دانشگاه علوم و فناوری اسلام آباد

یک مدل رمزگذاری چند لایه برای محافظت از داده های مراقبت های بهداشتی در محیط ابری

توسط

حسن عباس شاه

پایان نامه ارائه شده درجه کارشناسی ارشد

در

دانشکده محاسبات

گروه علوم کامپیوتر

سال ۲۰۲۰

حق کپی رایت ©۲۰۲۰ برای حسن عباس شاه:
کلیه حقوق محفوظ است؛ هیچ بخشی از این پایان‌نامه به هیچ وجه از طریق فتوکپی، ضبط، یا سایر روش‌های الکترونیکی یا مکانیکی، توسط هر سیستم ذخیره‌سازی و بازیابی اطلاعات بدون اجازه قبلی کتبی حسن عباس شاه، قابل تولید، توزیع یا انتقال نیست.***(MCS173006)***

این پایان‌نامه به معلمان، خانواده و دوستان عزیزم تقدیم می‌شود. من از پدر و مادر عزیزم، برادران، خواهران و همسرم تشکر ویژه ای دارم. من می‌خواهم از استاد راهنمای خود برای اعتقاد راسخ و اطمینان‌شان برای رسیدن به این نقطه عطف موفقیت شده تشکر کنم.

گواهی تصویب

یک مدل رمزگذاری چند لایه برای محافظت از داده‌های مراقبت های بهداشتی در محیط ابری

توسط

حسن عباس شاه

(MCS173006)

کمیته بررسی پایان نامه

شماره	آزمون‌گر	نام	سازمان
A	آزمون‌گر خارجی	دکتر منیر احمد	***BIIT***راولپندی
B	آزمون‌گر داخلی	دکتر امیر قیوم	***CUST***اسلام آباد
C	استاد راهنما	دکتر قمر محمود	***CUST***اسلام آباد

دکتر قمر محمود

استاد راهنمای پایان‌نامه

مه ۲۰۲۰

دکتر نایر مسعود سرگروه دپارتمان علوم کامپیوتر مه ۲۰۲۰	دکتر محمود عبدالقادر رئیس دانشکده محاسبات مه ۲۰۲۰

اعلامیه نویسنده

من، **حسن عباس شاه** بدین‌وسیله اظهار می‌کنم که پایان‌نامه کارشناسی ارشد خود با عنوان " **یک مدل رمزگذاری چند لایه برای محافظت از داده های مراقبت‌های بهداشتی در محیط ابری"** کار خود من است و قبلا برای دریافت مدرک دانشگاه علم و صنعت پایتخت توسط من در اسلام آباد یا هر جای دیگر(در داخل کشور/ خارج از کشور) ارسال نشده است.

اگر در هر زمان اظهارات من حتی بعد از فارغ التحصیلی من نادرست باشد؛ دانشگاه حق پس گرفتن مدرک کارشناسی ارشد من را دارد.

(حسن عباس شاه)

شماره ثبت : ***MCS173006***

تعهد سرقت ادبی

من رسما اعلام میکنم که کارهای تحقیقاتی ارائه شده در این پایان‌نامه با عنوان **" یک مدل رمزگذاری چند لایه برای محافظت از داده های مراقبت‌های بهداشتی در محیط ابری"** فقط کار تحقیقاتی من است و هیچ مشارکت قابل توجهی از شخص دیگری ندارد. مشارکت/ کمک هر کجا که گرفته شود؛ تأیید شده و پایان نامه کامل توسط من نوشته شده است.

من سیاست ***HEC*** و دانشگاه علم و صنعت پایتخت را در مورد دزدی ادبی درک می‌کنم. بنابراین، به عنوان نویسنده پایان‌نامه عنوان شده فوق اظهار می‌دارم که هیچ بخشی از پایان‌نامه من دزدی ادبی نشده است و هر ماده‌ای که به عنوان مرجع استفاده می‌شود به درستی ارجاع شده و استناد می شود.

من متعهد می‌شوم اگر در پایان‌نامه تحت عنوان فوق حتی پس از دریافت مدرک دانشگاهی مقصر شناخته شوم، این دانشگاه برای خود حق برکناری/ لغو مدرک کارشناسی ارشد را دارد و ***HEC***و دانشگاه حق دارند نام من را در وب سایت ***HEC / University*** که اسامی دانشجویانی که کارهای دزدی ادبی را ارسال کرده اند در آن قرار می گیرد؛ قرار دهد.

(حسن عباس شاه)

شماره ثبت : ***MCS173006***

سپاسگزای‌ها

به نام خداوند بخشنده، صاحب جهان را به خاطر برکاتی که به من عطا کرده است برای کمک به من در تکمیل این پایان‌نامه ستایش می‌کنم. این مطالعه؛ تلاشی است برای فهم و بیان اصول اصلی یکی از چند صد هزار پدیده، با ابزاری به نام مغز، گرانبهاترین هدیه خداوند متعال.

من می‌خواهم صمیمانه از استاد راهنمای مشتاق خود، **دکتر قمر محمود**، به خاطر نظارت، کمک و دانش بی نظیرش قدردانی کنم. من صمیمانه از او به خاطر حمایت مداوم، انگیزه و صبرش سپاسگزارم. کمک بی‌نظیر وی و نظرات و پیشنهادات سازنده در طول کار پایان‌نامه به موفقیت این تحقیق کمک کرده است. این یک تجربه شگفت‌انگیز بوده است و من از او به خاطر حمایت فوق العاده‌اش از صمیم قلب تشکر می کنم.

من از پدر و مادر عزیزم، همسر و فرزندانم بخاطر تحمل تغییرات روحی و تحمل روحیه من، عمیقا سپاسگزارم. من همچنین می‌خواهم از دوستانم تشکر کنم که مرا تشویق کردند و برای پایان کار تحقیقاتی به من انگیزه دادند.

(حسن عباس شاه)

شماره ثبت: ***MCS173006***

چکیده

الان عصر محاسبات ابری است و این موضوع برای هر سازمانی به بخشی جدایی‌ناپذیر 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 بالقوه ای را به بخش مراقبت های بهداشتی مبتنی بر فناوری اطلاعات ارائه می‌دهد. در مدل رایانش ابری بیمار می‌تواند از هر پزشکی در هرجای 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 آزمایش های تجربی بسیار مفید خواهد بود. وقتی داده‌ها در فضای ابری ذخیره می‌شوند، به‌وسیله 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 تکنیک های رمزنگاری را بهبود می‌بخشد. یک سیستم محلی برای آزمایش تنظیم کرده‌ایم. از ***RDBMS (Microsoft SQL Server)*** و ***Framework 4.5*** استفاده کرده‌ایم. 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.

فهرست

اعلامیه نویسنده iv
تعهد سرقت ادبی v
سپاسگزای‌ها vi
چکیده vii
لیست اشکال xi
لیست جداول xii
مخفف ها xiii
۱. مقدمه ۱
۱,۱ رایانش ابری ۲
۲,۱ تاریخچه مختصری از رایانش ابری ۳
۳,۱ ویژگی‌های رایانش ابری برای بخش مراقبت‌های بهداشتی ۳
۴,۱ مدل سرویس ابری برای خدمات بهداشتی الکترونیکی ۳
۱,۴,۱ نرم افزار به عنوان سرویس ***(SaaS)*** ۴
۲,۴,۱ پلت فرم به عنوان یک سرویس ***(PaaS)*** ۴
۳,۴,۱ زیرساخت به عنوان سرویس ***(IaaS)*** ۴
۵,۱ مروری بر رمزنگاری ۴
۱,۵,۱ چند کلمه درباره تاریخ رمزنگاری ۵
۲,۵,۱ انقلاب در زمینه رمزنگاری ۵
۳,۵,۱ انواع طرح‌های رمزنگاری ۶
۴,۵,۱ سرویس امنیتی برای رمزنگاری برای مراقبت های بهداشتی ۷
۶,۱ کار الگوریتم‌های مورد استفاده در طرح پیشنهادی ۸
۷,۱ قانون ***HIPAA*** و ***GDPR*** چیست؟ ۱۳
۸,۱ عامل انگیزه ۱۵
۹,۱ بیان مسئله ۱۵
۱۰,۱ سوالات تحقیق ۱۵
۱۱,۱ روش تحقیق ۱۵

۱۲,۱ هدف مطالعه ۱۶
۱۳,۱ اهمیت پایان‌نامه ۱۶
۱۴,۱ نتیجه‌گیری ۱۷
۱۵,۱ سازمان پایان‌نامه ۱۷
۲. بررسی ادبیات ۱۸
۲,۱ کار مرتبط ۱۸
۲,۲تجزیه و تحلیل بررسی ادبیات ۲۲
۳,۲ دست‌آوردهای تجزیه و تحلیل ۲۵
۴,۲ خلاصه ۲۵
۳. راه‌اندازی آزمایشی طرح پیشنهادی ۲۶
۱,۳ انتخاب مجموعه داده‌ها ۲۶
۲,۳ لایه رمزگذاری ***PHI Attribut ES*** ۲۶
۳,۳ معماری روش ۲۶
۴,۳ فرآیند رمزگذاری و رمزگشایی در ***RDBMS*** (***(Microsoft SQL Server)*** ۲۸
۱,۴,۳ چگونه رمزگذاری در ***SQL Server*** انجام می‌شود؟ ۲۸
۵,۳ نتیجه گیری ۲۹
۴. تجزیه و تحلیل آزمایشی طرح پیشنهادی ۳۱
۱,۴ انتخاب مجموعه داده ۳۱
۲,۴ نصب پیکربندی سخت‌افزار و نرم‌افزار ۳۱
۱,۲,۴ سخت‌افزار مورد نیاز ۳۱
۲,۲,۴ سیستم عامل و نرم‌افزار توسعه ۳۱
۳,۴ مرحله رمزگذاری داده‌ها ۳۲
۴,۴ مرحله رمزگشایی داده‌ها ۳۴
۵,۴ تحلیل نتایج ۳۴
۶,۴ نتیجه‌گیری ۳۸
۵. نتیجه‌گیری و آینده کار ۳۹

۱,۵ نتیجه‌گیری ۳۹
۲,۵ آینده کار ۳۹
فهرست منابع ۴۰

لیست اشکال

شکل ۱-۱: رایانش ابری ۲
شکل ۱-۲: رمزنگاری استگانوگرافی ۴
شکل ۱-۳: رمزگذاری کلید متقارن ۶
شکل ۱-۴: رمزگذاری نامتقارن کلید ۷
شکل ۱-۵: روش رمزگذاری چند لایه ۸
شکل ۱-۶: جایگزینی اولیه ۹
شکل ۱-۷: تابع **Round** ۱۰
شکل ۱-۸: گسترش جعبه جایگزینی ۱۰
شکل ۱-۹: تولید کلید ۱۱
شکل ۱-۱۰: نمودار معماری ۳□□□ ۱۲
شکل ۱-۱۱: معماری الگوریتم **AES** ۱۴
شکل ۱-۱۲: نمودار روش تحقیق ۱۶
شکل ۳-۱: تکنیک محافظت از چند لایه ۲۶
شکل ۳-۲: نمودار معماری روش‌شناسی ۲۷
شکل ۳-۳: فیش ورود به سیستم برای بیمار ۲۷
شکل ۳-۴: فرآیند رمزگذاری کلی ۲۹
شکل ۴-۱: نمونه مجموعه داده‌های ساختگی ۳۱
شکل ۴-۲: ایجاد کلیدها و گواهینامه ها ۳۲
شکل ۴-۳: فرم رمزگذاری شده داده‌ها ۳۳
شکل ۴-۴: : صفحه ورود به سیستم برای ورود بیمار ۳۴
شکل ۴-۵: جزئیات پرونده پزشکی یک بیمار ۳۵
شکل ۴-۶ : نمای گرافیکی زمان سپری شده الگو ۳۵
شکل ۴-۷ : نمای گرافیکی زمان **CPU** زمان الگوریتم رمزگذاری چندلایه و منفرد ۳۶
شکل ۴-۸: نمای گرافیکی اندازه جدول پایگاه داده بعد از ذخیره‌سازی ۳۶

لیست جداول

جدول ۱-۱: مقایسه بین رمزنگاری کلاسیک و مدرن ۵
جدول ۱-۲: اهمیت پایان نامه ۱۷
جدول ۲-۱: مرور آنالیز ادبیات ۲۴
جدول ۴-۱: مفایسه الگوریتم‌های منفرد و ترکیبی **۳DES** و **AES۲۵۶** ۳۸

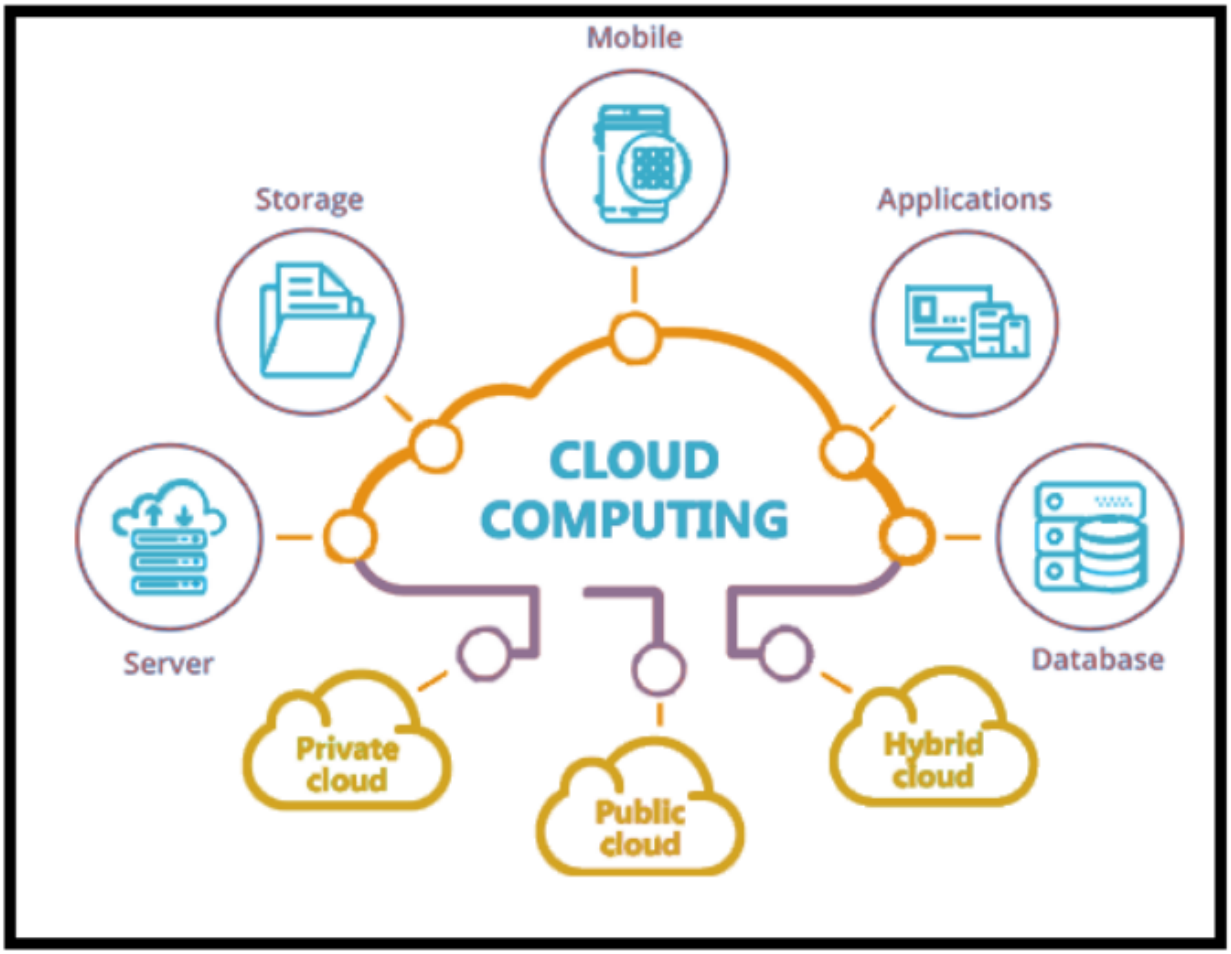
مخفف ها

ABE	***Attribute Based Encryption***
AES	***Advance Encryption Standard***
DES	***Data Encryption Standard***
EGC	***Elliptic Galois Cryptography***
GDPR	***General Data Protection Regulation***
HIPAA	***Health Insurance Portability and Accountability Act***
IFHDS	***Intelligent Framework for Healthcare Data Security***
LSB	***Least Significant Bit***
MSD	***Mass storage Device***
MR No	***Medical Record No***
PCEHR	***Personal Control Electronic Health Record***
PHI	***Protected Health Information***
RDBMS	***Relational Database Management System***
RSA	***Rivest, Shamir, and Adelman***
SHA	***Secure Hash Algorithm***
SNAP	***Subnetwork Access Protocol***
Three DES	***Triple Data Encryption Standard***

فصل ۱

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***[۱]***. 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 , D DoS*** 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 ***[۲]*** و به همین دلیل ***HIPAA*** و ***GDPR*** برای محافظت از صفات ***PHI*** نقش دارند. در مورد برخی از مزایای محیط ابر بحث خواهیم کرد و سپس نگاهی خواهیم انداخت به نقش رمزنگاری در داده‌های مراقبت‌های بهداشتی.



شکل ۱-۱: رایانش ابری[۱]

۱,۱ رایانش ابری

رایانش ابری *[۳]* سرویس محاسباتی مورد تقاضا است. به شکل ۱,۱ نگاه کنید. این بدان معناست که منابع محاسباتی در صورت تقاضا و در حد نیاز در دسترس هستند. اکنون رایانش ابری بزرگترین منبع خدمات رایانه‌ای به ویژه در بخش مراقبت‌های بهداشتی است. به بخش بهداشت الکترونیکی اجازه می‌دهد تا با حداقل تلاش مدیریتی، داده‌ها را در مکان‌هایی از راه دور ذخیره و دسترسی یابد. اصطلاح عمومی رایانش ابری مراکز داده‌ای هستند که در اینترنت در دسترس هستند که خدمات مختلفی را در اینترنت ارائه می‌دهند. بیمارستان‌ها نیازی به نگهداری مراکز داده خود ندارند. آن‌ها فقط باید سرور یا دستگاه را با توجه به تقاضای خود بخرند و با توجه به میزان استفاده به مراکز داده/ ارائه دهندگان پرداخت کنند. هدف اصلی رایانش ابری، به اشتراک گذاری منابع با سهولت و استفاده مناسب از آن است.

---

۱ **https://medium.com/@outrightsystems/cloud-computing-in-business-ab۱۹f۳۰۸۲۲۱d**

۲,۱ تاریخچه مختصری از رایانش ابری

در اوایل دهه ۱۹۶۰ 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 می‌شد. برای دسترسی به داده‌ها و پردازش، از ترمینال‌های تخلیه استفاده می‌شد.

- در سال ۲۰۰۶ آمازون شروع به فعالیت خود در زیر شاخه‌ای 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.

۳,۱ ویژگی‌های رایانش ابری برای بخش مراقبت‌های بهداشتی

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.

NIST [۴] پنج مزیت رایانش ابری را تعریف 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.

۴,۱ مدل سرویس ابری برای خدمات بهداشتی الکترونیکی

رایانش ابری به دلیل زیرساخت‌هایش، سرعت و بودجه انعطاف‌پذی، 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.***[۵]***

- نرم افزار به عنوان سرویس ***(SaaS)***
- بسترهای نرم افزاری به عنوان سرویس ***(PaaS)***
- زیرساخت به عنوان سرویس ***(IaaS)***

اکنون فقط برای داشتن دانش اولیه کمی در مورد این سرویس ها که در فضای ابری مجاز هستند بحث می‌کنیم.

۱,۴,۱ نرم افزار به عنوان سرویس *(SaaS)*

هر ارائه دهنده خدمات بهداشتی درمانی می‌تواند با استفاده از این منبع از ارائه‌دهنده خدمات ابری با تلاش مدیریتی بسیار کمتر، از برنامه داخلی سیستم مدیریت بیمارستان استفاده کند.

۲,۴,۱ پلت فرم به عنوان یک سرویس *(PaaS)*

PaaS برای بخش‌های بهداشتی است که می‌خواهند نرم‌افزار کاربردی سفارشی خود را بسازند.

۳,۴,۱ زیرساخت به عنوان سرویس *(IaaS)*

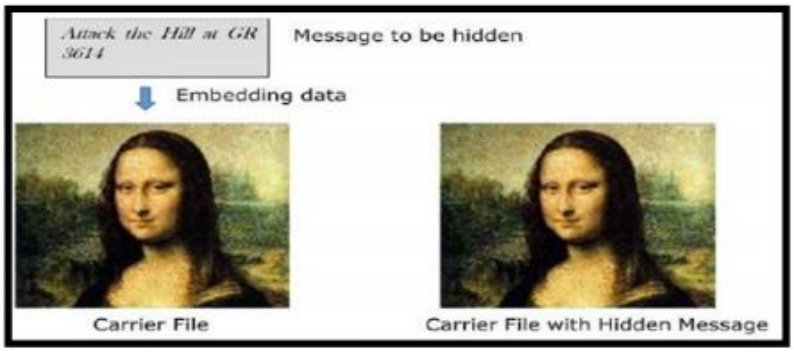
همان‌طور که از نام آن پیداست، هر سازمان بهداشتی می‌تواند سخت‌افزار کامل را خریداری کرده و نرم‌افزار و داده‌های خود را در فضای ابری نگه دارد.

چالش‌های داده‌های مراقبت‌های بهداشتی در فضای ابری:

- داده‌های بیمار در قالب دیجیتال در ***RDBMS*** ذخیره می‌شود. اگر نقش مناسبی برای دسترسی به داده‌های بیمار به نهادهای مختلف اختصاص داده نشود، ممکن است تغییر کند. نتیجه این است که محرمانگی و یکپارچگی داده ها از بین می‌رود.
- داده‌ها در خارج از قرارداد قرار دارند.
- سخت‌افزار بین بیماران مختلف به اشتراک گذاشته می‌شود و حمله‌کننده‌ای ممکن است داده‌ها را به خطر بیندازد.

۵,۱ مروری بر رمزنگاری

به طور کلی اصطلاح رمزنگاری ***[۶]*** به مطالعه اسرار اشاره دارد و در دنیای امروز با رمزگذاری زیاد ارتباط داریم. رمزگذاری فرایندی است که متن ساده را به متن مخفی/ متن رمزگذاری شده تبدیل می‌کند که باعث می‌شود متن ساده از امنیت بیشتری برخوردار باشد. بنابراین وقتی داده‌های مربوط به بیمار در ابر ذخیره می‌شوند؛ به حفاظت نیاز دارند. نکنیک‌های رمزنگاری، سطح محرمانگی و یکپارچگی مربوط به بیمار را بهبود می‌بخشد. به طور کلی رمزنگاری از تکنیک‌های مدل سازی ریاضی ***[۷]*** استفاده می‌کند. این تکنیک‌ها براساس رمزگذاری و رمزگشایی داده‌ها با استفاده از کلیدها است.



شکل ۱-۲: رمزنگاری استگانوگرافی [۲]

[۲] **https://www.tutorialspoint.com/cryptography/cryptosystems.htm**

۱,۵,۱ چند کلمه درباره تاریخ رمزنگاری

رمزنگاری رابطه نزدیک با تاریخچه نوشتن متن دارد. حدود ۴۰۰۰ سال پیش مصریان ارتباطات را با کلمات پنهانی آغاز کردند که هیروگلیف نامیده می‌شود. این زبان فقط برای نویسندگانی که از طرف پادشاهان پیام را منتقل می‌کردند؛ شناخته شده بود. در سالهای ۵۰۰ تا ۶۰۰ قبل از میلاد محققان روش‌های ساده رمزگذاری جایگزینی را شروع کردند. رومی‌ها تکنیک‌های جدیدی را معرفی کردند که به رمز سزار معروف است. در این روش کاراکترهای کلمات با برخی کاراکترهای دیگر جایگزین می‌شوند و در جایی دیگر این کاراکترها ذخیره می‌شوند که به پیام اصلی تبدیل شوند.

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 نهان‌نگاری 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.

۲,۵,۱ انقلاب در زمینه رمزنگاری

در قرن پانزدهم قبل از میلاد، در اروپا درکشور ایتالیا، ایالت پاپال پیشرفت بیشتری در رمزنگاری داشتند. تکنیک‌های مختلف تجزیه و تحلیل رمزنگاری و حملات در این دوره مورد توجه قرار گرفته است.

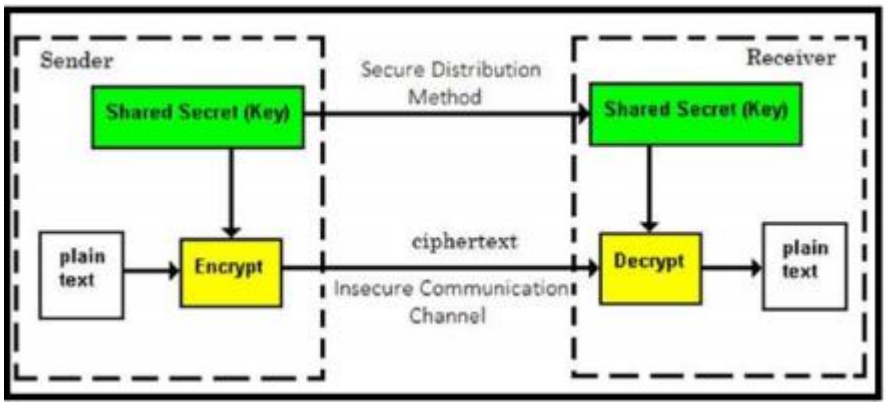
- تکنیک‌های کدگذاری ***vigenere*** در این عصر معرفی شده است.
- اما در قرن نوزدهم رمزنگاری از رویکردهای موقت به تکنیک های هنری مدرن‌تر تغییر یافته است.
- در قرن ۲۰ ماشین روتر انیگما معرفی شد.
- اما پس از جنگ جهانی دوم، روش‌های مدرن رمزنگاری معرفی شده است که برای رشته‌های علوم رایانه، مانند اکسیژن است.

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

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

جدول ۱-۱: مقایسه بین رمزنگاری کلاسیک و مدرن

در جدول فوق برخی از ویژگی‌های اساسی تکنیک‌های رمزنگاری کلاسیک و مدرن را با هم مقایسه کردیم که نشان می‌دهد که همیشه جای بحث در تکنیک‌های موجود به خوبی تحقیق در مورد تکنیک‌های جدید وجود دارد.



شکل ۱-۳: رمزگذاری کلید متقارن [۳]

۳,۵,۱ انواع طرح‌های رمزنگاری

دو نوع رمزگذاری عمومی در سیستم‌های رمزگذاری استفاده می‌شود:***[۶]***

- رمزگذاری متقارن
- رمزگذاری نامتقارن

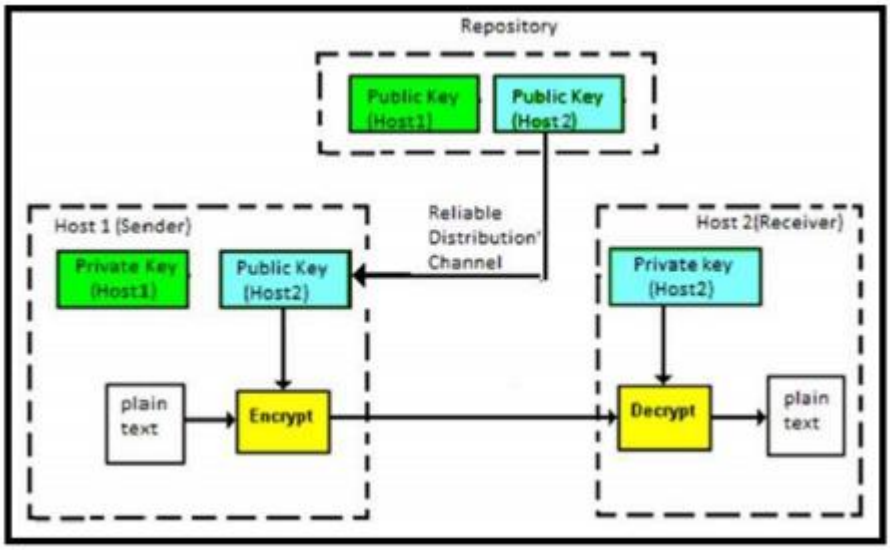
۱,۳,۵,۱ رمزگذاری کلید متقارن

در این نوع رمزگذاری فقط یک کلید برای رمزگذاری و رمزگشایی استفاده می‌شود. شکل ۱و۳ را مشاهده کنید. الگوریتم‌های معروف رمزگذاری متقارن عبارتند از: استاندارد رمزگذاری دیجیتال***(DES)*** ، ***Triple-DES (3DES)***، ***IDEA*** و***BLOWFISH.***

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 می توانند بصورت دوره ای یا بر اساس نیاز تغییر کنند .
- قبل از شروع ارتباط بین طرفین ، می توان کلید را به اشتراک گذاشت.

[۳] **https://www.tutorialspoint.com/cryptography/cryptosystems.htm**



شکل ۱-۴: رمزگذاری نامتقارن کلید[۴]

۲,۳,۵,۱ رمزگذاری نامتقارن

این مورد هم به عنوان رمزنگاری کلید عمومی شناخته می‌شود. که شامل دو کلید برای رمزگذاری و رمزگشایی است به شکل ۴,۱ مراجعه کنید. هر پیام یا داده‌ای را می‌توان با استفاده از کلید عمومی که برای همه به صورت عمومی شناخته شده است؛ رمزگذاری کرد. اما فرآیند رمزگشایی به کلید خصوصی نیاز دارد. این کلید گیرنده‌ای دارد که می‌خواهد آن را رمزگشایی کند.

رمزگذاری نامتقارن 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.

۴,۵,۱ سرویس امنیتی برای رمزنگاری برای مراقبت های بهداشتی

ویژگی‌های زیر را می‌توان از رمزنگاری مربوط به داده‌های بیمار بدست آورد.***[۹]***

۱,۴,۵,۱ محرمانه بودن

محرمانگی اساسی‌ترین سرویس امنیتی رمزنگاری است که اطلاعات پزشکی بیمار را از دسترسی غیرمجاز پنهان می‌کند.

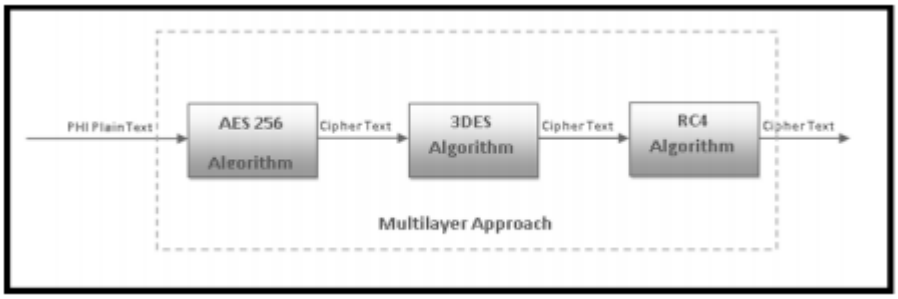
---

[۴] **https://www.tutorialspoint.com/cryptography/cryptosystems.htm**

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 می توان به سطحی از محرمانگی دست یافت.

۲,۴,۵,۱ 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.



شکل ۱-۵: روش رمزگذاری چند لایه

۳,۴,۵,۱ 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:

احراز هویت موجودیت: این اطمینان را به شما می‌دهد که پیام یا اطلاعات از یک نهاد خاص دریافت شده است.

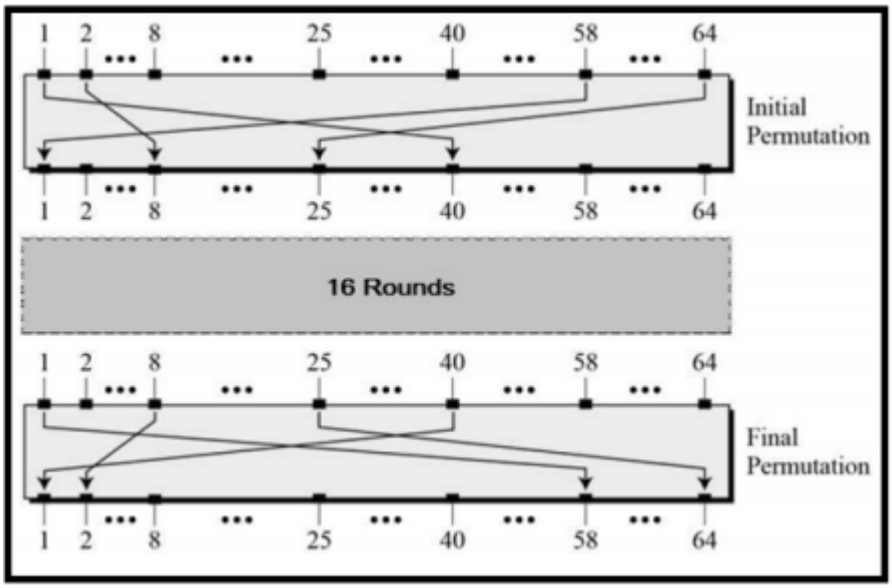
احراز هویت پیام: این اطلاعات بدون توصیف مسیر یا سیستمی که این اطلاعات را ارسال کرده است، اطلاعات مربوط به مبدع **پیام** را ارائه می‌دهد.

۴,۴,۵,۱ رمزگذاری چند لایه

به شکل ۵,۱ نگاه کنید؛ متن ساده را به یک الگوریتم با کلید منتقل خواهیم کرد و خروجی آن الگوریتم با کلید متفاوت به الگوریتم دوم منتقل می شود. چنین لایه‌هایی می‌توانند شامل دو یا چند الگوریتم باشند. بنابراین، می‌توان به یک سطح محرمانگی دست یافت.

۶,۱ کار الگوریتم‌های مورد استفاده در طرح پیشنهادی

استاندارد رمزگذاری داده‌ها(*DES*) یک الگوریتم متقارن است که توسط ***NIST*** بیان شد. این پیاده‌سازی براساس رمزگذاری فایستل است که در ۱۶ دور انجام می‌شود.



شکل ۱-۶: جایگزینی اولیه

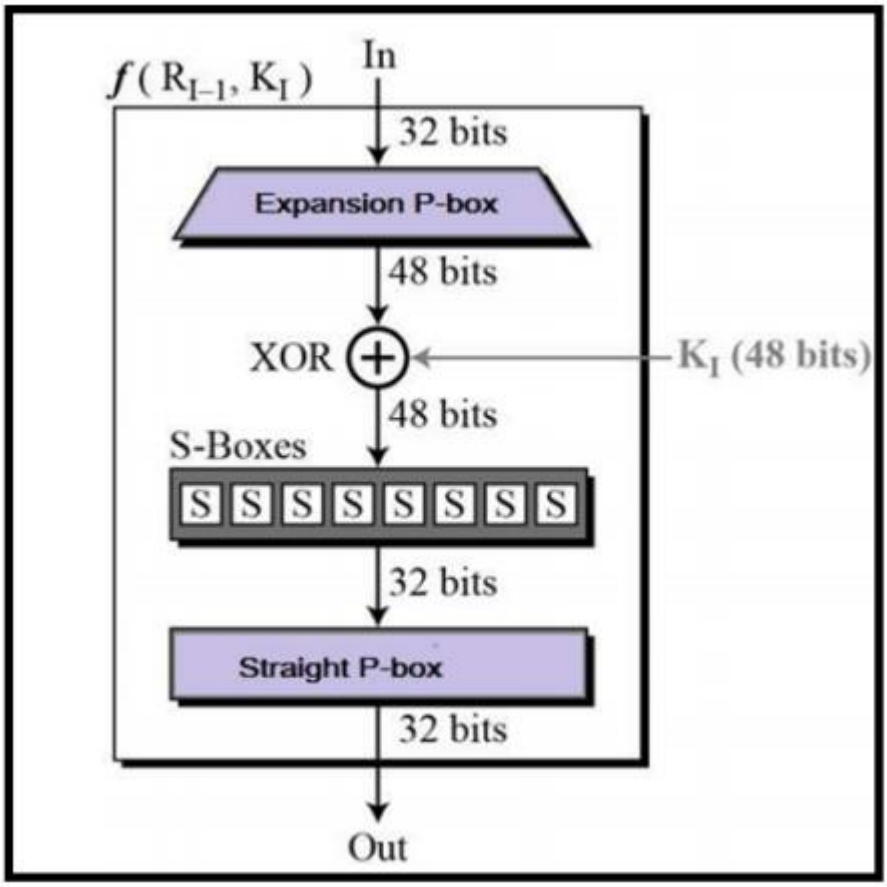
اندازه بلوک و اندازه کلید این الگوریتم ۶۴ بیت است اما طول کلید ۵۶ بیت است و ۸ بیت در رمزگذاری استفاده نمی‌شود. از عملیات زیر در ***DES*** استفاده می‌شود.

- جایگزینی اولیه
- عملکرد ***Round***
- برنامه‌ریزی کلید
- جایگزینی نهایی

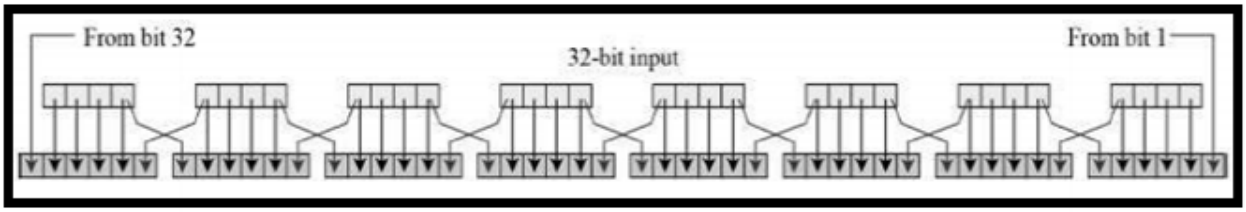
جایگشت اولیه: برای فهم جایگشت اولیه شکل ۱,۶ را مشاهده کنید.

عملکرد *Round*: عملکرد دور هسته اصلی عملکرد ***DES*** است. این عملکرد از کلید ۴۸ بیتی تشکیل شده‌است. ۳۲ بیت کلید که درست‌ترین حالت هستند، خروجی ۳۲ بیتی را تولید می‌کند. جزئیات در شکل ۱,۷ نشان داده شده است.

گسترش جعبه جایگشت: در کلید دور ۴۸ بیت است و ورودی ۳۲ بیت از سمت راست ۴۸ بیت است. نمودار این فرآیند شکل ۱,۸ نشان داده شده است.

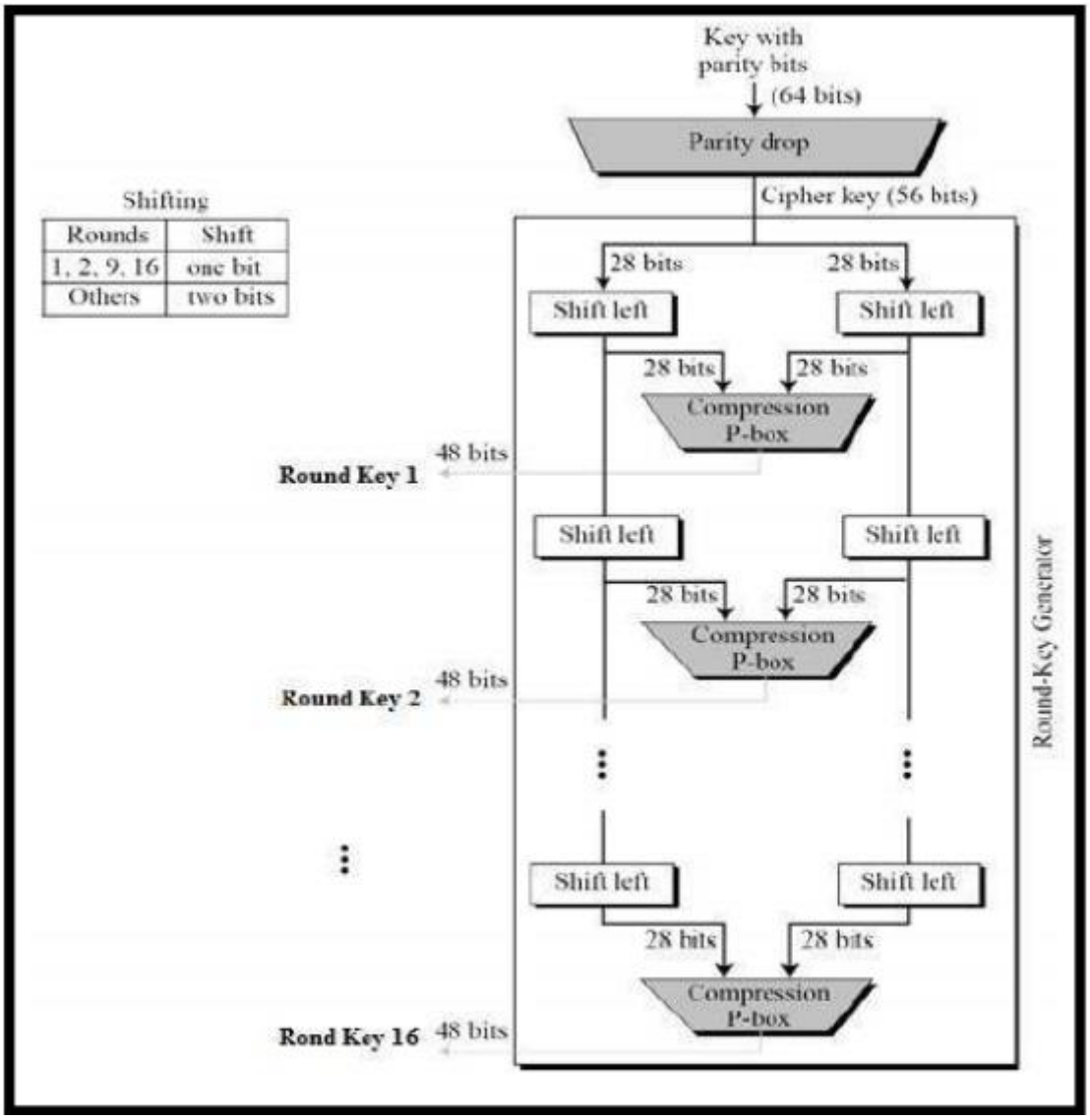


شکل ۱-۷: تابع ***Round***



شکل ۱-۸: گسترش جعبه جایگزینی[۵]

[۵] [۷]**https://www.tutorialspoint.com/cryptography/cryptosystems.htm**

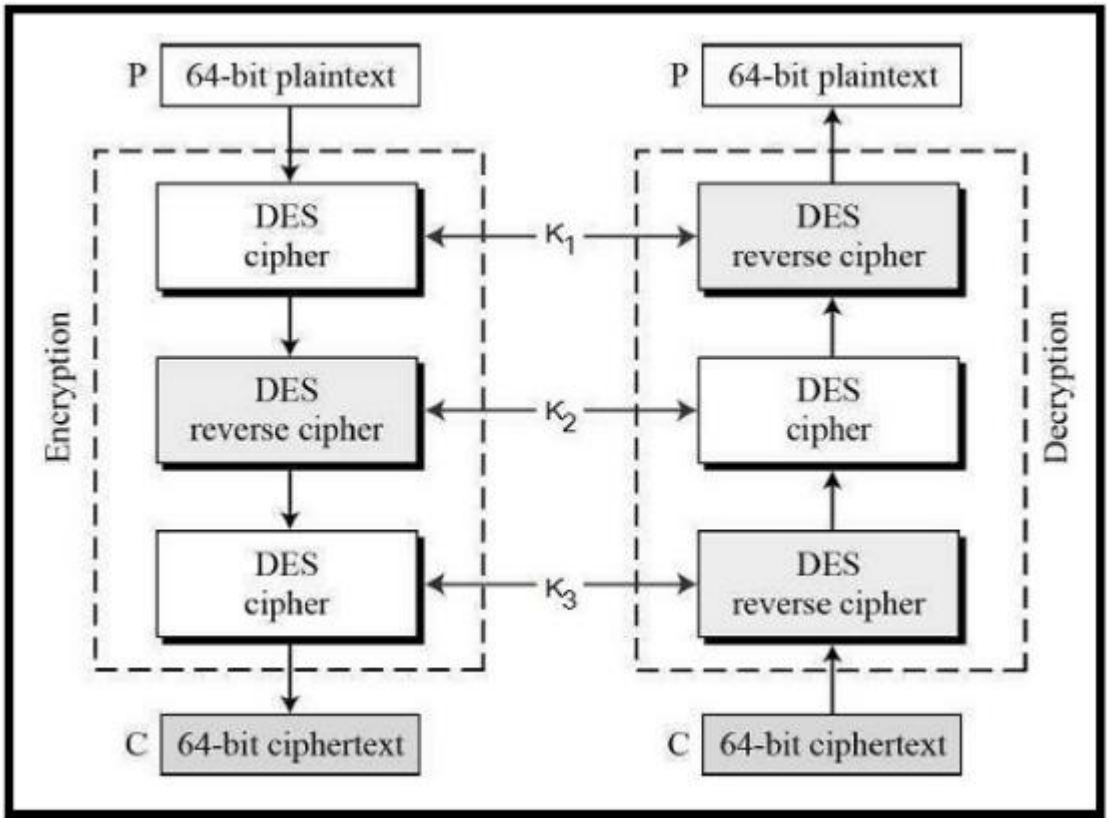


شکل ۱-۹: تولید کلید[۶]

تولید کلید: تابع ***Round*** الگوریتم ***DES*** ، ۱۶ بلوک از کلیدهای ۴۸ بیتی کلید رمزگذاری ۵۶ بیتی ما را ایجاد می‌کند. این فرایند در شکل ۱,۹ نشان داده شده است. اثر ***Avalanche*** به معنی یک تغییر بزرگ در متن رمزگذاری شده، وقتی یک تغییر کوچک در متن اولیه ایجاد شده است. اما طی چند سال گذشته، رمزنگارها گفته‌اند که ***DES*** به دلیل اندازه کلیدها الگوریتمی ضعیف است. به همین دلیل ***NIST*** از الگوریتم ***DES*** به **DES۳** ارتقا می‌یابد.

کار الگوریتم DES۳: شکل ۱,۱۰ را ببینید؛ اولین گام سه کلید ***K1*** ، ***K2***، ***K3.*** تولید می‌کند. اندازه هر کلید ۵۶ بیت است و اندازه کل ۳ کلید برابر با ۳ * ۵۶ = ۱۶۸ بیت است و مراحل رمزگذاری در زیر شرح داده شده است:

[۶] **https://www.tutorialspoint.com/cryptography/cryptosystems.htm**



شکل ۱-۱۰: نمودار معماری ***۳DES*** [۷]

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.

استانداردهای پیشرفته رمزگذاری: ***NIST*** یک الگوریتم متقارن الگوریتم دیگری با نام ***AES*** معرفی کرد؛ به شکل ۱,۱۱ مراجعه کنید. وینسنت ریجمن، جوآن دیمن این الگوریتم را در سال ۱۹۹۸ منتشر کردند. در آن از سه اندازه کلید ۱۲۸و۱۹۲و۲۵۶ بیت و اندازه بلوک ۲۵۶ بیت استفاده می‌شود. ویژگی های 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 ۱۲۸و۱۹۲و۲۵۶ ۵۶ اما اندازه کلید ۲۵۶ ایمن‌تر است.
- قدرت محاسبه سریع‌تر است.

[۷] **https://www.tutorialspoint.com/cryptography/cryptosystems.htm**

- معماری باز است و می‌تواند به راحتی به هر زبان رایانه‌ای طراحی شود.

کار الگوریتم AES

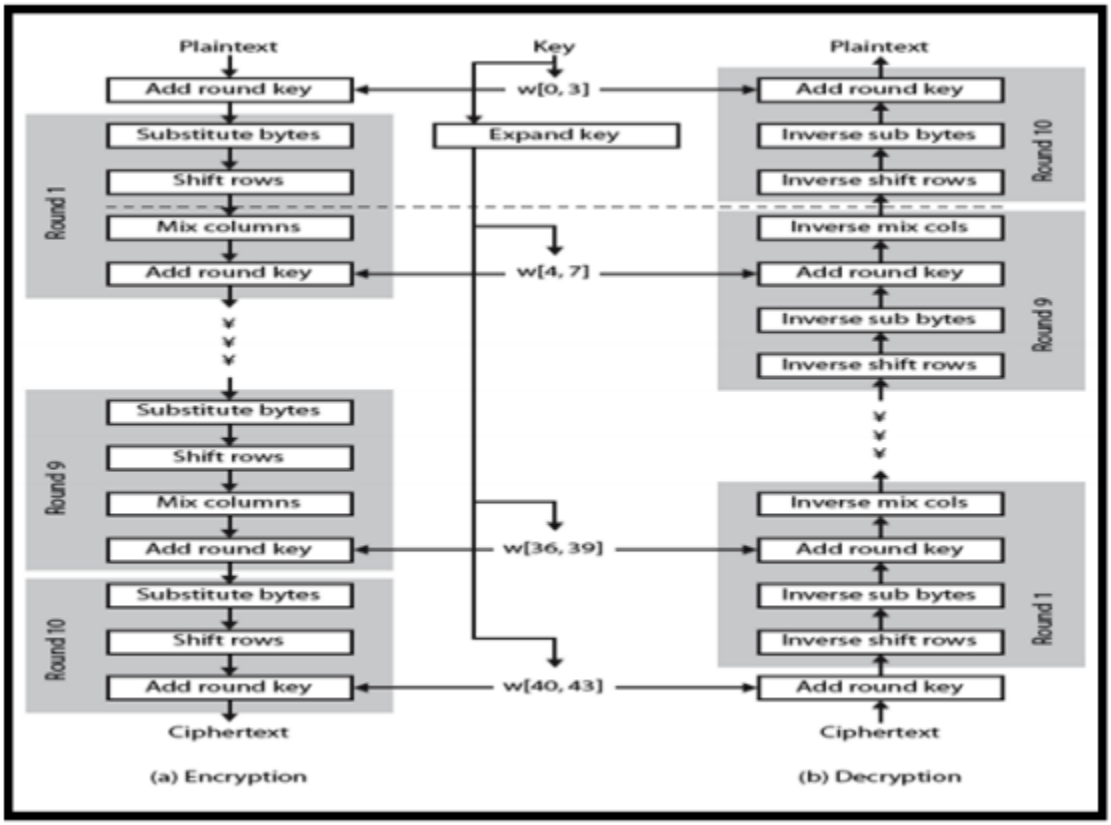
AES روی معماری فایستل کار نمی‌کند. در فایستل نیمی از بلوک داده برای اصلاح نیمی دیگر از داده‌ها استفاده می‌شد.
AES روی کل بلوک به عنوان یک ماتریس واحد برای جایگشت و جایگزینی در هر دور کار می‌کند.
کلید اصلی به مجموعه ای از چهل و چهار ۳۲ بیت کلمه تقسیم شده است. چهار کلمه مشخص با اندازه ۱۲۸ بیت برای کلید ***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 (۲۸)*** 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 می کند: رمزگذاری با یک مرحله ***Add Round Key*** شروع و پایان می یابد.
- اضافه کردن دورهای دور کلید مانند رمز ورنام انجام می شود 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، ردیف های ***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 می کنند. فرآیند 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.

۷,۱ قانون *HIPAA* و *GDPR* چیست؟

HIPAA [۱۰] مخفف قانون قابلیت حمل و پاسخگویی بیمه درمانی است. این مصوبه در سال ۱۹۹۶ توسط دولت ایالات متحده آمریکا برای محافظت از اطلاعات حساس بیمار تصویب شد. این بخش بهداشت و درمان را راهنمایی می‌کند که بیمار و نیازهای آن را حفاظت و امنیت بیشتر به ویژه هنگامی که داده‌ها در محیط ابر هستند؛ فراهم کند.



شکل ۱-۱۱: معماری الگوریتم ***AES*** [۸]

قوانین مختلفی در مورد دسترسی به داده‌ها و محافظت از داده‌ها با توجه به حساسیت داده‌ها ارائه می‌دهد. ۱۸ ویژگی زیر اعمالی که باید محافظت شوند را مشخص می‌کند [۱۱]:

- نام و نام خانوادگی بیمار
- آدرس شامل کد پستی، شهر، کشور
- همه تاریخ‌ها
- شماره تلفن
- نمابر
- شناسه ایمیل
- ***SSNo***(شماره تأمین اجتماعی)
- سوابق پزشکی شماره
- اطلاعات کارت سلامت
- حساب بانکی بدون/ اطلاعات کارت اعتباری
- گواهینامه یا گواهینامه رانندگی
- شماره خودرو
- شناسه دستگاه و شماره سریال

[۸] **http://pranav-mnit.tripod.com/aes.htm**

- آدرس وب
- آدرس پروتکل اینترنت ***(IP)***
- بیومتریک
- هر نوع تصویری
- هر مشخصه دیگری که بتواند منحصراً فرد را شناسایی کند.

GDPR[۱۲] (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.

۸,۱ عامل انگیزه

وقتی اطلاعات بهداشتی محافظت شده به بیرون درز کند، آن هم برای بیماران و هم برای سازمان بهداشت بسیار خطرناک خواهد بود. به عنوان مثال، اگر کارت اعتباری بیمار به سرقت رفته باشد، ممکن است پول خود را از دست بدهد. اما هنگامی که بیمار علیه آن سازمان شکایت می‌کنند، دادگاه آن سازمان را جریمه می‌کند. بنابراین، دو نوع از دست دادن در اینجا اتفاق می افتد. یک بیمار رنج می برد و در عین حال سازمان نیز اعتبار خود را از دست می‌دهد. این نکته ما را تشویق کرد که برای هر دو یک روش مطمئن و قابل اعتماد ارائه دهیم.

۹,۱ بیان مسئله

در مورد قابلیت اطمینان بودن داده‌های ***PHI*** هنگامی که در محیط ابر ذخیره می‌شوند، علامت سوال وجود دارد. این اطلاعات می‌تواند به دلیل ذخیره‌سازی قالب ساده یا با استفاده از الگوریتم‌های رمزگذاری ضعیف درز کند.

۱۰,۱ سوالات تحقیق

بیان مسئله فوق سوالات تحقیق زیر را ایجاد می‌کند- **:**

۱: چه نوع تکنیک‌های محرمانگی داده برای محیط مبتنی بر ابر در دسترس است؟

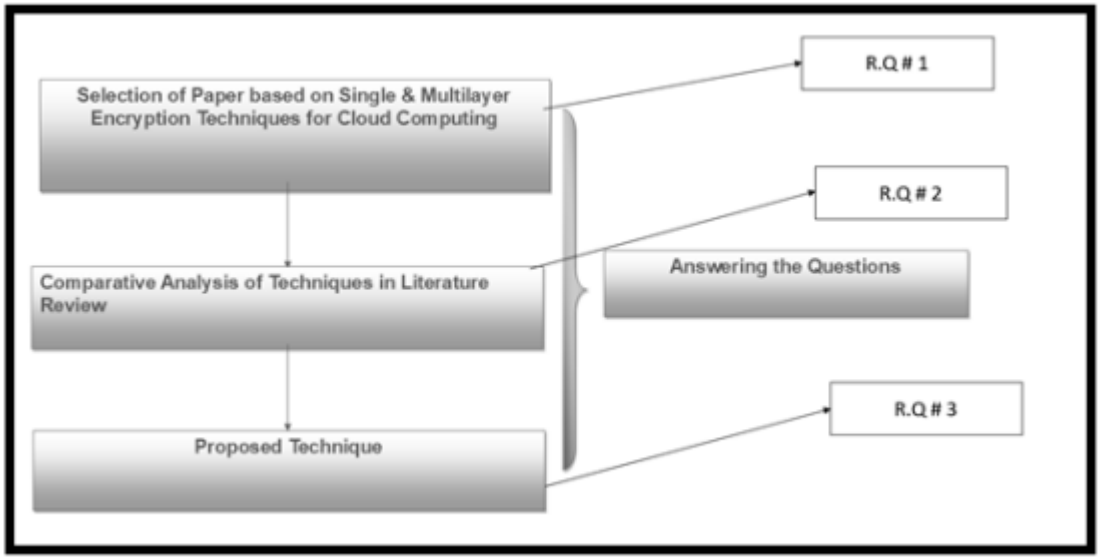
۲: عمده‌ترین ایرادات و نقایص موجود در این تکنیک‌ها چیست؟

۳: چگونه می‌توان از روش‌های رمزگذاری مبتنی بر چند لایه برای حفظ محرمانه بودن داده‌های مراقبت‌های بهداشتی استفاده کرد؟

۱۱,۱ روش تحقیق

روش تحقیق نقش بسیار مهمی برای دستیابی به هدف دارد. از روش نشان داده شده در شکل ۱,۱۲ برای پاسخ به سوالات بالا استفاده می‌کنیم زیرا این امر در یافتن شکاف تحقیقاتی به ما کمک می‌کند. در مرحله اول، ما مقاله را بر اساس تکنیک‌های رمزگذاری تک لایه و چند لایه برای محیط ابر انتخاب کرده‌ایم.

مجموعه‌ی ۴۵ صفحه‌ای انتخاب شده و سپس تجزیه و تحلیل مقایسه‌ای بر روی آن انجام می‌شود و در آخر یک روش پیشنهادی برای رمزگذاری چند لایه پیشنهاد می‌شود. اولین معیار انتخاب مقاله پاسخ دادن به سوال و تجزیه و تحلیل مقایسه‌ای به ما در یافتن شکاف تحقیق کمک می‌کند و در مرحله سوم قادر به تولید تکنیک جدیدی هستیم. این جریان کاری روش ماست که نشان می‌دهد به چه کسی به هدف خواهیم رسید و نشان می‌دهد که به چه کسی به هدف خواهیم رسید.



شکل ۱-۱۲: نمودار روش تحقیق

۱۲,۱ هدف مطالعه

هدف اصلی این رساله ارائه یک طرح جامع است که با در نظر گرفتن انطباق با ***HIPAA*** و ***GDPR*** ، رازداری، یکپارچگی داده‌های بیماران را فراهم می‌کند. این امر با رمزگذاری و رمزگشایی داده‌ها به صورت چند لایه به دست می‌آید و داده‌ها بر اساس تمام وقت در محیط ابر در دسترس هستند. الگوریتم‌هایی که برای رمزگذاری استفاده خواهیم کرد؛ الگوریتم‌های استاندارد هستند که توسط ***NIST***توصیه می‌شوند. ***[۱۳]***

بر اساس این روش، ما شکاف تحقیقاتی را پیدا کرده ایم که رمزگذاری لایه لایه برای بخشهای بهداشتی و همچنین سایر سازمان‌های مرتبط مناسب‌تر است.

۱۳,۱ اهمیت پایان‌نامه

لیست زیر اهمیت پایان‌نامه را نشان می‌دهد:

این مطالعه سطح محرمانگی اطلاعات مربوط به بیمار و بخش مراقبت‌های بهداشتی مبتنی بر فناوری اطلاعات را افزایش می‌دهد.

روش پیشنهادی با استفاده از رمزگذاری چند لایه امنیت بهتری را فراهم می کند.

ترکیب الگوریتم‌ها برای اطمینان از عملکرد و امنیت بهتر نیز انتخاب خواهد شد.

محرمانگی داده ها ، حریم خصوصی	مشکل
بیمارستان‌ها، بیمار، محیط رایانش ابری ، بیمه درمانی و سازمان‌های مرتبط	تأثیر می گذارد

ممکن است منجر به مرگ یک بیمار شود، ضرر زیادی برای سازمان مرتبط با سلامتی ایجاد شود، حریم خصوصی شخصی خدشه‌دار می‌شود. اطلاعات از بین خواهد رفت.	تأثیر آن است
محرمانگی داده‌ها، داده‌های بیمار باید به طور دائم ایمن، مطمئن و در دسترس باشد.	یک راه حل موفق ارائه خواهد شد

جدول ۱-۲: اهمیت پایان نامه

۱۴,۱ نتیجه‌گیری

در زیر نکات کلیدی فصل اول آورده شده است:

رایانش ابری و تاریخچه مختصری از آن .

مدل خدمات رایانش ابری برای بخش مراقبت‌های بهداشتی.

رمزنگاری چیست و یک نگاه اجمالی به تاریخچه آن.

الگوریتم‌های مورد استفاده در تنظیم آزمایشی چگونه کار خواهند کرد؟

چند نکته در مورد ***HIPAA*** و ***GDP R*** .

عامل انگیزشی پایان‌نامه و بیان مسئله.

روش تحقیق چگونه اتخاذ می‌شود؟

اهمیت این پایان‌نامه چیست؟

۱۵,۱ سازمان پایان‌نامه

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 داده ایم.
- 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.

فصل ۲

۲. بررسی ادبیات

برای ارائه یک راه حل جامع از مسئله بحث‌شده در فصل ۱، ما باید در طول بررسی ادبیات، به سوالات زیر پاسخ دهیم.
آیا تکنیک‌های چند لایه برای رمزگذاری و رمزگشایی استفاده می‌شود؟
رویکردهای پذیرفته شده در ادبیات کدام است؟
قدرت تکنیک‌های مورد استفاده کاربران، در چه حدی است؟
اشکال و ضعف در تکنیک‌های فعلی چیست؟
این بخش یک مرور جامع از ادبیات در مورد تحقیقات انجام شده در این زمینه را ارائه می‌دهد و بررسی‌های اساسی از همه روش‌های پیشنهادی را ارائه می‌دهد. ما این فصل را به دو بخش تقسیم کرده‌ایم. بخش ۲,۱ فنون روش تحقیق را نشان می‌دهد. بخش ۲,۲ کارهای مربوطه را نشان می دهد. بخش ۲,۳ بررسی‌های مهم بررسی ادبیات و ۲,۴ نتایج ادبیات را نشان می‌دهد.

۲,۱ کار مرتبط

در [۱۱] نویسنده روش چند لایه‌ای 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 کرده‌اند.
الگوریتم‌های رمزگذاری متقارن **۳DES** و تابع مقدار هش را معرفی کرده اند. نویسندگان از اندازه کلید ۱۹۳ بیت برای لایه ۱ و ۱۲۹ بیت تا ۱۹۲ بیت برای لایه ۲ و ۱۱۲ تا ۱۲۸ برای لایه ۳ و ۸۰ تا ۱۱۱ بیت برای لایه ۴ استفاده کرده‌اند. کار اصلی نویسندگان بر روی الگوریتم **۳DES** است. و از الگوریتم منفرد برای رمزگذاری و رمزگشایی استفاده می‌شود.

در [۱۲] نویسندگان این مقاله 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.
در [۱۳] نویسندگان 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 می‌کند و مالک تاریخ را در سرور ابری بارگذاری می‌کند و کلید را برای استفاده در آینده نگه می‌دارد.
در [۱۴] نویسنده مقاله با استفاده از ***AES*** با ***SOAP / XML*** و ***SHA-1*** فناوری رمزگذاری داده های پزشکی را معرفی کرده است. وی با استفاده از ***SOAP / XML*** داده‌ها را با الگوریتم ***AES*** رمزگذاری کرده است.
در [۱۵] نویسندگان روش جدیدی را برای تجزیه و تحلیل داده‌های بزرگ در بخش مراقبت‌های بهداشتی برای حفظ امنیت و حریم خصوصی پیش بینی کرده‌اند. آن‌ها برای تجزیه و تحلیل داده‌های بزرگ از پروتکل جفت سازی دوخطی استفاده کرده‌اند. آن‌ها همچنین از سیستم مدیریت کلید معتبر استفاده کرده‌اند. پیچیدگی زمان به اندازه کلید بستگی دارد. پیچیدگی محاسباتی با سیستم تطبیق دو خطی اندازه گیری می‌شود.
در [۱۶] نویسندگان الگوریتم ***DES*** ، ***AES***، **۳DES**، ***CAMELLIA***، ***Height*** و ***RECTANGLE*** را با اندازه کلید مختلف و اندازه بلوک داده‌ها مقایسه کرده و نتایج را مقایسه کرده‌اند. آن‌ها همچنین پیشنهاد کرده‌اند که یک ***S-Box*** جدید برای سیستم‌های سلامت الکترونیکی تهیه شود که باعث افزایش سرعت و توان عملیاتی می‌شود.

در [۱۷] نقصی در [۱۸] برای اجرای ***USB MSD*** (دستگاه ذخیره‌سازی انبوه) بیان می‌شود. سپس یک ***ERP*** جدید برای سیستم مراقبت‌های بهداشتی هوشمند معرفی می‌شود که ایمن تر از [۱۷] است.

در [۱۹] نویسندگان 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.

در [۲۰] 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 [۲۱] 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.

در [۲۲] نویسندگان یک روش ترکیبی را پیشنهاد کرده‌اند. آن‌ها با استفاده از الگوریتم ***ElGamal*** برای امنیت داده‌های مراقبت‌های بهداشتی، از روش کدگذاری خطی شبکه استفاده کرده‌اند. برای تبادل کلید از روش رمزگذاری مجدد ***ElGamal*** استفاده شده است. سپس مقایسه‌ای بر اساس ضریب اطمینان حاصل از ***LNC*** با سایر طرح‌ها انجام می‌شود امل رمزگذاری منفرد بر روی داده‌های بیمار انجام می‌شود.

در [۲۳] پروتکل ***EGC*** (رمزنگاری بیضوی گالویس) معرفی شده است که امنیت حفاظت از داده را بالا می‌برد. تمرکز اصلی نویسندگان بر انتقال داده اینترنت اشیا بین ابر و اینترنت اشیا است. با ***ECC***در زمینه ***Galois***، پروتکل پیشنهادی ***EGC*** امنیت بهتری را فراهم می‌کند.

در [۲۴] طرح‌های مدرن در مورد امنیت و حفظ حریم خصوصی، به اشتراک‌گذاری داده‌های پزشکی دهه گذشته با تمرکز بر رویکردهای مبتنی بر بلاکچین بررسی می‌شود. آن را به روش‌های مبتنی بر زنجیره مجاز بدون بلوک و رویکردهای مبتنی بر بلوک اجازه طبقه بندی کرده و مزایا و معایب آن‌ها را تحلیل می‌کنند. همچنین در مورد مباحث بالقوه تحقیقی در مورد به اشتراک‌گذاری داده های پزشکی مبتنی بر بلاکچین بحث کردند.

در [۲۵] ، روش ***ECC*** را برای حفاظت از داده‌های بیمار در ***WBAN*** ارائه داده‌شده‌است. الگوریتم رمزگذاری متقارن ***DES*** و فایستل را برای رمزگذاری و رمزگشایی روی حساس به بیمار اعمال کردند و از ***ECC*** برای مدیریت کلیدهای توزیع، تغییر و ذخیره‌سازی استفاده کردند.

در [۲۶] نویسنده اطلاعات بیماران را با استفاده از الگوریتم استاندارد رمزگذاری پیشرفته ***(AES)*** رمزگذاری کرده‌است. سپس داده‌های پنهان با استفاده از الگوریتم کم‌اهمیت مهم در پشت تصویر محافظت می‌شود. داده‌های محافظت شده، برای گیرنده مورد نظر ارسال می‌شود. در انتها، گیرنده تکنیک ***Inverse*** برای رمزگشایی روی داده‌های رمزگذاری شده را اعمال می‌کند. آن‌ها ادعا کردند که تکنیک آن‌ها با ترکیبی از رمزنگاری و استگانوگرافی امنیت بهتری را فراهم می‌کند.

در [۲۷] نویسندگان روش‌های حسابرسی دیجیتال و مارک گذاری را معرفی کرده‌اند. آن‌ها گفتند که اطلاعات داخلی برای داده‌های بیمار در محیط ابر خطرناک‌تر است و علامت‌گذاری با کیفیت پایین را روی داده‌های کم اهمیت و اهمیت بالا اعمال کردند.

در [۲۸] نویسندگان رویکرد مبتنی بر رمزگذاری ستونی و رمزگشایی مطرح کرده‌اند. طرح جدیدی با نام ***IFHDS*** ساخته شده است. این طرح اطلاعات شخصی و حساس را پوشانده است. مضمون این چارچوب این است که داده های حساس را بر اساس معادله تقسیم کرده و رمزگذاری را روی آن انجام می‌دهد و در ابر ذخیره می‌کند. نویسندگان ادعا کردند که اگر حمله رخ دهد، فقط بخش کوچکی از داده‌ها درگیر خواهند شد نه همه‌شان. آزمایش های مختلفی را روی داده‌های حساس انجام دادند و بهترین روش را بیان کردند اما فقط رمزگذاری تک نوع روی اطلاعات حساس در آن انجام می‌شود.

در [۲۹] یک روش جدید را با استفاده از الگوریتم خوشه‌بندی برای داده‌هایی که به صورت عمودی تقسیم شده اند، ارائه دادند. توان الگوریتم را با استفاده از آزمایش‌های مختلف بررسی کردند. پس از آن، با استفاده از رمزنگاری همومورفیک نسخه محلی از پروتکل را ارائه دادند.

در [۳۰] نویسندگان ایده ای به نام مدل ***MIDEA*** را پیشنهاد کردند. فرآیند رمزگذاری به سرور ابری اختصاص داده شده است. آنها بیان کردند که مقیاس‌پذیری افزایش می‌یابد و هزینه و داده‌های محاسباتی را کاهش می‌دهد. پس از آن متن رمزگذاری ***MAC*** برای محافظت بهتر با داده های ذخیره شده، پیوست می شود.

در [۳۱] نویسندگان کارایی الگوریتم ***AES*** برای حفاظت از داده‌ها را توصیف کردند. آنها در تحقیقات خود الگوریتم ***AES*** را برای افزایش امنیت اصلاح کردند و از تکنیک لایه‌بندی یک‌زمانه، استفاده کردند. ماتریس مربع پلی بیوس را پیاده سازی کردند و همچنین تعداد دورها را برای محافظت از داده‌ها افزایش دادند.

در [۳۲] نویسندگان پیام را با استفاده از تأیید اعتبار ***MAC*** رمزگذاری کردند. آن‌ها از رمز ***AES128*** و ***block block*** برای رمزگذاری پیام استفاده کرده‌اند و تکنیک جدیدی را با الگوریتم ***AES*** بسیار کم قدرت با ۸ بیت معرفی کردند. آنها بیان کردند که این روش از مصرف برق کم با بهره‌وری بیشتر از منابع استفاده می‌کند.

در [۳۳] تکنیکی را به نام رمزگذاری مبتنی بر ویژگی با نام ***HealthShare*** معرفی کرده است و بر روی به اشتراک گذاشتن داده‌های بیمار بود که در ابرهای مختلف بین سازمان‌های مختلف ذخیره می‌شود. آنها پروتکل جدیدی را تهیه کردند که بر اساس رمزگذاری بر اساس ویژگی و سیاست کلید قابل لغو بود و گفتند که ابر داده رمزگذاری شده بیمار بر اساس تمایل بیمار و صاحب داده در سازمانه‌ای مختلف به اشتراک گذاشته می‌شود.

در [۳۴] پروتکل جدیدی را برای محافظت از ذخیره اطلاعات در ابر ابداع کرد. نظریه آن‌ها بر دو نکته اصلی استوار است. در ابتدا سیستم بهداشت و درمان زیمنس را با نام ***Melior*** توصیف کرد. دوم، در مورد چالش مهاجرت سیستم سلامت بیمار در ابر و اینکه چه شرایط اساسی امنیتی برای حرکت در ابر مورد نیاز است، بحث کرده‌اند.

در [۳۵] نویسندگان روش رمزگذاری داده های متن ساده را با الگوریتم‌های منفرد که در حال حاضر در بازار موجود است، توضیح دادند. آن‌ها گفتند که اگر می‌خواهید داده‌های بزرگ بخش مراقبت‌های بهداشتی را تأمین کنید، باید برخی از رویکردهای جدید را اتخاذ کنید که مبتنی بر فرآیندهای توزیع شده بزرگ و ذخیره سازی در فضای ابری است.

در [۳۶] نویسنده به بخش مراقبت‌های بهداشتی درباره حمله داخلی و خارجی هشدار داده است. وی گفت که نسبت حملات خودی نسبت به افراد خارجی بسیار زیاد است. همچنین می‌گوید که ۵۲٪ بیمارستان‌های بهداشتی معتقدند که به دلیل افراد داخلی در معرض خطر بالایی قرار دارند. از آن‌جا که افراد داخلی می‌توانند سوابق بیمار را به راحتی تغییر دهند و می‌توانند به راحتی داده‌ها را برای هر نوع خرابکاری بفروشند. همچنین می‌تواند از بیمار باج‌گیری و درخواست پول کند.

در [۳۷] نویسندگان گفتند که استفاده از داده‌های اینترنتی بسیار محبوب و آسان شده است. اینترنت منبعی است که از طریق آن می‌توان داده‌ها را سریع و بسیار دقیق به مقصد منتقل کرد. اما، مهاجمان ممکن است از آن سواستفاده کنند. آن‌ها گفتند که روش‌های رمزنگاری و استگانوگرافی برای این امر بسیار مفید است. در این مقاله از الگوریتم کمترین اهمیت ***(LSB)*** در داده‌های مبتنی بر تصویر بیمار مانند اشعه ایکس، ***MRI*** و غیره برای رمزگذاری استفاده کرده‌اند و از برخی روش‌های یادگیری ماشین برای مقایسه استفاده کرده‌اند.

در [۳۸] نویسندگان روش جدیدی ایجاد کرده‌اند که می‌تواند برای پنهان کردن اطلاعات در تصویر استفاده شود. آن‌ها فایلی را که نیاز به رمزگذاری دارد فشرده کرده‌اند. سپس بر روی فایل فشرده شده الگوریتم ***AES*** را اعمال کرده و پس از آن تکنیک‌های استگانوگرافی را با استفاده از الگوریتم‌های ***LSB*** اعمال کردند.

در [۳۹] نویسندگان تشخیص و گزارش پزشکان را در تصاویر اسکن شده اعمال کردند و سپس از استگانوگرافی و رمزنگاری استفاده کردند.

در [۴۰] نویسندگان الگوریتم فایستل را بدون ***S-Box*** ساده کرده اند. سپس رمزگذاری و رمزگشایی را روی داده‌های حساس بیمار اعمال کرده‌اند. آن‌ها نتایج را با الگوریتم‌های قدیمی ***DES*** مقایسه کرده‌اند و اذعان کرده‌اند که به دلیل حذف ***S-Box*** ، تکنیک‌هایشان دارای اثر ضعیف است.

در [۴۱] نویسندگان از پروتکل ***ECC*** و ***SNAP*** برای ایمن سازی اطلاعات بیمار برای ***WBAN*** استفاده کرده‌اند و گفتند که هر سنسور دارای یک دستگاه بیومتریک است که بیمار را تأیید می‌کند و سپس می‌تواند اطلاعات بخش‌ها را به اشتراک بگذارد.

در [۴۲]نویسندگان یک سیستم کنترل دسترسی مبتنی بر نقش به نام ***(CPRBAC)*** برای حفاظت از داده‌های ابری ایجاد کرده‌اند. همچنین یک تکنیک حسابرسی ایجاد کرده‌اند که برای نظارت فعال و گزارش هرگونه فعالیت غیرقانونی بر روی سیستم استفاده می‌شود اما در کارشان از هیچ روش رمزنگاری استفاده نشده است و درنتیجه جامعیت و محرمانگی ممکن است حفظ نشود.

در [۴۳] نویسنده یک سیستم الکترونیکی بیمار محور معرفی کرده است. با استفاده از این بخش‌های انتخابی می‌توان داده‌ها را در ابر به اشتراک گذاشت. آن‌ها از رمزگذاری ویژگی پخش بر روی پرونده‌های بیمار استفاده کرده‌اند. همچنین از رمزگذاری کلید عمومی با تکنیک‌های جستجوی رمزگذاری کلید عمومی استفاده کرده‌اند اما الگوریتم را تعریف نکرده‌اند.

در [۴۴] نویسندگان برای محافظت از اطلاعات بیمار، روش بلاک را با روش مبتنی بر امضا مخلوط کرده‌اند. تکنیک‌های مبتنی بر امضا تأیید می‌کنند که داده‌ها از زنجیره اصلی ارسال و بلوک ارائه می‌کنند. اما تمام داده‌ها را در بلوک‌های زنجیره‌ای ذخیره کرده‌اند که تأثیر زیادی بر عملکرد شبکه دارد.

در [۴۵] نویسندگان ***PHR*** را با رمزگذاری بر اساس ویژگی در محیط ابر نیمه مطمئن فراهم کرده‌اند و گفتند که دامنه عمومی برای پزشکان و محققان و حوزه شخصی برای خانواده و دوستان است. تکنیک‌های ***ABE*** را برای ابر عمومی و خصوصی به طور جداگانه تقسیم کرده‌اند. این امر بار سنگینی را بر دوش بیمار می‌گذارد که چگونه می‌تواند کلیدها را مدیریت کرده و به کاربران اجازه دهد.

در [۴۶] نویسندگان یک الگوریتم ایجاد کرده‌اند و تکنیک‌های رمزگذاری چند فازی و چندگانه را ترکیب می‌کنند. آن‌ها از الگوریتم های***AES 256*** ، ***RSA***، ***DES***، ***Blowfish*** برای روند رمزگذاری چند فاز تصادفی استفاده کرده‌اند. در پایان آنها پیچیدگی زمان و امنیت داده‌ها راروی اندازه‌های مختلف داده، مقایسه کردند.

در [۴۷] نویسندگان الگوریتم ***ECC*** را برای رمزگذاری چندین بار پیاده سازی کرده‌اند. آن‌ها مشاهده کردند که استفاده چندگانه از زمان استفاده از الگوریتم ***ECC*** باعث پیچیدگی زمان می‌شود. به گفته آن‌ها بین امنیت و زمان رابطه وجود دارد.

در [۴۸] نویسندگان چندین رمزگذاری را در انتقال الکترونیکی ایمن پیاده سازی کرده‌اند. آن‌ها گفتند که این فرآیند رمزگذاری چندگانه امنیت بهتری را فراهم می‌کند. آن‌ها استراتژی خود را در تبادلات خودپرداز اعمال کرده‌اند.

در [۴۹] نویسندگان الگوریتم‌های هومومورف را مقایسه کرده‌اند. آن‌ها فقط توضیح داده‌اند که کلیدهای رمزگذاری و رمزگشایی بر روی ابر چگونه کار می‌کنند.

در [۵۰] نویسندگان گفتند که ***IDM*** (مدیریت هویت) مشکل اصلی در محیط ابر است. آنها روش ***IDM*** را پیشنهاد کردند که به اشخاص ثالث اعتماد نمی‌کند. از کلید توزیع ***RSA*** و روش رمزگذاری مبتنی بر ویژگی برای امنیت داده‌های حساس استفاده کرده اند.

در [۵۱] الگوریتم‌های مختلف رمزگذاری برای امنیت داده‌ها در ابر بررسی شده‌اند. نویسندگان سطح امنیتی الگوریتم‌های مختلف استانداردها را مقایسه کرده‌اند.

در [۵۲] چالش‌های مختلف محیط ابر برجسته شده است. نویسندگان برای امنیت داده‌ها، پیشنهادات مختلفی را به ارائه‌دهندگان مختلف ابر ارائه داده‌اند.

در [۵۳] نویسندگان یک رویکرد جدید برای بهبود امنیت داده‌ها ارائه داده‌اند و پیشنهاد کردند که چگونه یک ابر سازمانی از تکنیک‌های خاص رمزگذاری به نام رمزگذاری مبتنی بر مکان استفاده می‌کند.

در [۵۴] امنیت داده مورد بحث است. ***ECC*** نیز از اهمیت برخوردار است و بحث می‌شود.

در [۵۵] چالش‌های مختلف امنیتی رایانش ابری بازنگری شده، تکنیک‌های مختلف امنیت داده مورد بحث قرار گرفت که قابلیت اطمینان را ایجاد می‌کند.

۲,۲ تجزیه و تحلیل بررسی ادبیات

ما یک تجزیه و تحلیل آزمایشی را بر اساس بررسی ادبیات انجام داده ایم و نتایج نویسندگان مختلف را بر اساس مطالب فوق مقایسه کرده و سپس یک شکاف تحقیقاتی پیدا کرده ایم به جدول ۲,۱مراجعه کنید. با این حال ، برخی از مفهوم رمزگذاری مبتنی بر چند لایه توسط نویسندگان مختلف در مورد اطلاعات محافظت شده ارائه شده است ، اما دریافتیم که هیچ کس از این روش ساخته شده در***RDBMS*** (سرور ***Micro soft SQL***و پشتیبانی از الگوریتم های رمزنگاری) به ویژه مدیریت کلیدها در مورد متقارن و نامتقارن استفاده نکرده است. **ترجیح می دهیم از کلید متقارن استفاده کنیم** زیرا در اینجا در ماژول ما نمی خواهیم کلیدها را با بیمار نیز به اشتراک بگذاریم. این امر باعث افزایش سطح امنیت می شود.

کاغذ	رویکرهای چند لایه	امنیت هدف	نقاط قوت	نقاط ضعف
[۱۱]	بله	محرمانگی اطلاعات	**۳DES** و الگوریتم هش	چگونگی کلیدهای به اشتراک گذاشته شده، استانداردهای ***HIPAA*** و ***GDPR***
[۱۲]	خیر	محرمانگی اطلاعات	الگوریتم چند لایه	چگونگی کلیدهای به اشتراک گذاشته شده، استانداردهای ***HIPAA*** و ***GDPR*** و ***RDBMS*** تعبیه شده

[۱۳]	خیر	محرمانگی اطلاعات	الگوریتم ***ECC***	روش رمزگذاری منفرد استفاده شده است ، از هر استانداردی استفاده نکرده است.
[۱۴]	خیر	محرمانگی اطلاعات	الگوریتم ***AES***	روش رمزگذاری منفرد استفاده شده است. از هر استانداردی مانند ***HIPAA***، ***GDPR***پیروی نکرده است.
[۱۵]	بله	محرمانگی اطلاعات	جفت سازی دوخطی و کلید احراز هویت	مسائل کلیدی مدیریت وانطباق ***HIPAA***و***GDPR***
[۱۶]	خیر	محرمانگی اطلاعات	نظرسنجی روی الگوریتم‌های ***AES***و***DES***و**۳DES**	پیاده‌سازی ندارد.
[۱۷] [۱۸]	خیر	محرمانگی اطلاعات	محافظت ***USB*** برای داده‌های مراقبت بهداشتی	رمزنگاری تک لایه
[۱۹]	بله	محرمانگی اطلاعات	***EPR*** و ***LSB***	رمزگذاری مبتنی بر تصویر از هیچ استانداردی مانند ***GDPR,IPAA*** پیروی نمی‌کند.
[۲۰]	خیر	محرمانگی اطلاعات	رمزگذاری مبتنی بر نقش	از هیچ استانداردی مانند ***HIPAA***و***GDPR*** پیروی نمی‌کند.
[۲۱]	بله	محرمانگی اطلاعات	مبتنی بر اینترنت اشیا	رمزگذاری منفرد
[۲۲]	خیر	محرمانگی اطلاعات	الگوریتم***Elgmal***	رمزگذاری منفرد
[۲۳]	خیر	محرمانگی اطلاعات	***ECC***	رمزگذاری منفرد
[۲۴]	خیر	محرمانگی اطلاعات	بلاکچین	از هیچ استانداردی مانند ***HIPAA***و***GDPR*** پیروی نمی‌کند.
[۲۵]	بله	محرمانگی اطلاعات	***DES***و فایستل و مدیریت ***WBAN***	از هیچ استانداردی مانند ***HIPAA***و***GDPR*** پیروی نمی‌کند.
[۲۶]	بله	محرمانگی اطلاعات	الگوریتم ***AES,LSB***	به عنوان رمزگذاری مبتنی تصویر استفاده می‌شود.
[۲۷]	بله	محرمانگی اطلاعات	نشانه گذاری روی داده‌ها	از هیچ استانداردی مانند ***HIPAA***و***GDPR*** پیروی نمی‌کند.

[۲۸]	خیر	محرمانگی اطلاعات	پارتیشن‌بندی داده‌ها و اعمال رمزگذاری منفرد داده‌ها	بدون رمزگذاری چند لایه
[۲۹]	خیر	محرمانگی اطلاعات	پارتیشن‌بندی عمودی و فعال‌سازی رمزگذاری	رمزگذاری منفرد
[۳۰]	خیر	محرمانگی اطلاعات	مدل ***MIDEA*** برای رمزگذاری و رمزگذاری مبتنی بر ***MAC***	
[۳۱]	بله	محرمانگی اطلاعات	رمزگذاری مبتنی بر ***AES*** و پنهان کردن داده‌ها در پشت مستطیل گوشه‌گرد	رمزگذاری مبتنی بر تصویر و داده ها در ***RDBMS*** ذخیره می‌شوند و سپس فعال میشوند.
[۳۲]	بله	محرمانگی اطلاعات	***AES128*** بیتی و بلاکچین	پیاده‌سازی روی ***RDBMS*** و از هیچ استانداردی مانند ***HIPAA*** ، ***GDPR*** پیروی نمی‌کند.
[۳۳]	بله	محرمانگی اطلاعات	رمزگذاری مبتنی بر ویژگی و کلید قابل لغو	پیاده‌سازی روی ***RDBMS*** و از هیچ استانداردی مانند ***HIPAA*** ، ***GDPR*** پیروی نمی‌کند.
[۳۴]	خیر	محرمانگی اطلاعات	نظر سنجی	
[۳۵]	خیر	محرمانگی اطلاعات	رمزگذاری منفرد	
[۳۶]	خیر	محرمانگی اطلاعات	مهاجمان خودی از خارجی خطرناک‌تر هستند.	
[۳۷]	بله	محرمانگی اطلاعات	استگانوگرافی با استفاده از ***LSB*** و تبدیل به تصویر	روی خصوصیات ***PHI*** ممکن نیست.
[۳۸]	بله	محرمانگی اطلاعات	***AES*** با کمی تغییر و سپس ***LSB***	تبدیل به داده‌های مبتنی بر تصویر
[۳۹]	خیر	محرمانگی اطلاعات	استگانوگرافی	رمزگذاری منفرد
[۴۰]	بله	محرمانگی اطلاعات	الگوریتم فایستل ریتم با تغییر ***S-box*** و ***DES***	استفاده از تکنیک های قدیمی

جدول ۲-۱: مرور آنالیز ادبیات

۳,۲ دست‌آوردهای تجزیه و تحلیل

از این تجزیه و تحلیل مهم مشخص شده است که تمام تکنیک ها برای حفاظت از داده های حساس به روش‌های مختلف استفاده می‌شوند. برخی از نویسندگان الگوریتم رمزنگاری مختلفی را برای نتایج بهتر ترکیب کرده‌اند. تعداد کمی از تکنیک‌های قدیمی رمزگذاری و رمزگشایی استفاده کرده‌اند. برخی استانداردهای ***HIPAA*** را تا حدی در نظر گرفته‌اند. گروه دیگری از الگوریتم یادگیری ماشین مختلف استفاده کرده و داده‌ها را به شکل تصاویر در ابر ذخیره کرده‌اند. با این حال، نشان دادیم که تکنیک‌های تحقیق شده عملکرد ***HIPAA*** و ***GDPR*** را در ویژگی‌های ***PHI*** با رمزگذاری چند لایه ترکیب نکرده‌اند. به اشتراک‌گذاری کلیدها نیز بین رمزگذاری و رمزگشایی مسئله بزرگی است. برای به اشتراک گذاشتن کلیدها باید شخص ثالثی را درگیر کنیم یا باید به‌ازای هر کلید هزینه کنیم. به همین دلیل راه حل گران خواهد شد.

درتحقیقات، نشان دادسم که در ویژگی های ***HIPAA*** و ***GDPR*** برای اطمینان از داده‌های حساس بیمار، توجه بیشتری لازم است. بنابراین، تکنیک‌های جدیدی را ارائه داده‌ایم که در آن ویژگی‌های داده بیمار را مطابق با ***HIPAA*** و ***GDPR*** گرفته و رمزگذاری چند لایه را بر روی آن اعمال کرده و سپس نتایج را با سایر روش‌ها برای بررسی محرمانگی و عملکرد مقایسه خواهیم کرد. مطمئنا این روش باعث افزایش محرمانگی، اعتماد بیمار و همچنین بخش مبتنی بر بهداشت فناوری اطلاعات می‌شود. همچنین مفهوم جدیدی از حفاظت در بخش مراقبت‌های بهداشتی باز خواهد شد.

۴,۲ خلاصه

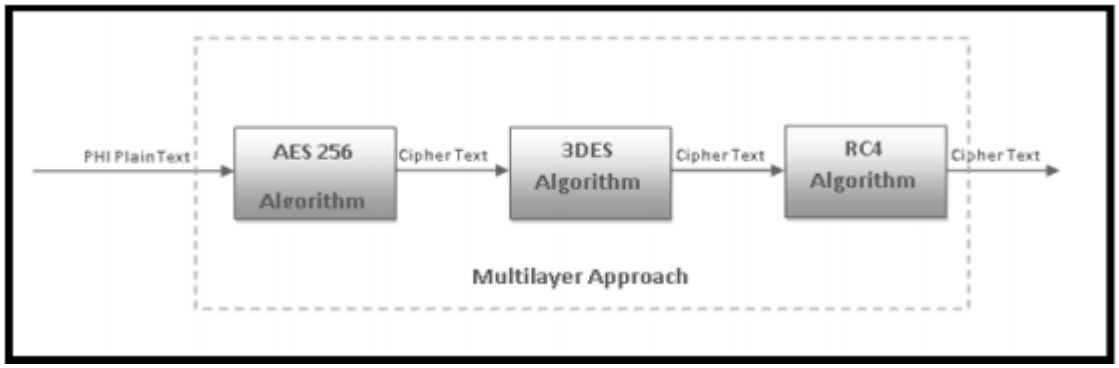
در مجموع ۴۵ مقاله تحقیقاتی را مرور کردیم که ۸ مقاله در اینجا نشان داده شده است. در ادبیات ما ۸-۱۰ تکنیک مبتنی بر الگوریتم های رمزنگاری منفرد است که ۵-۶ نویسنده بر روی داده‌های مبتنی بر تصویر کار کرده‌اند و داده‌ها را به تصاویر تبدیل کرده‌اند و ۲ نویسنده نیز بر روی رمزگذاری بر اساس نقش کار کرده اند، نظریه دیگر مربوط به تکنیک های بلاکچین است. دو تکنیک مربوط به شبکه بی‌سیم بدن منطقه است. توجه برخی از نویسندگان بیشتر به داده‌های مبتنی بر ***IOT*** است. یک نویسنده بر حملات خودی تأکید کرده و گفته است که خودی ها خطرناک‌تر از خارجی‌ها هستند. بنابراین نتیجه این است که ما دریافتیم هیچکدام با در نظر گرفتن اقدامات ***HIPAA*** و ***GDPR*** تکنیک های رمزگذاری چند لایه را برای محافظت از صفات ***PHI*** بیمار ترکیب نکرده است. فکر می‌کنیم که این پژوهش می‌تواند برای بخش مراقبت‌های بهداشتی مفید باشد که از طریق آن اطلاعات بیمار محافظت شود و سطح محرمانگی افزایش یابد.

فصل ۳

۳. راه‌اندازی آزمایشی طرح پیشنهادی

در این فصل، ما روش‌های پیشنهادی را تجزیه و تحلیل کرده‌ایم. این طرح بر روش‌های رمزگذاری و رمزگشایی متمرکز است که چگونه از اطلاعات محافظت شده/ حساس بیماران محافظت کنیم. ما طرحی را توسعه داده‌ایم که داده‌های ***PHI*** را با توجه به الگوریتم چندلایه رمزگذاری می‌کند. سپس داده‌های رمزگذاری شده در هر سرور مبتنی بر ابر قابل اعتماد بارگذاری می‌شود که برای آینده احتمالی بیمار در دسترس خواهد بود. ما با استفاده از معماری کلاینت/ سرور که باید از طریق شبکه منتقل شود، طرح فوق را توسعه داده ایم.

ما این فصل را به بخش‌های مختلفی تقسیم کرده‌ایم. بخش ۳,۱ نحوه دستیابی به مجموعه داده را توصیف می‌کند، بخش ۳,۲ نحوه رمزگذاری داده‌ها را توصیف می‌کند، بخش ۳,۳ معماری متد را توصیف می‌کند ، بخش ۳,۴توضیح می‌دهد که امکانات رمزگذاری در پایگاه داده سرور ***SQL*** برای تبلیغ رمزگذاری موجود است. بخش ۳,۵ نتیجه‌گیری است.



شکل ۳-۱: تکنیک محافظت از چند لایه

۱,۳ انتخاب مجموعه داده‌ها

برای توسعه طرح و تجزیه و تحلیل هدف، یک مجموعه داده ساختگی(برای ایمنی بیمار) از حدود ۵۰۰ بیمار را انتخاب کرده‌ایم و از نمودار زیر برای رمزگذاری ***PHI*** هر ویژگی استفاده کرده‌ایم.

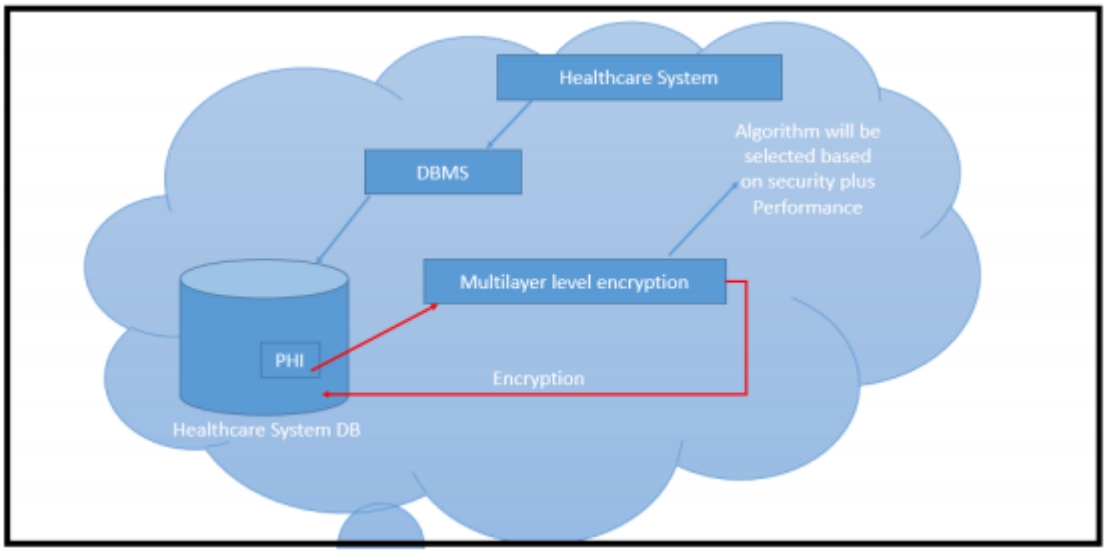
۲,۳ لایه رمزگذاری *PHI Attribut ES*

شکل ۱,۳ نشان می‌دهد که یک ویژگی از داده‌های ***PHI*** به شکل متن ساده انتخاب شده است. این ویژگی به یک الگوریتم منتقل می‌شود. به عنوان مثال ***AES256*** با یک کلید و سپس خروجی این الگوریتم که متن رمزگذاری شده‌ای است و با یک کلید دیگر به الگوریتم **۳DES** منتقل می‌شود. این مفهوم رمزگذاری چند لایه است که از داده‌ها محافظت می‌کند و سطح محرمانگی را افزایش می‌دهد.

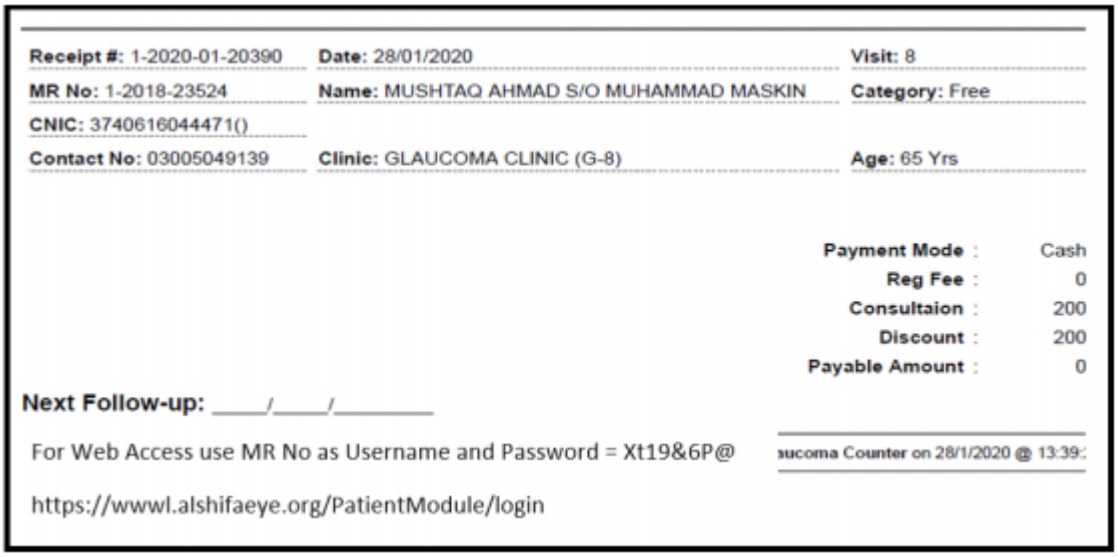
۳,۳ معماری روش

شکل ۲,۳ یک سیستم مراقبت‌های بهداشتی با سیستم مدیریت پایگاه‌داده را نشان می‌دهد. تمام داده‌های مربوط به ***PHI*** در پایگاه‌داده ذخیره می‌شوند. داده‌های تست ساختگی را از پایگاه‌داده گرفته و الگوریتم‌های رمزگذاری موجود در ***RDBMS*** را اعمال

و الگوریتم‌های استاندارد را روی ویژگی‌های ***PHI*** اعمال می‌کنیم و داده‌ها را در محیط ابر ذخیره می‌کنیم. در آغاز ثبت نام بیماران، شماره ***MR*** با رمز عبور پیچیده‌ای که به طور تصادفی ایجاد شده است، برای اطلاعات بیمار اختصاص می‌یابد.



شکل ۳-۲: نمودار معماری روش‌شناسی



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
Consultaion :	200
Discount :	200
Payable Amount :	0

Next Follow-up: ____/____/_____

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

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

https://wwwl.alshifaeye.org/PatientModule/login

شکل ۳-۳: فیش ورود به سیستم برای بیمار

برای دسترسی در وب سایت(به شکل ۳,۳ مراجعه کنید) 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 **۳DES** بر روی داده‌ها اعمال می‌کنیم زیرا 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.

۴,۳ فرآیند رمزگذاری و رمزگشایی در *RDBMS* (*(Microsoft SQL Server)*

سرور ***SQL*** با استفاده از کلید نامتقارن یا متقارن ارائه شده **۳DES** و انواع مختلف ***AES*** را برای رمزگذاری و رمزگشایی فراهم کرده است. سرور ***SQL*** گواهی نامه‌های داخلی را حفظ می‌کند. با این کار گواهینامه‌ها و کلیدها سلسله مراتبی را برای رمزگذاری و رمزگشایی فراهم می کند. به این ویژگی ***SQL*** ذخیره سازی مخفی گفته می‌شود.

ویژگی اصلی فرایندهای رمزگذاری پشتیبانی شده توسط سرور ***SQL*** سرعت است. روش‌های رمزگذاری متقارن بسیار سریع هستند و با حجم زیادی از داده‌ها کار می‌کنند. ویژگی دیگر این است که چندین کلید متقارن می‌توانند همزمان باز شوند و رمزگذاری و رمزگشایی از این طریق انجام می‌شود.

۱,۴,۳ چگونه رمزگذاری در *SQL Server* انجام می‌شود؟

شکل ۴,۳ روند رمزگذاری کلی از ***SQL Server*** بر روی یک ستون از یک جدول را نشان می‌دهد.

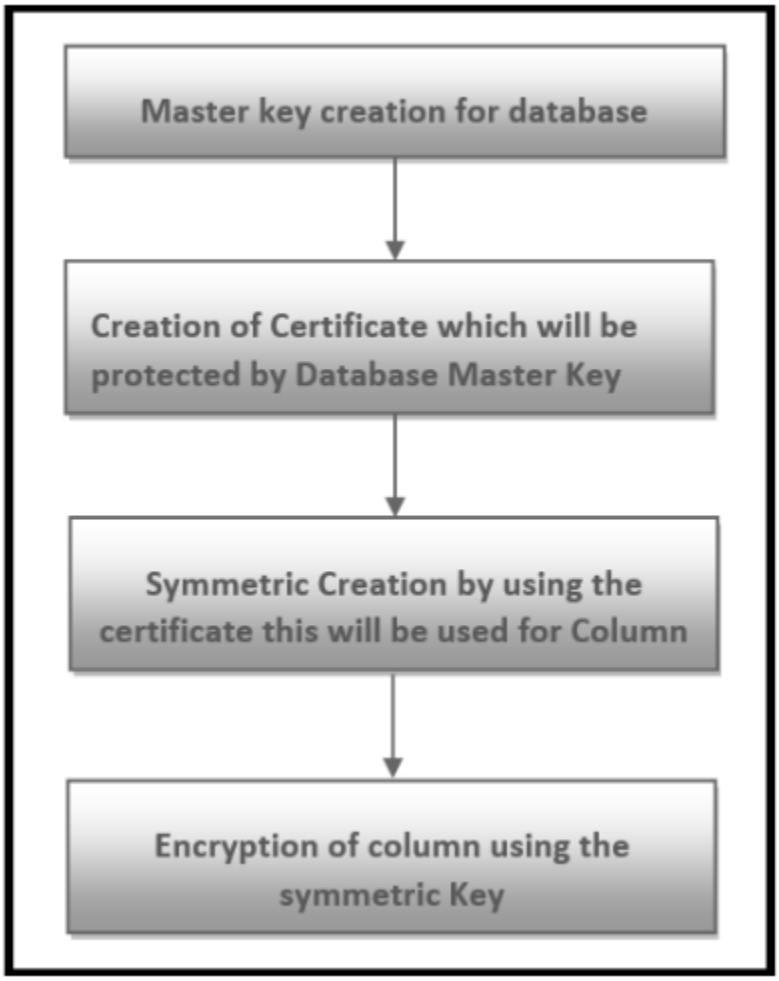
هدف اصلی کلید اصلی پایگاه‌داده، محافظت از کلیدها و گواهینامه‌های خصوصی است که در پایگاه‌داده ذخیره می‌شوند که بر اساس روش متقارن است. این کلید توسط رمز عبور در زمان ایجاد محافظت می‌شود.

۱,۱,۴,۳ ایجاد کلید اصلی

در مراحل رمزگذاری قبل از هر چیز یک کلید اصلی با رمز عبور مورد نیاز است. پس از آن یک گواهینامه بر اساس کلید اصلی تولید می شود.

۲,۱,۴,۳ ایجاد گواهی

در این‌جا ***RDBMS*** یک گواهینامه دیجیتالی نیاز دارد که برای محافظت از کلید اصلی پایگاه‌داده مورد استفاده قرار می‌گیرد.



شکل ۳-۴: فرآیند رمزگذاری کلی

۳,۱,۴,۳ کلید متقارن

در مرحله بعدی، یک کلید متقارن مورد نیاز است که برای رمزگذاری و رمزگشایی استفاده می‌شود. این کلید بر اساس الگوریتم‌های رمزگذاری است که در سرور ***sql*** ساخته شده است؛ به عنوان مثال***AES128*** ، ***AES192***و***AES256*** . برای رمزگذاری کلید متقارن از سرور ***SQL*** از گواهی دیجیتالی که قبلاً در بالا ایجاد کرده‌ایم استفاده می‌کنیم.

۴,۱,۴,۳ ایجاد گواهی

اکنون، برای تغییر داده‌های رمزگذاری شده در ذخیره‌سازی، باید شمای جدول و فیلدهایی با حداکثر طول ستون را تغییر دهیم. در اینجا، فرم کلی رمزگذاری را شرح داده‌ایم که نحوه انجام یک رمزگذاری در ***RDBMS*** (سرور***SQL***) و اجرای آن در فصل بعد شرح داده شده است.

۵,۳ نتیجه گیری

در این فصل این نکات اصلی را شرح داده‌ایم:

- چگونه مجموعه داده‌ای را برای طرح پیشنهادی ترتیب می‌دهیم ؟
- چگونه رمزگذاری چند لایه روی ویژگی‌های ***PHI*** انجام می‌شود؟

- روش ما چگونه خواهد بود؟
- نحوه رمزگذاری و رمزگشایی در ***RDBMS***
- مفهوم کلید اصلی چیست؟
- هدف از گواهی‌نامه چیست؟
- کلید متقارن در ***RDBMS*** چگونه کار می‌کند؟
- گواهی و کلیدها چگونه ایجاد می‌شوند؟

فصل ۴

۴. تجزیه و تحلیل آزمایشی طرح پیشنهادی

این فصل به طور دقیق روش عملی رمزگذاری در یک جدول و نتایج بدست‌آمده از این طرح را با جزئیات شرح می‌دهد. فصل ۴ به بخش‌های مختلف تقسیم شده است. بخش ۱,۴ در مورد داده ها و اطلاعات بحث می‌کند. بخش ۲,۴ تنظیمات آزمایشی را توصیف می‌کند. بخش ۳,۴ فرآیند رمزگذاری را تشریح می‌کند. بخش ۴,۴ روند رمزگشایی را توصیف می‌کند و آخرین بخش ۴,۵ مربوط به بخش تجزیه و تحلیل نتایج است.

۱,۴ انتخاب مجموعه داده

ما یک مجموعه داده ساختگی از ۵۰۰ بیمار را برای هدف آزمایش آماده کرده‌ایم. نمونه مجموعه داده در شکل ۱,۴ نشان داده شده است. برخی از ویژگی‌ها 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 ویژگی‌ها 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 گرفته‌ایم.

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	M IBRAHIM	1	GILGIT	01/01/1973	08/02/2018	08/02/2018	7110347468740	3469557182
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 GHAFOOR	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	3429459488	3429459488
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	JHANZAIB	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 ۴-۱ : نمونه مجموعه داده‌های ساختگی

۲,۴ نصب پیکربندی سخت‌افزار و نرم‌افزار

برای پیاده‌سازی از سخت‌افزار و نرم‌افزار زیر استفاده می‌شود.

۱,۲,۴ سخت‌افزار مورد نیاز

برای ساخت چارچوب از سخت‌افزار زیر استفاده می‌شود.

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

۲,۲,۴ سیستم عامل و نرم‌افزار توسعه

برای ساخت چارچوب از نرم‌افزارهای زیر استفاده می‌شود:

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

```
CREATE MASTER KEY ENCRYPTION
BY PASSWORD = 'MCS173006'

CREATE CERTIFICATE ThesisCertificate WITH SUBJECT = 'Patientdata'
GO

CREATE SYMMETRIC KEY DProtect1
WITH ALGORITHM = AES_128
ENCRYPTION BY CERTIFICATE ThesisCertificate;
GO
```

Messages

```
Command(s) completed successfully.
```

شکل ۴-۲: ایجاد کلیدها و گواهینامه ها

۳,۴ مرحله رمزگذاری داده‌ها

در این مرحله داده‌های حساس بیمار که باید روی ابرها بارگذاری شوند؛ تهیه شده و فرآیند رمزگذاری روی آن اعمال می‌شود.

مراحل رمزگذاری نمونه مرحله به مرحله در شکل ۲,۴ نشان داده شده است.

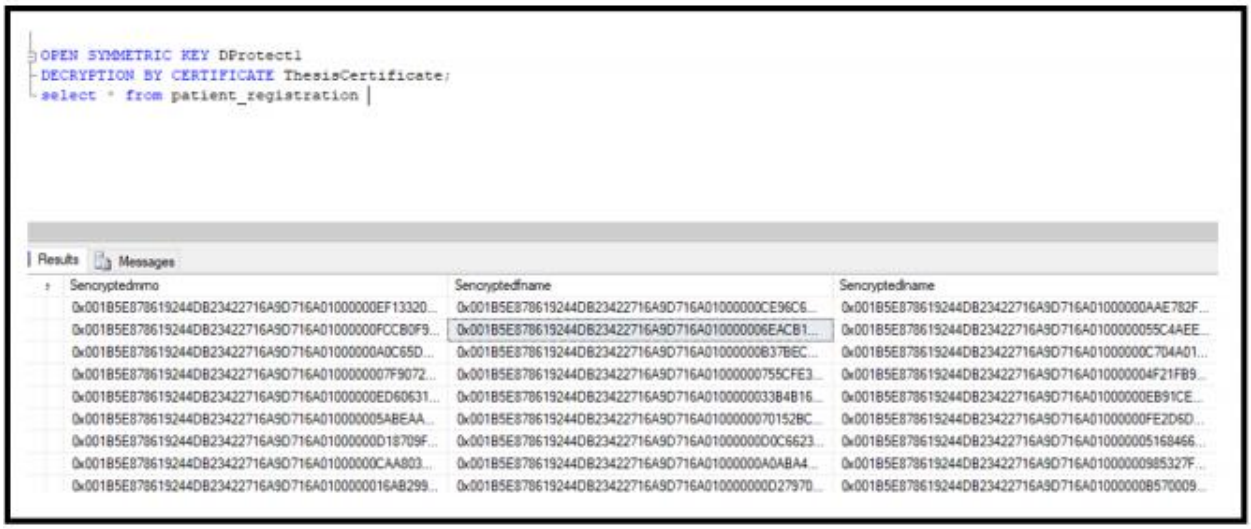
Step 1: CREATE MASTER KEY ENCRYPTION BY PASSWORD = MCS173006
Step 2: CREATE CERTIFICATE ThesisCertifificate WITH SUBJECT = 'Patientdata'
GO
Step 3: CREATE SYMMETRIC KEY DProtect1 WITH ALGORITHM = AES 128
ENCRYPTION BY CERTIFICATE ThesisCertifificate;
GO
Step 4: ALTER TABLE patient registration ADD Sencryptedmrno varbinary(MAX)NULL,
Sencryptedfname varbinary(MAX)NULL,
Sencryptedlname varbinary(MAX)NULL,

Sencryptedrlname varbinary(MAX)NULL,
Sencryptedgender varbinary(MAX)NULL,
Sencryptedaddress varbinary(MAX)NULL,
Sencrypteddob varbinary(MAX)NULL,
Sencrypteddoreg varbinary(MAX)NULL,
Sencryptednic varbinary(MAX)NULL,

Sencryptedmobile varbinary(MAX)NULL,
Sencryptedregamount varbinary(MAX)NULL,
Sencryptedconsamount varbinary(MAX)NULL,
Sencryptedtotamount varbinary(MAX)NULL,
Sencryptedrelwithrelative varbinary(MAX)NULL
go
Step 5: OPEN SYMMETRIC KEY DProtect1
DECRYPTION BY CERTIFICATE ThesisCertifificate;
Step 6: OPEN SYMMETRIC KEY DProtect1
DECRYPTION BY CERTIFICATE ThesisCertifificate;
set statistics time on
UPDATE patient registration
set Sencryptedmrno=EncryptByKey(Key GUID('DProtect1'), mrno),
Sencryptedfname =EncryptByKey(Key GUID('DProtect1'), FirstName),
Sencryptedlname=EncryptByKey(Key GUID('DProtect1'), lastname),
Sencryptedrlname =EncryptByKey(Key GUID('DProtect1'), relativename),
Sencryptedgender=EncryptByKey(Key GUID('DProtect1'), gender),
Sencryptedaddress =EncryptByKey(Key GUID('DProtect1'),address),
Sencrypteddob=EncryptByKey(Key GUID('DProtect1'), dateofbirth) ,
Sencrypteddoreg =EncryptByKey(Key GUID('DProtect1'), dateofregistration),
Sencryptednic=EncryptByKey(Key GUID('DProtect1'), nic),
Sencryptedmobile=EncryptByKey(Key GUID('DProtect1'), mobileno) ,
Sencryptedregamount=EncryptByKey(Key GUID('DProtect1'), regamount)
Sencryptedconsamount=EncryptByKey(Key GUID('DProtect1'),consultamount),

Sencryptedtotamount=EncryptByKey(Key GUID('DProtect1'), otalamount)
Sencryptedrelwithrelative =EncryptByKey(Key GUID('DProtect1'), relwithrelatiive)

مرحله هفتم: اکنون داده‌ها در جدول پایگاه‌داده با این فرمت که در شکل ۳,۴ نشان داده شده، ذخیره می‌شوند.



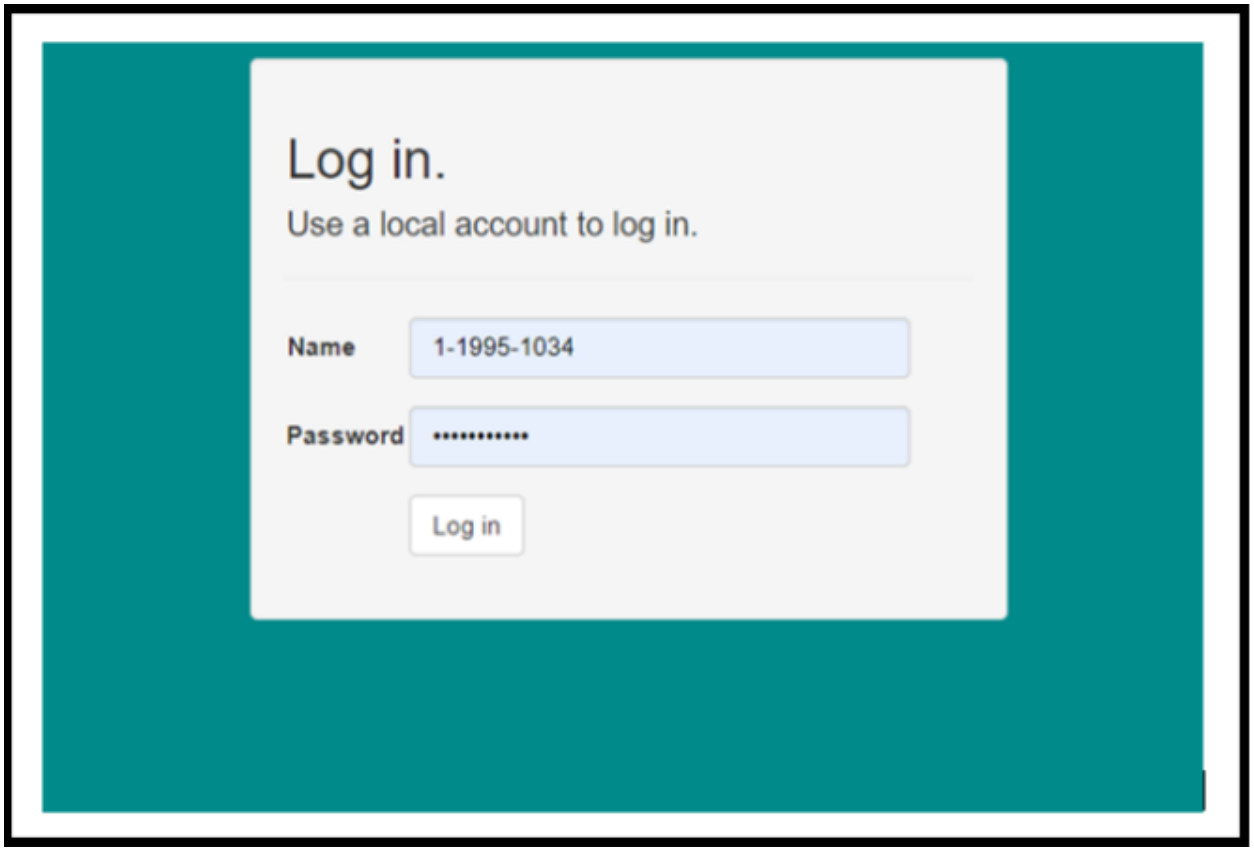
شکل ۴-۳: فرم رمزگذاری شده داده‌ها

۴,۴ مرحله رمزگشایی داده‌ها

بیمار از ***URL*** که در برگه ثبت نام چاپ شده است بازدید می‌کند.و از شماره پرونده پزشکی به عنوان نام کاربری و رمز عبور استفاده می‌کند و بر روی ورود کلیک می‌کند. سابقه بیمار در شکل ۴,۴ و شکل۵,۴ نشان داده شده است.

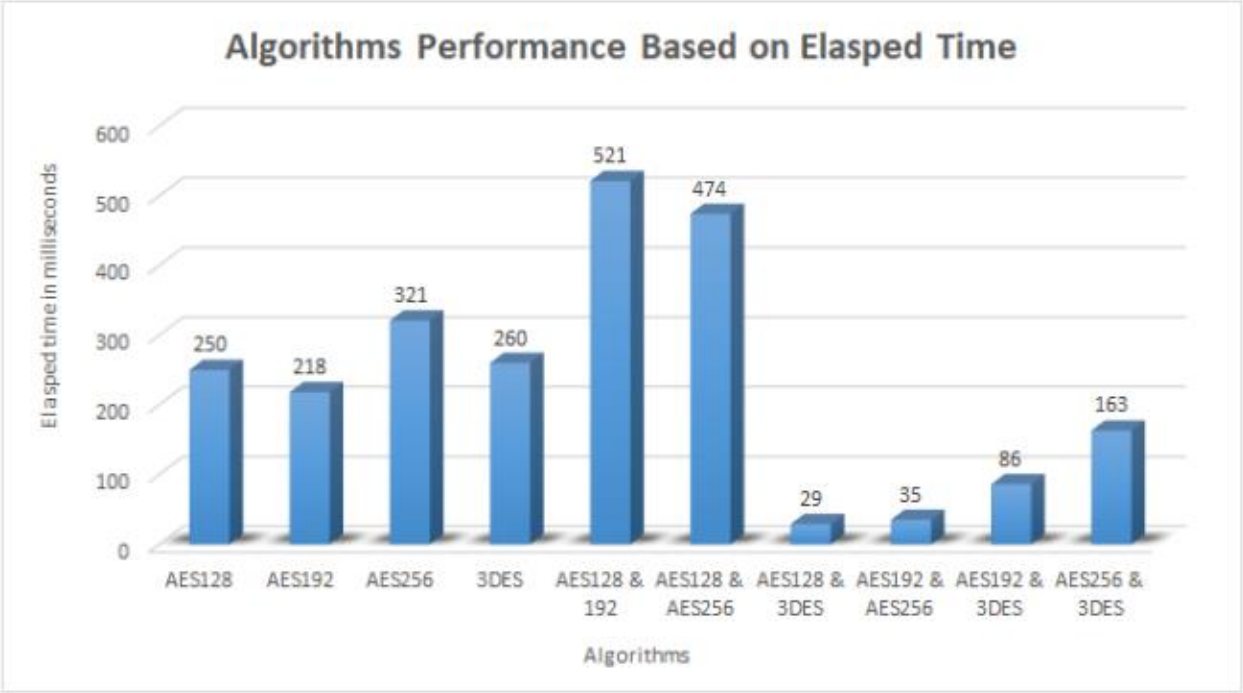
۵,۴ تحلیل نتایج

در این بخش نتایج بدست آمده با روش‌های منفرد و ترکیبی مقایسه می‌شود. نمودارهای زیر در شکل ۶,۴ و شکل ۷,۴ و شکل۸,۴؛ نتایج زمان سپری شده، زمان پردازنده و ظرفیت ذخیره‌سازی داده‌های الگوریتم‌های رمزگذاری شده مختلف را نشان می‌دهد. شکل ۷,۴ زمان سپری شده روی ۵۰۰ رکورد با الگوریتم‌های رمزگذاری منفرد نشان می‌دهد.

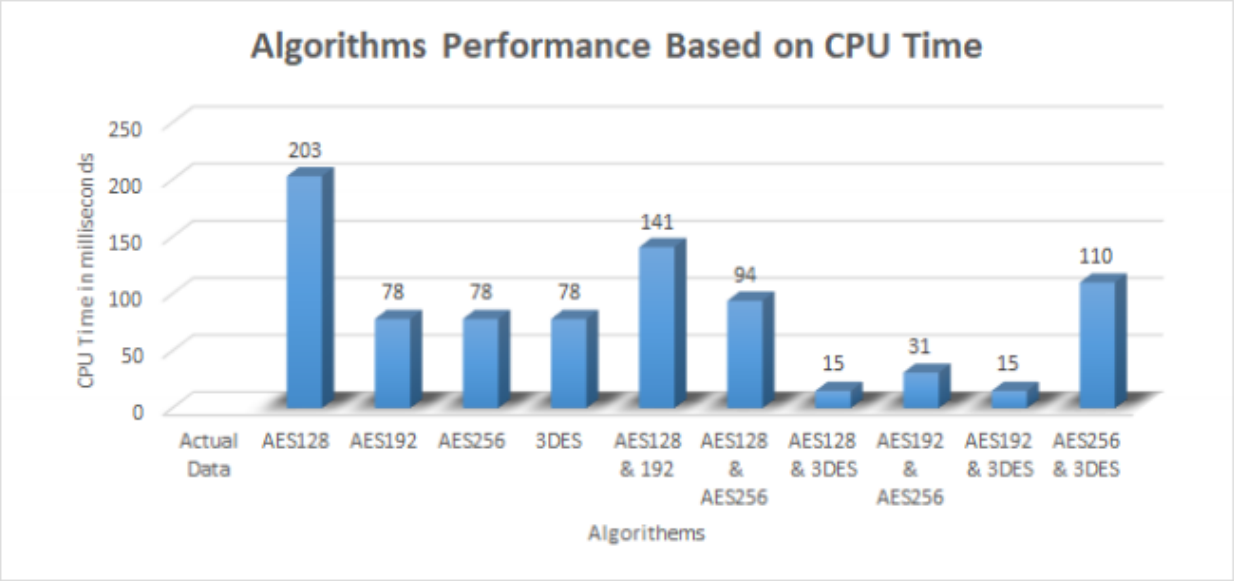


شکل ۴-۴: : صفحه ورود به سیستم برای ورود بیمار

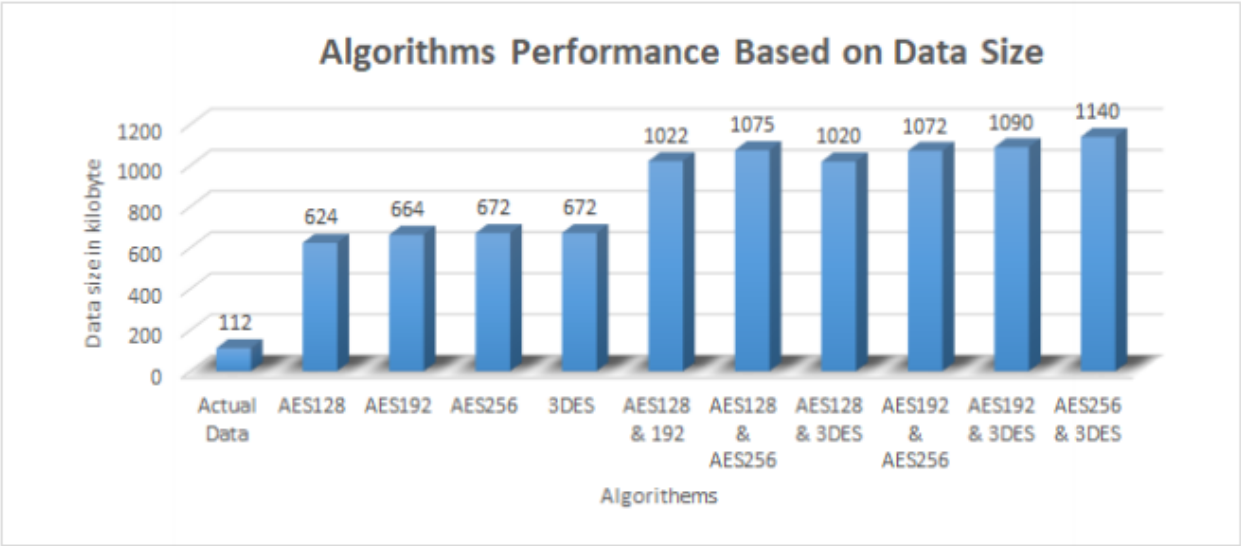
شکل ۴-۵: جزئیات پرونده پزشکی یک بیمار



شکل ۴-۶ : نمای گرافیکی زمان سپری شده الگو



*شکل ۴-۷ : نمای گرافیکی زمان **CPU** زمان الگوریتم رمزگذاری چندلایه و منفرد*



شکل ۴-۸: نمای گرافیکی اندازه جدول پایگاه داده بعد از ذخیره‌سازی

- اگر الگوریتم رمزگذاری منفرد ***AES*** با اندازه کلید ۱۲۸ بیتی اعمال شود، کل زمان سپری شده ۲۵۰ میلی‌ثانیه خواهدبود.
- اگر ***AES*** با اندازه کلید ۱۹۲ بیتی اعمال شود، کل زمان سپری شده ۲۱ میلی‌ثانیه خواهدبود.
- اگر ***AES*** با اندازه کلید ۲۱۸ بیتی اعمال شود، کل زمان سپری شده ۳۲۱ میلی‌ثانیه خواهدبود.
- اگر **۳DES** به تنهایی اعمال شود، کل زمان سپری شده ۲۶۰ میلی‌ثانیه خواهدبود.

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

- اگر ترکیبی از ***AES128*** و ۱۹۲ استفاده شود؛ زمان سپری شده ۵۲۱ میلی‌ثانیه خواهدبود.

- اگر ترکیبی از ***AES128*** و ۲۵۶ استفاده شود؛ زمان سپری شده ۴۷۴ میلی‌ثانیه خواهدبود.
- اگر ترکیبی از ***AES128*** و **۳DES** استفاده شود، زمان سپری شده ۲۹ میلی‌ثانیه خواهدبود.
- اگر ترکیبی از ***AES192*** و ***AES256*** استفاده شود، مدت زمان سپری شده ۳۵ میلی ثانیه خواهد بود.
- اگر ترکیبی از ***AES192*** و **۳DES** استفاده شود، مدت زمان سپری شده ۸۶ میلی‌ثانیه خواهدبود.
- اگر ترکیبی از ***AES256*** و **۳DES** استفاده شود، مدت زمان سپری شده ۱۶۳ میلی ثانیه خواهدبود.

شکل ۸,۴ زمان پردازنده را در میلی‌ثانیه برای ۵۰۰ رکورد با الگوریتم‌های رمزگذاری منفرد به ما ارائه می‌دهد.

- ***AES128*** زمان پردازنده ۲۰۳ میلی ثانیه را می‌گیرد.
- ***AES192*** زمان پردازنده ۷۸ میلی‌ثانیه است.
- ***AES256***، ۷۲میلی‌ثانیه طول می‌کشد.
- **۳DES**، 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 **۳DES** ، ۱۵ میلی‌ثانیه طول می‌کشد.
- ***AES256*** و **۳DES** ، ۱۱۰ میلی‌ثانیه طول می‌کشد.

اگرچه زمان پردازنده با ***AES256*** و **۳DES** به زمان ***CPU*** بیشتری نیاز دارد اما زمان سپری شده ***AES256*** و **۳DES** طرح بهتری را برای رویکردهای چندلایه ارائه می‌دهد زیرا رمزگذاری فقط بارگذاری اطلاعات را انجام می‌دهد. برای بهترین سطح محرمانگی ***AES256*** با **۳DES** خوب است.

AES256	**۳DES**	**چند لایه** ***AES128*** **& ۳DES**	**چند لایه** ***AES192*** **& ۳DES**	**چند لایه** ***AES256*** **& ۳DES**	
کم	کم	متوسط	متوسط	بالا	سطح محرمانه بودن [۵۶]
سریع	سریع	سریع	متوسط	متوسط	سرعت رمزگذاری و رمزگشایی [۵۶]
تک کلید	تک کلید	دو کلید	دو کلید	دو کلید	تعداد کلید استفاده شده[۵۶]
دشوار	دشوار	سخت	سخت	خیلی سخت	امکان حمله[۵۶]
۱۲	۴۸	۱۲	۴۸	۶۰	تعداد دورها[۵۶]

۲۵۶	۱۲۸و۱۹۲	۲۵۶	۱۲۸و۱۹۲	متفاوت	طول کلید برحسب بایت [۵۶]

*جدول ۴-۱: مقایسه الگوریتم‌های منفرد و ترکیبی **۳DES** و **AES256***

در جدول ۱,۴ مقایسه الگوریتم‌های مختلف را با یک لایه و چند لایه انجام داده‌ایم. سطح محرمانگی به سه حالت تقسیم می شود:

- کم
- متوسط
- بالا

این دقیقا 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. ردیف دوم جدول ۱,۴ در مورد 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. ردیف سوم جدول ۱,۴ نشان‌دهنده ترکیب کلید 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.

۶,۴ نتیجه‌گیری

در این فصل این نکات اصلی را شرح داده ایم:

- چگونه مجموعه داده‌ها را برای آزمایش‌ها گرفته ایم ؟
- رمزگشایی و رمزگذاری بر روی داده چگونه انجام می‌شود؟
- چگونه آزمایش روی داده انجام می‌شود؟
- تجزیه و تحلیل نتیجه و نتایج آزمایش مورد بحث قرار گرفته است.

فصل ۵

۵. نتیجه‌گیری و آینده کار

۱,۵ نتیجه‌گیری

حفاظت از اطلاعات حساس بیمار به دلیل امنیت مسئله چالش برانگیزی است. تکنیک‌های معرفی شده را در چارچوب ادبیات بررسی کردیم. یافتن تکنیک جدید نیز بسیار چالش برانگیز است. می‌دانیم که تکنیک‌های رمزگذاری چند لایه نیز 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 می‌گیرد. در ادامه مزایای استفاده از تکنیک‌های پیشنهادی آمده است:

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

۲,۵ آینده کار

اهداف زیر برای نوآوری‌های آینده وجود دارد:

- انتخاب الگوریتم رمزگذاری به صورت تصادفی
- الگوریتم استانداردهای بیشتری اضافه شود.
- افزایش سرعت رمزگذاری
- پیاده سازی الگوریتم‌های چند لایه روی داده‌های مبتنی بر تصویر

فهرست منابع

[۱] Son, Ha Xuan, Minh Hoang Nguyen, and Hong Khanh Vo., “Toward an privacy protection based on access control model in hybrid cloud for healthcare systems.“, ۱۰th International Conference on EUropean Transnational Education (ICEUTE ۲۰۱۹), ۲۰۱۹.
[۲] S. M and Altowaijri, “An architecture to improve the security of cloud computing in the healthcare sector,” in Smart Infrastructure and Applications. Springer, pp.۲٤۹–۲٦٦،۲۰۲۰.
[۳] “https://tutorialspoint.com/cloud-computing/cloud-computing-overview.htm/“
[٤] “https://timesofcloud.com/cloud-tutorial/characteristics-of-cloud-computing-as-per-nist/“

[٥] F. Gao, S. Thiebes, and A. Sunyaev, “Rethinking the meaning of cloud com-puting for health care: A taxonomic perspective and future research direc-tions,”Journal of medical Internet research, vol. ۲۰, no. ۷, p. e۱۰۰٤۱, ۲۰۱۸.

[٦] Z. Yan, R. H. Deng, and V. Varadharajan, “Cryptography and data security in cloud computing,” ۲۰۱۷.
[۷] T. M. Damico, “A brief history of cryptography,” Inquiries Journal, vol. ۱, no. ۱۱, ۲۰۰۹.
[۸] “https://www.garykessler.net/library/crypto.html/ “

[۹] Babatunde, A. O., A. J. Taiwo, and E. G. Dada., “Information Security in Health Care Centre Using ryptography and Steganography.,” arXiv preprint arXiv:۱۸۰۳,۰٥٥۹۳،۲۰۱۸.
[۱۰] J. K. Oherrin, N. Fost, and K. A. Kudsk, “Health insurance portability accountability act (hipaa) regulations: effffect on medical record research,” Annals of surgery, vol. ۲۳۹, no. ٦, p. ۷۷۲, ۲۰۰٤.
[۱۱] 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. ۱٦۹۱–۱۷۰۳, ۲۰۱۱.
[۱۲] K. Sudheep and S. Joseph, “Review on securing medical big data in healthcare cloud,” in ۲۰۱۹ ٥th nternational Conference on Advanced Computing & Communication Systems (ICACCS). IEEE, ۲۰۱۹, pp. ۲۱۲–۲۱٥.
[۱۳] 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. ۱۰۲۱–۱۰۳٥, ۲۰۱۹.
[۱٤] 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. ٥, p. ۹۷۱, ۲۰۱۳.
[۱٥] E. Shanmugapriya and R. Kavitha, “Medical big data analysis: preserving security and privacy with hybrid loud technology,” Soft Computing, vol. ۲۳, no. ۸, pp. ۲٥۸٥–۲٥۹٦, ۲۰۱۹.
[۱٦] F. Shahbodin, A. Azni, T. Ali, and C. K. N. C. K. Mohd, “Lightweight cryptography techniques for mhealth cybersecurity,” in Proceedings of the ۲۰۱۹ Asia Pacifific Information Technology Conference, ۲۰۱۹, pp. ٤٤–٥۰.
[۱۷] D. He, N. Kumar, J.-H. Lee, and R. S. Sherratt, “Enhanced three-factor security protocol for consumer usb ass storage devices,” IEEE Transactions on Consumer Electronics, vol. ٦۰, no. ۱, pp. ۳۰–۳۷, ۲۰۱٤.
[۱۸] K. Renuka, S. Kumari, and X. Li, “Design of a secure three-factor authentication scheme for smart healthcare,” Journal of medical systems, vol. ٤۳, no. ٥, p. ۱۳۳, ۲۰۱۹.
[۱۹] 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. ۲٦۷–۳۰۹.
[۲۰] L. Zhou, V. Varadharajan, and K. Gopinath, “A secure role-based cloud storage system for encrypted patient-centric health records,” The Computer Journal, vol. ٥۹, no. ۱۱, pp. ۱٥۹۳–۱٦۱۱, ۲۰۱٦.
[۲۱] 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. ۱۸٥–۱۹٦, ۲۰۱۹.
[۲۲] K. J. Modi and N. Kapadia, “Securing healthcare information over cloud using hybrid approach,” in Progress in advanced computing and intelligent engineering. Springer, ۲۰۱۹, pp. ٦۳–۷٤.
[۲۳] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and B. Balusamy, “Securing data in internet of things (iot) using cryptography and steganography techniques,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. ٥۰, no. ۱, pp. ۷۳–۸۰, ۲۰۱۹.
[۲٤] H. Jin, Y. Luo, P. Li, and J. Mathew, “A review of secure and privacypreserving medical data sharing,” IEEE Access, vol. ۷, pp. ٦۱ ٦٥٦–٦۱ ٦٦۹, ۲۰۱۹.
[۲٥] Y. S. Lee, E. Alasaarela, and H. J. Lee, “An effiffiffficient encryption scheme using elliptic curve cryptography (ecc) with symmetric algorithm for healthcare system,” International journal of security and its applications, vol. ۸, no. ۳, pp. ٦۳–۷۰, ۲۰۱٤.

[۲٦] P. D. Nayana Banjan, “Medical data security using combination of cryptography and steganography with aes-lsb algorithm,” International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), Tech. Rep.
[۲۷] G. Garkoti, S. K. Peddoju, and R. Balasubramanian, “Detection of insider attacks in cloud based e-healthcare environment,” in ۲۰۱٤ International Conference on Information Technology. IEEE, ۲۰۱٤, pp. ۱۹٥–۲۰۰.
[۲۸] Y. M. Essa, E. E.-D. Hemdan, A. El-Mahalawy, G. Attiya, and A. El-Sayed, “Ifhds: Intelligent framework for securing healthcare bigdata,” Journal of medical systems, vol. ٤۳, no. ٥, p. ۱۲٤, ۲۰۱۹.
[۲۹] A. M. Elmisery and H. Fu, “Privacy preserving distributed learning clustering of healthcare data using cryptography protocols,” in ۲۰۱۰ IEEE ۳٤th Annual Computer Software and Applications Conference Workshops. IEEE, ۲۰۱۰, pp. ۱٤۰–۱٤٥.
[۳۰] A. M. Badr, Y. Zhang, A. Umar, and H. Gulfam, “Dual authenticationbased encryption with a delegation system to protect medical data in cloud computing,” Electronics, vol. ۸, no. ۲, p. ۱۷۱, ۲۰۱۹.
[۳۱] Jammu, Aashmeen, and Harjinder Singh, “Improved AES for Data Security in E-Health IEEE,” International Journal of Advanced Research in Computer Science ۸,٥ ۲۰۱۷.
[۳۲] K.-L. Tsai, Y.-L. Huang, F.-Y. Leu, I. You, Y.-L. Huang, and C.-H. Tsai, “Aes-۱۲۸ based secure low power communication for lorawan iot environments,” IEEE Access, vol. ٦, pp. ٤٥ ۳۲٥–٤٥ ۳۳٤, ۲۰۱۸.
[۳۳] A. Michalas and N. Weingarten, “Healthshare: Using attribute-based encryption for secure data sharing between multiple clouds,” in ۲۰۱۷ IEEE ۳۰th International Symposium on Computer-Based Medical Systems (CBMS). IEEE, ۲۰۱۷, pp. ۸۱۱–۸۱٥.
[۳٤] A. Michalas, N. Paladi, and C. Gehrmann, “Security aspects of e-health systems migration to the cloud,” in ۰۱٤ IEEE ۱٦th International Conference on e-Health Networking, Applications and Services (Healthcom). IEEE, ۲۰۱٤, pp. ۲۱۲–۲۱۸.
[۳٥] H. Asri, H. Mousannif, H. Al Moatassime, and T. Noel, “Big data in healthcare: Challenges and opportunities,” in ۲۰۱٥ International Conference on Cloud Technologies and Applications (CloudTech). IEEE, ۲۰۱٥, pp. ۱–۷.
[۳٦] J. Oltsik, “Vormetric/ESG Insider Threat Report: Profifile on HealthCare, ۲۰۱٤, pp. ۱–۷. [۳۷] V Mahalakshmi, S Satheeshkumar and Dr. S Sivakumar, “Performance of steganographic methods in medical imaging, International Journal of Computational and Applied Mathematics Vol. ۱۲, no. ۱, pp ٥٤۹-٥٥٦،۲۰۱۷.
[۳۸] PratikshaSethi and V Kapoor, “A Secured System for Information Hiding in Image Steganography using enetic algorithm and Cryptography, International Journal of Computer Applications, Vol. ۱٤٤, No. ۹Et.al.,۲۰۱٦.
[۳۹] “Steganography and cryptography approaches combined using medical digital images,” International Journal of Engineering Research & Technology (IJERT), vol. ٤, ۲۰۱٥.
[٤۰] J. L. Pan, S. P. Li and D. Y. Zhang, A Study of two algorithms based on feistel cipher in wireless medical ensor networks (in Chinese), Chinese J. Sens. Actuators, vol. ۲۳, pp. ۱۰۳۰-۱۰۳٦،۲۰۱۰
[٤۱] C. Jiang, B. Li, and H. Xu, “An effiffifficient scheme for user authentication in wireless sensor networks,” IEEE, pp. ٤۳۸–٤٤۲, ۲۰۰۷.
[٤۲] L. Chen and D. B. Hoang, “Novel data protection model in healthcare cloud,” IEEE, pp. ٥٥۰–٥٥٥, ۲۰۱۱.
[٤۳] S. Narayan and M. Gagn, and R. Safavi-Naini, Privacy preserving EHR system using attribute-based infrastructure,in Proc. ACM Workshop Cloud Comput. Secur. Workshop. New York, NY, USA: ACM, pp. ٤۷٥۲.,۲۰۱۰
[٤٤] R. Guo, H. Shi, Q. Zhao, and D. Zheng, “Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems,” pp. ۱۱ ٦۷٦–۱۱ ٦۸٦, ۲۰۱۸.
[٤٥] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, Scalable and secure sharing of personal health records in cloud computing using attributebased encryption, IEEE Trans. Parallel Distrib. Syst., vol. ۲٤, no. ۱, pp. ۱۳۱۱٤۳, Jan.۲۰۱۳.
[٤٦] H. Kaur, H. P. S. Gill, and D. Sarmah, “Multiphase and multiple encryption,” IEEE, pp. ۱–۸.
[٤۷] Kumar, Vishal, et al. ”Multiple Encryption using ECC and its Time Complexity Analysis.” International Journal of Computer Engineering In Research Trends ۳,۱۱, pp. ٥٦۸-٥۷۲, ۲۰۱٦.
[٤۸] Tebaa, Maha, and Said El Hajji., ”Secure cloud computing through homo morphic encryption.” empharXiv preprint arXiv:۱٤۰۹,۰۸۲۹, (۲۰۱٤).
[٤۹] Sarhan, Akram, and LeszekLilien, ”An Approach to Identity Management in Clouds without Trusted Third Parties.” empharXiv preprint arXiv:۱۹۰٤,۰۰۸۸۰, (۲۰۱۹).
[٥۰] R. Arora, A. Parashar, and C. C. I. Transforming, “Secure user data in cloud computing using encryption algorithms,” pp. ۱۹۲۲–۱۹۲٦, ۲۰۱۳.
[٥۱] Padhy, Rabi Prasad, ManasRanjanPatra, and Suresh Chandra Satapathy, ”Cloud computing: security issues and research challenges.”, ”International Journal of Computer Science and Information Technology and Security (IJC SITS) ۱,۲”, : pp. ۱۳٦-۱٤٦،۲۰۱۱.

[٥٢] M. S. Abolghasemi, M. M. Sefifidab, and R. E. Atani, “Using location based encryption to improve the security of data access in cloud computing,” IEEE, pp. ٢٦١–٢٦٥, ٢٠١٣.
[٥٣] Albugmi, Ahmed, et al., ”Data security in cloud computing.”, ٢٠١٦ Fifth International Conference on Future Generation Communication Technologies (FGCT). IEEE, ٢٠١٦.
[٥٤] V. Gampala, S. Inuganti, and S. Muppidi, “Data security in cloud computing with elliptic curve cryptography,” pp. ١٣٨–١٤١, ٢٠١٢.
[٥٥] Ahamed, Farhad, SeyedShahrestani, and AthulaGinige., ”Cloud computing: security and reliability issues.”, Communications of the IBIMA ٢٠١٣, ٢٠١٣.
[٥٦] Babatunde, AO and Taiwo, AJ and Dada, EG, ”Information Security in Health Care Centre Using Cryptography and Steganography”, arXiv preprint arXiv:١٨٠٣,٠٥٥٩٣, ٢٠١.