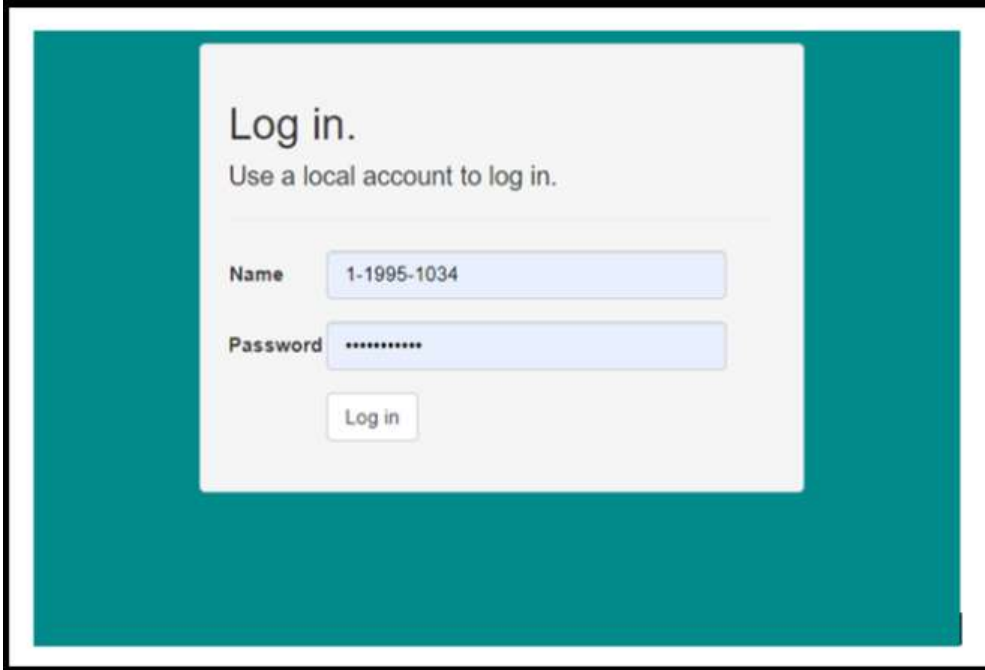
```

Results	Messages
Sencryptedidno	Sencryptedidname
0x001B5E878619244DB23422716A9D716A01000000EF1332D...	0x001B5E878619244DB23422716A9D716A01000000CE96C6...
0x001B5E878619244DB23422716A9D716A01000000FCCB0F9...	0x001B5E878619244DB23422716A9D716A01000000EACB1...
0x001B5E878619244DB23422716A9D716A01000000A0C65D...	0x001B5E878619244DB23422716A9D716A01000000B37BEC...
0x001B5E878619244DB23422716A9D716A0100000007F9072...	0x001B5E878619244DB23422716A9D716A01000000755CFE3...
0x001B5E878619244DB23422716A9D716A010000000ED60631...	0x001B5E878619244DB23422716A9D716A0100000033B4B16...
0x001B5E878619244DB23422716A9D716A010000005ABEAA...	0x001B5E878619244DB23422716A9D716A0100000070152BC...
0x001B5E878619244DB23422716A9D716A01000000D18709F...	0x001B5E878619244DB23422716A9D716A010000000C6623...
0x001B5E878619244DB23422716A9D716A01000000CAAB03...	0x001B5E878619244DB23422716A9D716A01000000A0ABA4...
0x001B5E878619244DB23422716A9D716A0100000015AB299...	0x001B5E878619244DB23422716A9D716A010000000D27970...


شکل ۳-۷: فرم رمزگذاری شده داده‌ها (Shah, ۲۰۲۰)

۶-۳ 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. ورود بیمار در شکل ۸-۳ و جزئیات پرونده پزشکی بیمار در شکل ۹-۳ نشان داده شده است.



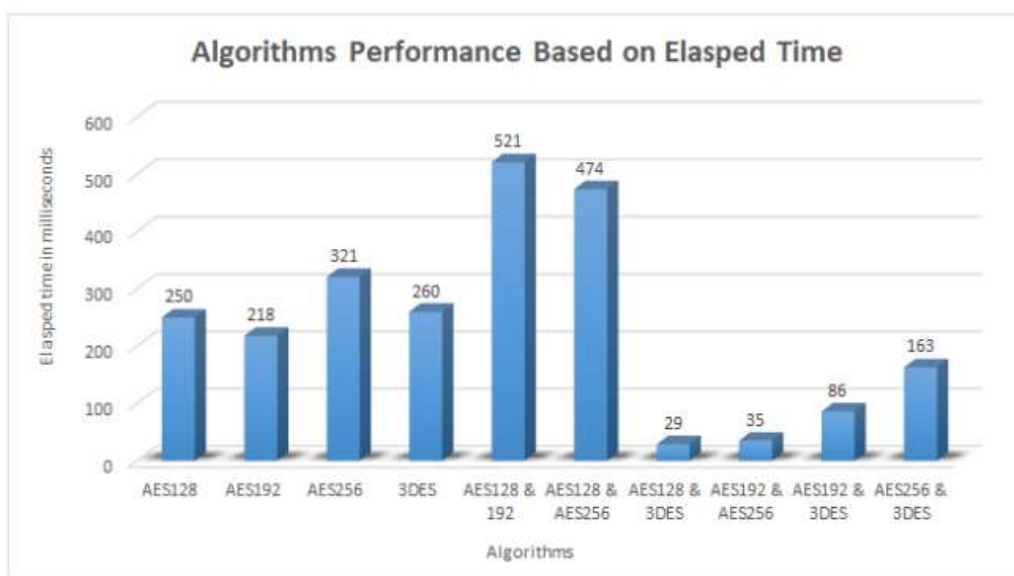
شکل ۸-۳ : صفحه ورود به سیستم برای ورود بیمار (Shah, ۲۰۲۰)



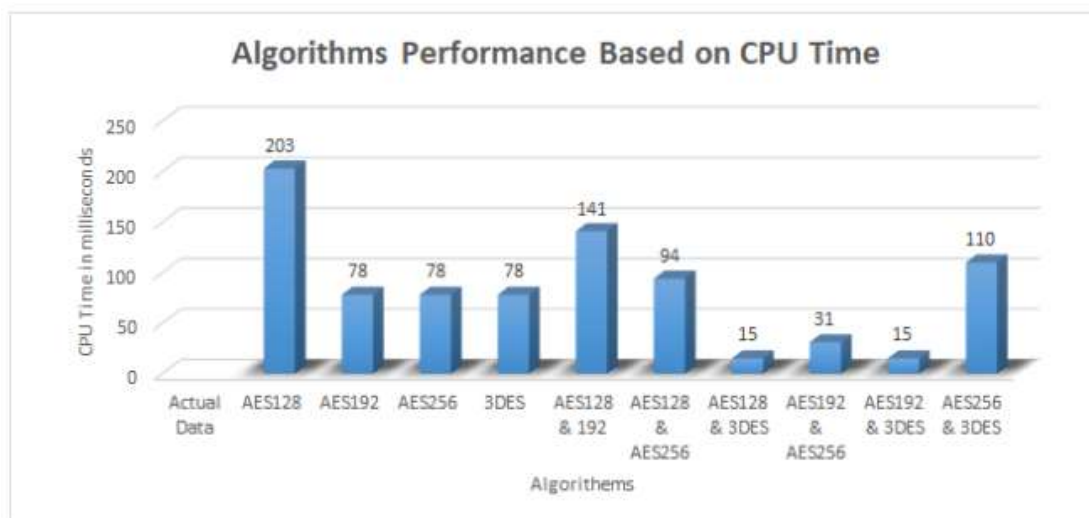
شکل ۹-۳ : جزئیات پرونده پزشکی یک بیمار (Shah, ۲۰۲۰)

۷-۳ تحلیل نتایج

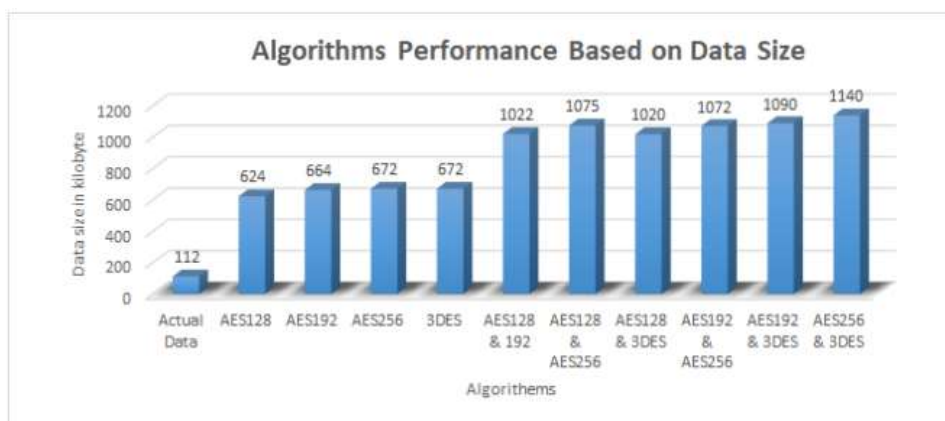
در این بخش نتایج بدست آمده با روش‌های مختلف مقایسه می‌شود. نمودارهای زیر در شکل ۳-۱۰ و شکل ۳-۱۱ و شکل ۳-۱۲؛ نتایج زمان سپری شده، زمان پردازنده و ظرفیت ذخیره‌سازی داده‌های الگوریتم‌های رمزگذاری شده مختلف را نشان می‌دهد.



شکل ۳-۱۰: نمای گرافیکی زمان سپری شده الگو (Shah, ۲۰۲۰)



شکل ۳-۱۱: نمای گرافیکی زمان CPU زمان الگوریتم رمزگذاری چندلایه و منفرد (Shah, ۲۰۲۰)



شکل ۳-۱۲: نمای گرافیکی اندازه جدول پایگاه داده بعد از ذخیره‌سازی (Shah, ۲۰۲۰)

- اگر الگوریتم رمزگذاری منفرد *AES* با اندازه کلید ۱۲۸ بیتی اعمال شود، کل زمان سپری شده ۲۵۰ میلی‌ثانیه خواهد بود.
 - اگر *AES* با اندازه کلید ۱۹۲ بیتی اعمال شود، کل زمان سپری شده ۲۱ میلی‌ثانیه خواهد بود.
 - اگر *AES* با اندازه کلید ۲۵۶ بیتی اعمال شود، کل زمان سپری شده ۳۲۱ میلی‌ثانیه خواهد بود.
 - اگر *3DES* به تنهایی اعمال شود، کل زمان سپری شده ۲۶۰ 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 *AES192* استفاده شود؛ زمان سپری شده ۵۲۱ میلی‌ثانیه خواهد بود.
 - اگر ترکیبی از *AES128* و *AES256* استفاده شود؛ زمان سپری شده ۴۷۴ میلی‌ثانیه خواهد بود.
 - اگر ترکیبی از *AES128* و *3DES* استفاده شود، زمان سپری شده ۲۹ میلی‌ثانیه خواهد بود.
 - اگر ترکیبی از *AES192* و *AES256* استفاده شود، مدت زمان سپری شده ۳۵ میلی‌ثانیه خواهد بود.
 - اگر ترکیبی از *AES192* و *3DES* استفاده شود، مدت زمان سپری شده ۸۶ میلی‌ثانیه خواهد بود.
 - اگر ترکیبی از *AES256* و *3DES* استفاده شود، مدت زمان سپری شده ۱۶۳ میلی‌ثانیه خواهد بود.
- زمان پردازنده را در میلی‌ثانیه برای ۵۰۰ رکورد با الگوریتم‌های رمزگذاری منفرد مقایسه می‌کنیم.
- *AES128* زمان پردازنده ۲۰۳ میلی‌ثانیه را می‌گیرد.
 - *AES192* زمان پردازنده ۷۸ میلی‌ثانیه است.
 - *AES256*، ۷۲ میلی‌ثانیه طول می‌کشد.
 - *3DES*، ۷۸ میلی‌ثانیه طول می‌کشد.
- نتایج زمان پردازنده برای چندین ترکیب الگوریتم با مجموعه داده‌های مشابه نیز در این شکل نشان داده شده است.
- *AES128* و ۱۹۲، ۱۴۱ میلی‌ثانیه طول می‌کشد.
 - *AES128* و *AES256*، ۹۴ میلی‌ثانیه طول می‌کشد.
 - *AES192* و *AES256* ۳۱ میلی‌ثانیه طول می‌کشد.

○ $AES192$ و $3DES$ ، ۱۵ میلی ثانیه طول می کشد.

○ $AES256$ و $3DES$ ، ۱۱۰ میلی ثانیه طول می کشد.

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 می دهد زیرا رمزگذاری فقط بارگذاری اطلاعات را انجام می دهد. برای بهترین سطح محرمانگی $AES256$ با $3DES$ مناسب است.

فصل چهارم

۴. کاربرد الگوریتم‌های چندگانه رمزگذاری روی داده‌های مراقبت

بهداشتی-مزایا و معایب

۴-۱ مقدمه

حفاظت از اطلاعات بیمار به دلیل نیاز به امنیت و نگهداری آن‌ها در فضای مناسب جهت استفاده احتمالی بیمار در آینده مسئله مهمی است که امروزه به عنوان علم روز و تکنولوژی جدید مورد نیاز بیمارستان‌ها و مراکز مربوطه است. تکنیک‌های معرفی شده در چارچوب ادبیات بررسی شد. یافتن تکنیک جدید نیاز به دقت و تست دارد. تکنیک‌های رمزگذاری چند لایه می‌توانند برای محافظت از داده‌های بیمار مفید باشند. این رویکرد مدل رمزگذاری چند لایه برای داده‌های مراقبت‌های بهداشتی در محیط ابر بر روی داده‌های بیمار اعمال شده و اثرات آن مورد تجزیه و تحلیل قرار گرفت.

۴-۲ دستورالعمل‌های موجود

قانون HIPAA و GDPR

HIPAA یک کلمه اختصاری به مفهوم "قابلیت حمل و پاسخگویی بیمه درمانی است". این مصوبه قوانین مختلفی را درباره حفاظت از داده‌های بیمار ارائه می‌دهد.

۱۸ ویژگی زیر اعمالی که باید محافظت شوند را مشخص می‌کند:

- نام و نام خانوادگی بیمار
- آدرس شامل کد پستی، شهر، کشور
- همه تاریخ‌ها
- شماره تلفن
- نمابر
- شناسه ایمیل
- SSN (شماره بیمه)
- 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 (IP)
 - بیومتریک
 - هر نوع تصویری
 - هر مشخصه دیگری که بتواند منحصرأ فرد را شناسایی کند. (Sulaiman, Sharma, Ma, Tran, 2011)
- GDPR* (مقررات عمومی حفاظت از داده ها) مقررات اتحادیه اروپا است که در سال ۲۰۱۶ پذیرفته شده است. پس از سال ۲۰۱۸ این قانون برای کلیه سازمان های کشورهای اتحادیه اروپا اجباری شده است که ذخیره اطلاعات شخصی فرد را باید مطابق با *GDPR* باشد. (Sudheep, Joseph, 2019)

۴-۳ آینده کار

- در ادامه کار و جهت پیشرفت های بیشتر می توان روی موضوعات زیر کار کرد
- انتخاب الگوریتم رمزگذاری به صورت تصادفی
 - استانداردهای الگوریتم بیشتری اضافه شود.
 - افزایش سرعت رمزگذاری
 - پیاده سازی الگوریتم های چند لایه روی داده های مبتنی بر تصویر (
 - (Shah, 2020)

۴-۴ مزایا و معایب استفاده از تکنیک های پیشنهادی

۴-۴-۱ مزایا

- امنیت داده ها با استفاده از تکنیک های چند لایه انجام می شود.
- علاوه بر این، با استفاده از روش داخلی، مسئله مدیریت کلید حل می شود.
- سطح محرمانه بودن در محاسبات ابری افزایش می یابد.
- بیماران اعتماد پیدا می کنند.
- هزینه مناسب
- سطح اطمینان در رایانش ابری افزایش می یابد.
- تکنیک چند لایه برای سایر بخش هایی که به امنیت نیاز دارند؛ نیز مناسب است.
- راه های جدیدی را برای محققان برای افزایش سطح اطمینان باز می شود. (Shah, 2020)

۴-۴-۲ معایب

معایبی که وجود دارد در برابر مزایا، ارزش هزینه و زمان را دارد. مشخص است که ترکیب چند الگوریتم با اینکه می تواند سطح محرمانگی و سرعت را بالا ببرد ولی در مواردی ممکن است سرعت و پیچیدگی کار به نسبت وجود یک الگوریتم بالا رود که به مراتب خدمات و قدرت بالاتری خواهد داشت و لذا ارزش آن را دارد. تنها می توان بهترین ترکیب چند لایه را تست کرد که تلاش این پایان نامه همین بوده است. همچنین یکی از کمبودهایی که می تواند در ادامه کار پایان نامه و در جایی دیگر رفع شود؛ به نظر من توجه بیشتر به داده های تصویری و ... است که باید امنیت بیشتری داده باشند.

۴-۵ پاسخ به سوالات تحقیق

اکنون می توان با توجه به مطالب بیان شده به سوالات که فصل اول این گزارش مطرح شده بود؛ پاسخ داد
جواب سوال ۱: انواع الگوریتم متقارن و نامتقارن و غیره رمزگذاری وجود دارد.
جواب سوال ۲: هر کدام معایب و مزایای خاص خود در زمینه های مختلف داشته که در جدول زیر این مقایسه ها ذکر می شود.

جدول ۴-۱: مقایسه الگوریتم های منفرد و ترکیبی ^۳DES و AES^{۲۵۶} (Shah, ۲۰۲۰)

AES256	^۳ DES	چند لایه AES128 & ^۳ DES	چند لایه AES192 & ^۳ DES	چند لایه AES256 & ^۳ DES	
کم	کم	متوسط	متوسط	بالا	سطح محرمانگی
سریع	سریع	سریع	متوسط	متوسط	سرعت رمزگذاری و رمزگشایی
تک کلید	تک کلید	دو کلید	دو کلید	دو کلید	تعداد کلید استفاده شده
دشوار	دشوار	سخت	سخت	خیلی سخت	امکان حمله
۱۲	۴۸	۱۲	۴۸	۶۰	تعداد دورها
۲۵۶	۱۹۲ و ۱۲۸	۲۵۶	۱۹۲ و ۱۲۸	متفاوت	طول کلید برحسب بایت

جواب سوال ۳: الگوریتم های DES و AES و ^۳DES و ترکیب این الگوریتم ها به عنوان یک الگوریتم چندلایه که امنیت بالاتر را ایجاد کند.

جواب سوال ۴: با توجه به مقایسات مطرح شده باید از چند الگوریتم رمزگذاری که ترکیب آن ها با یکدیگر بیشترین مزایا و کمترین معایب را داشته باشد؛ استفاده کرد. ورودی به سیستم الگوریتم رمزگذاری چندلایه، همان

متن ساده است که لازم است برای استفاده مجدد در آینده و ذخیره‌سازی روی فضای ابری رمزگذاری شود و در الگوریتم، رمزگذاری متناسب انجام و به عنوان ورودی الگوریتم بعدی داده می‌شود و در نهایت خروجی نهایی، تحویل داده می‌شود.

۴-۶ جمع بندی

الگوریتم‌های چند لایه بررسی شده در این پایان‌نامه دارای کارایی موثر بوده‌اند. هر چند معایبی مانند سرعت دارند که باز به توجه به مزایا و بخصوص محرمانگی بیشتر به صرفه است. می‌توان برای بالارفتن سرعت از استانداردهای دیگری در ادامه کار استفاده کرد و آن را تست نمود. مطلبی دیگر که در این پایان نامه زیاد تاکید نشده؛ کار الگوریتم‌های رمزگذاری چندگانه روی داده‌های تصویر و ... است که نیاز به کار بیشتر دارد.

فصل پنجم

۵. جمع‌بندی و پیشنهادها

۵-۱ مقدمه

در این بخش به نتایج حاصل از تحقیق با توجه به استفاده از الگوریتم‌های رمزگذاری چندگانه روی داده‌های مراقبت‌های بهداشتی، به نتیجه‌گیری و ارائه پیشنهاد در خصوص بهبود طرح پرداخته می‌شود. و نهایتاً نتیجه‌گیری بر اساس مزایا و قابلیت‌های طرح مذکور ارائه می‌گردد.

۵-۲ نتایج حاصل از تحقیق

در کل و به عنوان نتیجه تحقیق، مقایسه الگوریتم‌های مختلف را با یک لایه و چند لایه انجام داده‌ایم. سطح محرمانگی به سه حالت تقسیم می‌شود:

- کم
- متوسط
- بالا

این دقیقاً مانند شخصی است که وسیله نقلیه دارد و هنگامی که وسیله نقلیه خود را در محلی عمومی پارک می‌کند و از یک قفل واحد برای ایمنی استفاده می‌کند. سپس، ذهن او همچنان فکر می‌کند که ممکن است وسیله نقلیه او به سرقت رفته باشد. که نشان دهنده سطح محرمانگی است. حال در صحنه دوم، فرض کنید که قفل دیگری به آن متصل شده باشد اما از امنیت کمتری برخوردار باشد، او از یک سطح رضایت بیشتری دارد اما ترس از سرقت خودرو ممکن است همیشه در ذهن او باقی بماند. در سناریوی سوم، او دو قفل را روی وسیله نقلیه خود اعمال کرده و هر دو بسیار محکم هستند. سپس سطح محرمانگی، به دلیل روش‌هایی که روی آن اعمال کرده است؛ بسیار بالا می‌رود. این مورد در مورد بیماران و سازمان‌های بهداشتی نیز وجود دارد. اگر الگوریتم ضعیفی را نسبت به بیماران اعمال کرده باشند و اطلاعات در معرض خطر است. اما اگر داده‌هایی که در فضای ابری ذخیره می‌شوند با الگوریتم‌های متعددی رمزگذاری شوند، سطح محرمانگی بسیار بالا خواهد بود. سرعت الگوریتم متفاوت است. سرعت AES256 و ۳DES متوسط است، سرعت AES192 و ۳DES نیز متوسط است اما سرعت AES256 و ۳DES به تنهایی بهتر از الگوریتم‌های چند لایه است. تنها نقطه ضعف الگوریتم ۳DES سرعت است. به همین دلیل است که وقتی با الگوریتم دیگری استفاده می‌شود روند ترکیبی را نیز کند می‌کند. دلیل این امر ۴۸ دور آن است. به دلیل ترکیب کلید، سطح اطمینان نیز افزایش می‌یابد زیرا داده‌ها با چندین کلید رمزگذاری

می‌شوند. در نتیجه، روش چند لایه به دلیل رمزگذاری لایه ای از سرعت کمی برخوردار است اما از نظر محرمانه بودن از سطح بالایی برخوردار است. (Shah, 2020)

۳-۵ پیشنهادها

زمانی که به عنوان سمینار دانشجویی، کار بر روی این پایان‌نامه را شروع کردم؛ جذب موضوع آن شدم. امنیت داده‌های مربوط به بیمار و حفظ و نگهداری اطلاعات برای استفاده مجدد بیمار و پزشک. دانشجویان ارشد الگوریتم‌های رمزگذاری را به خوبی می‌دانند اما ترکیب آن‌ها و رسیدن به حالت ایده‌آل کاری است که راستای فکری این پایان‌نامه بوده است. طراحی نرم‌افزار به کاررفته در این سیستم، تقریباً راحت بوده و نوشتن برنامه رمزنگاری به توجه به ترکیب الگوریتم‌های راحت است. موردی که نیاز به دقت دارد و در واقع نیرو محرکه کار و عامل برتری طرح می‌باشد؛ ژیدا کردن بهترین ترکیب‌های الگوریتم‌های رمزگذاری است که بتوان به صورت چند لایه استفاده کرد.

در مورد مشخصات سخت‌افزاری مورد نیاز طرح، اکثر سیستم‌های 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 ۱۰ ممکن است روی بعضی سیستم‌ها قابل نصب نباشد. لذا یکی از پیشنهادها 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 احیاناً 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 راهنمای نگارش پایان‌نامه معاونت آموزشی و تحصیلات تکمیلی دانشگاه پیام‌نور باشد. شیوه ارجاع در این پایان‌نامه به صورت لینک به منابع بود و شخصاً کار مشکلی در درک مفاهیم آن داشتم.

۴-۵ 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 سیستم‌ها

۵-۵ جمع‌بندی و نتیجه‌گیری

در این گزارش سعی شده پایان‌نامه با موضوع "مدل رمزگذاری چند لایه برای محافظت از داده‌های مراقبت‌های بهداشتی در محیط ابری" مورد تجزیه و تحلیل قرار بگیرد. مطالب درک شده و در جاهایی نیاز بود با توجه به منابع موجود گسترش داده شد

این گزارش شامل ۵ فصل است. فصل اول به تعریف و مقدمه، فصل دوم مفاهیم عمومی رمزگذاری، فصل سوم مروری است بر کارهای انجام شده طرح پیشنهادی پایان‌نامه، فصل چهارم کاربردها و مزایا و معایب الگوریتم‌های رمزگذاری و فصل پنجم نیز جمع‌بندی و نتیجه‌گیری نهایی است

پس از درک موضوع و تجزیه و تحلیل آن‌ها در راستای ادامه کار موضوعات پیشنهادی بیان شد و به خصوص جهت بومی‌سازی این طرح در ایران پیشنهادهایی مطرح شد.

مراجع

- فراهی، احمد. (۱۳۹۸). «پایگاه داده پیشرفته»، تهران: دانشگاه پیام نور ۴۰۰ ص
- Babatunde, A. O., A. J. Taiwo, and E. G. Dada., “Information Security in Health Care Centre Using Cryptography and Steganography.” arXiv preprint arXiv:۱۸۰۳.۰۵۵۹۳, ۲۰۱۸.
- T. M. Damico, “A brief history of cryptography,” *Inquiries Journal*, vol. ۱, no. ۱۱, ۲۰۰۹.
- F. Gao, S. Thiebes, and A. Sunyaev, “Rethinking the meaning of cloud computing for health care: A taxonomic perspective and future research directions,” *Journal of medical Internet research*, vol. ۲۰, no. ۷, p. e۱۰۰۴۱, ۲۰۱۸.
- V. S. V. Hema and R. Kesavan, “Ecc based secure sharing of healthcare data in the health cloud environment,” *Wireless Personal Communications*, vol. ۱۰۸, no. ۲, pp. ۱۰۲۱–۱۰۳۵, ۲۰۱۹.
- 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-۱,” *Journal of medical systems*, vol. ۳۷, no. ۵, p. ۹۹۷۱, ۲۰۱۳.
- Outright Systems.(۲۰۱۹). Cloud Computing in Business Retrieved from <https://medium.com/@outrightsystems/cloud-computing-in-business-ab۱۹f۳۰۸۲۲۱d>
- 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, ۲۰۱۹, pp. ۲۶۷–۳۰۹
- H.A.Shah. (۲۰۲۰). “A Multilayer Encryption Model To Protect Healthcare Data in Cloud Environment”. (Unpublished master’s thesis). University of Islamabad
- 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, ۲۰۱۹, pp. ۲۱۲–۲۱۵
- 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. ۷, no. ۱۱, pp. ۱۶۹۱–۱۷۰۳, ۲۰۱۱.
- Vrema.sushil.(۲۰۱۹). characteristics-of-cloud-computing-as-per-nist Retrieved <https://timesofcloud.com/cloud-tutorial/characteristics-of-cloud-computing-as-per-nist>
- 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. ۹۷, pp. ۱۸۵–۱۹۶, ۲۰۱۹.
- Z. Yan, R. H. Deng, and V. Varadharajan, “Cryptography and data security in cloud computing,” ۲۰۱۷
- L. Zhou, V. Varadharajan, and K. Gopinath, “A secure role-based cloud storage system for encrypted patient-centric health records,” *The Computer Journal*, vol. ۵۹, no. ۱۱, pp. ۱۵۹۳–۱۶۱۱, ۲۰۱۶.

واژه‌نامه

واژه‌نامه فارسی به انگلیسی

Communication	ارتباط
History	تاریخچه
Combination	ترکیب
Multilayer	چندلایه
Cloud computing	رایانش ابری
Cryptography	رمزگذاری
Symmetric	متقارن
Healthcare	مراقبت‌های بهداشتی
Architecture	معماری
Cost	هزینه

واژه‌نامه انگلیسی به فارسی

Architecture	معماری
Cloud computing	رایانش ابری
Combination	ترکیب
Communication	ارتباط
Cost	هزینه
Cryptography	رمزگذاری
Healthcare	مراقبت‌های بهداشتی
History	تاریخچه
Multilayer	چندلایه
Symmetric	متقارن

Abstract

This is the era of cloud computing and it has become an integral part for any organization. It is equally suitable for all the organizations e.g. education, government, public sector, health care department. Main features of cloud computing are broad network, shared resources, rapid elasticity and pay per use. Cloud computing is also providing highly potential services to IT based healthcare sector. In cloud computing model a patient can get consultancy from any doctor available in the world. There are two types of patient information i.e. protected/sensitive health information and general information. Protected information (Phone no, ATM, Security no, MR no etc.) requires more confidentiality as compared to general information. Therefore, for some protected health information without patient association (general disease name, symptoms) will be very helpful for research experiments. Health information is protected by achieving confidentiality, integrity and availability, when data is stored in cloud environment.

There can be many types of attacks possible on protected health information stored on cloud e.g. if patient credit card information is hacked by a hacker than he may lose his all money. Similarly, if the disease information of a celebrity is leaked out than he/she may lose the career. That's why protected/sensitive information requires protection in cloud environment. Cryptography methods provide different techniques to protect the data stored in cloud environment. In this thesis, we have suggested a multilayer encryption technique to ensure the confidentiality of data stored in cloud environment. This suggested technique will improve the security of cryptographic techniques when used in multilayered format. We have set up a local system for the experiment. We have used the RDBMS (Microsoft SQL Server) and Framework ξ, ρ . A set of $\rho \cdot \cdot \cdot$ dummy patient records is used to test the proposed techniques. The experiment was performed to check the confidentiality of the suggested techniques. This experiment shows us that multilayer encryption techniques is more suitable for public health sectors when data is in cloud environment.

Keywords

Cloud computing , healthcare , Encryption , key



Payam Noor University

Department of Computer Engineering and Information Technology

Seminar Report (M.Sc)

Title:

**A Multilayer Encryption Model to Protect
Healthcare Data in Cloud Environment(Review)**

Supervisor:

Dr. Ali Razavi

By:

Somayeh Karbasy

August ۲۰۲۱