*دانشگاه علوم و فناوری اسلام آباد*

**

*یک مدل رمزگذاری چند لایه برای محافظت از داده های مراقبت هاي بهداشتی در*

*محیط ابري*

*توسط*

*حسن عباس شاه*

*پایان نامه ارائه شده درجه کارشناسی ارشد*

*در*

*دانشکده محاسبات*

*گروه علوم کامپیوتر*

*سال 2020*

*حق كپي رايت2020© براي 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 راهنماي خود برای اعتقاد راسخ و اطمینان‌شان براي رسيدن به اين نقطه عطف موفقيت شده تشکر کنم.*

*گواهی تصویب*

*يك مدل رمزگذاری چند لایه برای محافظت از داده‌هاي مراقبت هاي بهداشتي در محیط ابری*

*توسط*

*حسن عباس شاه*

*(MCS173006)*

*کمیته بررسی پایان نامه*

|  |  |  |  |
| --- | --- | --- | --- |
| *شماره* | *آزمون‌گر* | *نام* | *سازمان* |
| *A* | *آزمون‌گر خارجي* | *دکتر منیر احمد* | *BIIT راولپندی* |
| *B* | *آزمون‌گر داخلي* | *دکتر امیر قیوم* | *CUST اسلام آباد* |
| *C* | *استاد راهنما* | *دکتر قمر محمود* | *CUST اسلام آباد* |

*دکتر قمر محمود*

*استاد راهنمای پایان‌نامه*

*مه 2020*

|  |  |
| --- | --- |
| *دكتر نایر مسعود*  *سرگروه*  *دپارتمان علوم كامپيوتر*  *مه 2020* | *دكتر محمود عبدالقادر*  *رئيس*  *دانشكده محاسبات*  *مه 2020* |

# *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 مراقبت‌هاي بهداشتی در محیط ابري" 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 میكنم كه كار‌هاي تحقيقاتي ارائه شده در اين پايان‌نامه با عنوان " یک مدل رمزگذاری چند لایه‌ برای محافظت از داده های مراقبت‌هاي بهداشتی در محیط ابري" فقط کار تحقیقاتی من است و هیچ مشارکت قابل توجهی از شخص دیگری ندارد. مشاركت/ كمك هر كجا كه گرفته شود؛ تأیید شده و پایان نامه كامل توسط من نوشته شده است.*

*من سیاست HEC و دانشگاه علم و صنعت پایتخت را در مورد دزدی ادبی درک مي‌کنم. بنابراین، به عنوان نویسنده پایان‌نامه عنوان شده فوق اظهار مي‌دارم 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 بركناري/ 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 دزدي ادبي 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*

*اكنون 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 اهميت دارد. ویژگی‌های اصلی رایانش ابری؛ شبکه گسترده، منابع مشترک، کشش سریع و پرداخت به ازای هر استفاده مي‌باشد. 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: 1- اطلاعات سلامت محافظت شده / حساس 2- اطلاعات عمومی. اطلاعات محافظت شده(شماره تلفن، ای تی ام، شماره امنیتی و غیره) در مقایسه با اطلاعات عمومی به محرمانگي بیشتری نیاز دارد. بنابراین برخی از اطلاعات بهداشتی محافظت شده بدون اجتماع بیمار (نام عمومي بيماري، علائم) برای آزمایش های تجربی بسیار مفید خواهد بود. وقتی داده‌ها در فضای ابری ذخیره می‌شوند، به‌وسيله 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 500 پرونده ساختگی بیمار برای استفاده از روش‌های پیشنهادی استفاده می‌شود. اين آزمایش برای بررسی محرمانگي روش‌های پیشنهادی انجام شده است. اين 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](#_Toc77779752)

[*تعهد سرقت ادبی* v](#_Toc77779753)

[*سپاسگزای‌ها* vi](#_Toc77779754)

[*چکیده* vii](#_Toc77779755)

[*ليست اشكال* xi](#_Toc77779756)

[*ليست جداول* xii](#_Toc77779757)

[*مخفف ها* xiii](#_Toc77779758)

[1. مقدمه 1](#_Toc77779759)

[*1.1 رایانش ابری* 2](#_Toc77779760)

[*2.1 تاریخچه مختصري از رایانش ابري* 3](#_Toc77779761)

[*3.1 ویژگی‌های رایانش ابری برای بخش مراقبت‌های بهداشتی* 3](#_Toc77779762)

[*4.1  مدل سرويس ابري برای خدمات بهداشتی الکترونیکی* 3](#_Toc77779763)

[*1.4.1  نرم افزار به عنوان سرویس (SaaS)* 4](#_Toc77779764)

[*2.4.1 پلت فرم به عنوان یک سرویس (PaaS)* 4](#_Toc77779765)

[*3.4.1 زیرساخت به عنوان سرویس (IaaS)* 4](#_Toc77779766)

[*5.1  مروری بر رمزنگاری* 4](#_Toc77779767)

[*1.5.1  چند کلمه درباره تاریخ رمزنگاری* 5](#_Toc77779768)

[*2.5.1  انقلاب در زمینه رمزنگاری* 5](#_Toc77779769)

[*3.5.1  انواع طرح‌های رمزنگاری* 6](#_Toc77779770)

[4.5.1 سرویس امنیتی برای رمزنگاری برای مراقبت های بهداشتی 7](#_Toc77779771)

[*6.1 کار الگوریتم‌های مورد استفاده در طرح پیشنهادی* 8](#_Toc77779772)

[*7.1  قانون HIPAA و GDPR چیست؟* 13](#_Toc77779773)

[*8.1  عامل انگیزه* 15](#_Toc77779774)

[*9.1  بیان مسئله* 15](#_Toc77779775)

[*10.1  سوالات تحقیق* 15](#_Toc77779776)

[*11.1  روش تحقیق* 15](#_Toc77779777)

[*12.1 هدف مطالعه* 16](#_Toc77779778)

[*13.1 اهمیت پایان‌نامه* 16](#_Toc77779779)

[*14.1  نتیجه‌گیری* 17](#_Toc77779780)

[*15.1 سازمان پایان‌نامه* 17](#_Toc77779781)

[*2.* *بررسی ادبیات* 18](#_Toc77779782)

[*2.1  کار مرتبط* 18](#_Toc77779783)

[2.2 تجزیه و تحلیل بررسی ادبیات 22](#_Toc77779784)

[*3.2 دست‌آوردهای تجزیه و تحلیل* 25](#_Toc77779785)

[*4.2  خلاصه* 25](#_Toc77779786)

[3. راه‌اندازی آزمایشی طرح پیشنهادی 26](#_Toc77779787)

[*1.3  انتخاب مجموعه داده‌ها* 26](#_Toc77779788)

[*2.3  لایه رمزگذاری PHI Attribut ES* 26](#_Toc77779789)

[*3.3  معماری روش* 26](#_Toc77779790)

[*4.3  فرآیند رمزگذاری و رمزگشایی در RDBMS ( (Microsoft SQL Server)* 28](#_Toc77779791)

[*1.4.3  چگونه رمزگذاری در SQL Server انجام می‌شود؟* 28](#_Toc77779792)

[*5.3  نتیجه گیری* 29](#_Toc77779793)

[*4.* *تجزیه و تحلیل آزمايشي طرح پیشنهادی* 31](#_Toc77779794)

[*1.4  انتخاب مجموعه داده* 31](#_Toc77779795)

[*2.4  نصب پیکربندی سخت‌افزار و نرم‌افزار* 31](#_Toc77779796)

[*1.2.4  سخت‌افزار مورد نياز* 31](#_Toc77779797)

[*2.2.4  سیستم عامل و نرم‌افزار توسعه* 31](#_Toc77779798)

[*3.4  مرحله رمزگذاری داده‌ها* 32](#_Toc77779799)

[*4.4 مرحله رمزگشایی داده‌ها* 34](#_Toc77779800)

[*5.4 تحلیل نتایج* 34](#_Toc77779801)

[*6.4  نتیجه‌گیری* 38](#_Toc77779802)

[*5.* *نتیجه‌گیری و آینده کار* 39](#_Toc77779803)

[*1.5  نتیجه‌گیری* 39](#_Toc77779804)

[*2.5 آینده کار* 39](#_Toc77779805)

[فهرست منابع 40](#_Toc77779806)

# *ليست اشكال*

[شکل ‏1‑1: رایانش ابری 2](#_Toc77779807)

[شکل ‏1‑2: رمزنگاری استگانوگرافی  4](#_Toc77779808)

[شکل ‏1‑3: رمزگذاری کلید متقارن 6](#_Toc77779809)

[شکل ‏1‑4: رمزگذاری نامتقارن کلید 7](#_Toc77779810)

[شکل ‏1‑5: روش رمزگذاری چند لایه 8](#_Toc77779811)

[شکل ‏1‑6: جایگزینی اولیه 9](#_Toc77779812)

[شکل ‏1‑7: تابع Round 10](#_Toc77779813)

[شکل ‏1‑8: گسترش جعبه جایگزینی 10](#_Toc77779814)

[شکل ‏1‑9: تولید کلید 11](#_Toc77779815)

[شکل ‏1‑10: نمودار معماری 3DES 12](#_Toc77779816)

[شکل ‏1‑11: معماري الگوريتم AES 14](#_Toc77779817)

[شکل ‏1‑12: نمودار روش تحقیق 16](#_Toc77779818)

[شکل ‏3‑1: تکنیک محافظت از چند لایه 26](#_Toc77779819)

[شکل ‏3‑2: نمودار معماری روش‌شناسی 27](#_Toc77779820)

[شکل ‏3‑3: فیش ورود به سیستم برای بیمار 27](#_Toc77779821)

[شکل ‏3‑4: فرآیند رمزگذاری کلی 29](#_Toc77779822)

[شکل ‏4‑1: نمونه مجموعه داده‌های ساختگی 31](#_Toc77779823)

[شکل ‏4‑2: ایجاد کلیدها و گواهینامه ها 32](#_Toc77779824)

[شکل ‏4‑3: فرم رمزگذاری شده داده‌ها 33](#_Toc77779825)

[شکل ‏4‑4: : صفحه ورود به سیستم برای ورود بیمار 34](#_Toc77779826)

[شکل ‏4‑5: جزئیات پرونده پزشکی یک بیمار 35](#_Toc77779827)

[شکل ‏4‑6 : نمای گرافیکی زمان سپری شده الگو 35](#_Toc77779828)

[شکل ‏4‑7 : نمای گرافیکی زمان CPU زمان الگوریتم رمزگذاری چندلایه و منفرد 36](#_Toc77779829)

[شکل ‏4‑8: نمای گرافیکی اندازه جدول پایگاه داده بعد از ذخیره‌سازی 36](#_Toc77779830)

# *ليست جداول*

[جدول ‏1‑1: مقایسه بین رمزنگاری کلاسیک و مدرن 5](#_Toc77779885)

[جدول ‏1‑2: اهمیت پایا‌ن نامه 17](#_Toc77779886)

[جدول ‏2‑1: مرور آنالیز ادبیات 24](#_Toc77779887)

[جدول ‏4‑1: مفایسه الگوریتم‌های منفرد و ترکیبی 3DES و AES256 38](#_Toc77779888)

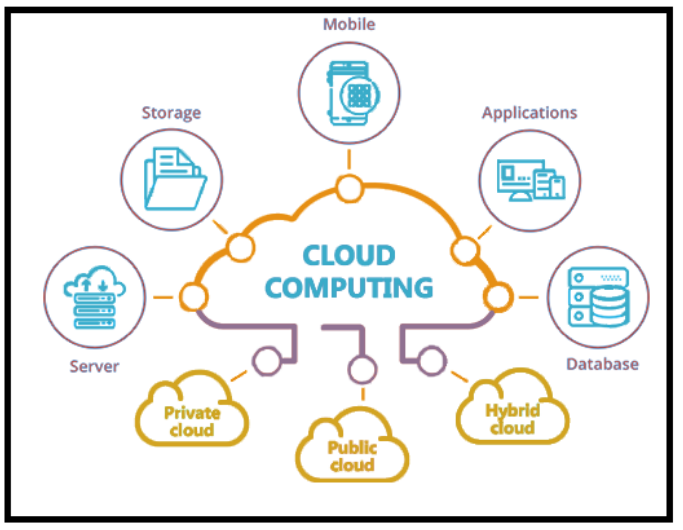
# *مخفف ها*

|  |  |
| --- | --- |
| *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 1*

# 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[* [*1*](#ش1) *]. 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 [*[*2*](#ش2)*] 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 ‏1‑1: رایانش ابری[[1]](#footnote-1)

## *1.1 رایانش ابری*

*رایانش ابری [*[*3*](#ش3)*] سرويس محاسباتی مورد تقاضا است. به شكل* [*1.1*](#شكل1و1) *نگاه کنيد. 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 مکان‌هايی از راه دور ذخیره و دسترسی یابد. اصطلاح عمومی رایانش ابری مراکز داده‌اي هستند كه 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.*

## *2.1 تاریخچه مختصري از رایانش ابري*

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

* *در سال 2006 آمازون شروع به فعالیت خود در زیر شاخه‌ای به نام خدمات وب آمازون کرد.*
* *گوگل نسخه آزمایشی Google App Engine را در آوریل 2008 منتشر کرد. در همان سال ناسا OpenNebula را نیز معرفی کرد. این اولین پروژه منبع آزاد بود که برای خصوصیات ابرهای ترکیبی به کار گرفته شد.*
* *در سال 2010 مایکروسافت Azure توسط مایکروسافت منتشر شد.*
* *در سال 2012، موتور محاسبه Google قبل از اینکه در دسامبر 2013 در دسترس عمومی قرار بگیرد، در حالت پیش‌نمایش منتشر شد.*

## *3.1 ویژگی‌های رایانش ابری برای بخش مراقبت‌های بهداشتی*

*خدمات محاسبات ابری برای بخش بهداشت و درمان به دلايل زير 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 ذخیره‌سازي و استفاده از داده‌های بیمار انجام می‌شود.*
* *هيچ 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 (‌موسسه بين‌المللي استانداردها و تكنولوژي) پنج مزیت رایانش ابری را به شرح زير بيان مي‌كند:*

* *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.*
* *هزينه خدمات اندازه‌گیری مانند استفاده از اینترنت یا خدمات اتومبیل است.[[2]](#footnote-2)*

## *4.1  مدل سرويس ابري برای خدمات بهداشتی الکترونیکی*

*رایانش ابری به دلیل زیرساخت‌هايش، 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 [*[*5*](#ش5)*].*

* *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.*

### *1.4.1  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.*

### *2.4.1 پلت فرم به عنوان یک سرویس (PaaS)*

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

### *3.4.1 زیرساخت به عنوان سرویس (IaaS)*

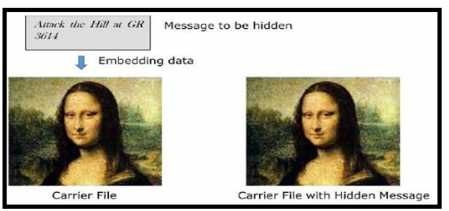
*همان‌طور که از نام آن پیداست، هر سازمان بهداشتی می‌تواند سخت‌افزار کامل را خریداری کرده و نرم‌افزار و داده‌های خود را در فضای ابری نگه دارد.*

*چالش‌هاي 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 محرمانگي و یکپارچگی داده ها از بین می‌رود.*
* *داده‌ها در خارج از قرارداد قرار دارند.*
* *سخت‌افزار بین بيماران مختلف به اشتراک گذاشته می‌شود و حمله‌کننده‌ای ممكن است داده‌ها را به خطر بيندازد.*

## *5.1  مروری بر رمزنگاری*

*به طور کلی اصطلاح رمزنگاری [*[*6*](#ش6)*] 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 محرمانگي و یکپارچگی مربوط به بیمار را بهبود می‌بخشد. به طور کلی رمزنگاری از تکنیک‌های مدل سازی ریاضی [*[*7*](#ش7)*] استفاده می‌کند. این تکنیک‌ها براساس رمزگذاری و رمزگشایی داده‌ها با استفاده از کلیدها است.*

**

شکل ‏1‑2: رمزنگاری استگانوگرافی  [[3]](#footnote-3)

### *1.5.1  چند کلمه درباره تاریخ رمزنگاری*

*رمزنگاری رابطه نزدیک با تاریخچه نوشتن متن‌ دارد.  حدود 4000 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 500 تا 600 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* [*1.2*](#شکل1و2) *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.*

### *2.5.1  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.*

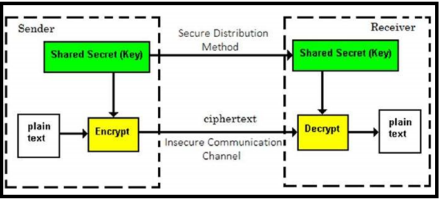
* *تکنیک‌های کدگذاری vigenere در این عصر معرفی شده است.*
* *اما در قرن نوزدهم رمزنگاری از رویکردهای موقت به تکنیک های هنری مدرن‌تر تغییر یافته است.*
* *در قرن 20 ماشین روتر انیگما معرفی شد.*
* *اما پس از جنگ جهانی دوم، روش‌های مدرن رمزنگاری معرفی شده است که برای رشته‌های علوم رایانه، مانند اکسیژن است.*

*مقایسه مختصری بین رمزنگاری کلاسیک و مدرن در جدول*[*1.1*](#جدول1و1) *نشان داده شده است.*

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

جدول ‏1‑1: 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 جاي بحث در تکنیک‌های موجود به خوبي تحقیق در مورد تکنیک‌های جدید وجود دارد.*

**

شکل ‏1‑3: رمزگذاری کلید متقارن [[4]](#footnote-4)

### *3.5.1  انواع طرح‌های رمزنگاری*

*دو نوع رمزگذاری عمومی در سیستم‌های رمزگذاری استفاده می‌شود [*[*6*](#ش6)*]:*

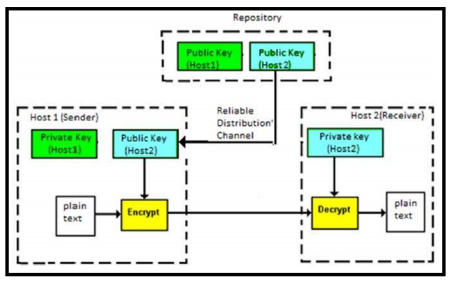
* *رمزگذاری متقارن*
* *رمزگذاری نامتقارن*

#### 1.3.5.1 رمزگذاری کلید متقارن

*در این نوع رمزگذاری فقط یک کلید برای رمزگذاری و رمزگشایی استفاده می‌شود. شکل*[*1و3*](#شکل1و3) *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.*

**

شکل ‏1‑4: رمزگذاری نامتقارن کلید[[5]](#footnote-5)

#### 2.3.5.1 رمزگذاری نامتقارن

*اين مورد هم به عنوان رمزنگاری کلید عمومی شناخته می‌شود. كه شامل دو کلید برای رمزگذاری و رمزگشایی است به شکل* [*4.1*](#شکل1و4) *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.*

### 4.5.1 سرویس امنیتی برای رمزنگاری برای مراقبت های بهداشتی

*ویژگی‌های زیر را می‌توان از رمزنگاری مربوط به داده‌های بیمار بدست آورد [*[*9*](#ش9)*].*

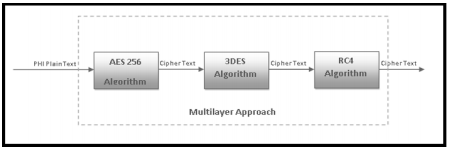
#### 1.4.5.1  محرمانه بودن

*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 می توان به سطحی از محرمانگی دست یافت.*

#### 2.4.5.1 جامعیت

*جامعیت با اصلاح داده‌ها سروکار دارد. این سرویس، داده‌های بیمار را تأیید می‌کند و تضمین میكند توسط هیچ شخص غیر مجاز، آگاهانه یا ناآگاهانه داده‌ها اصلاح نمي‌شوند. همچنین از عدم تغییر داده‌ها پس از ایجاد آن اطمینان حاصل می‌کند. جامعيت 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 ‏1‑5: روش رمزگذاری چند لایه

#### 3.4.5.1  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.*

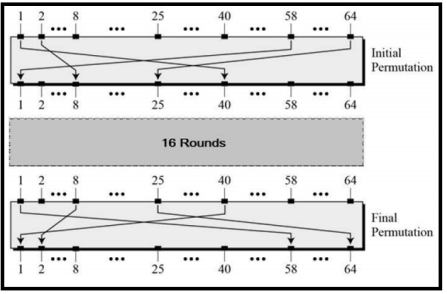
*احراز هویت پیام: این اطلاعات بدون توصیف مسیر یا سیستمی که این اطلاعات را ارسال کرده است، اطلاعات مربوط به مبدع پیام را ارائه می‌دهد.*

#### 4.4.5.1  رمزگذاری چند لایه

*به شکل* [*5.1*](#شکل1و5) *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.*

## *6.1 کار الگوریتم‌های مورد استفاده در طرح پیشنهادی*

*استاندارد رمزگذاری داده‌ها(DES) یک الگوریتم متقارن است که توسطNIST  بیان شد. این پیاده‌سازی براساس رمزگذاری فایستل است که در 16 دور انجام می‌شود.*

**

شکل ‏1‑6: جایگزینی اولیه

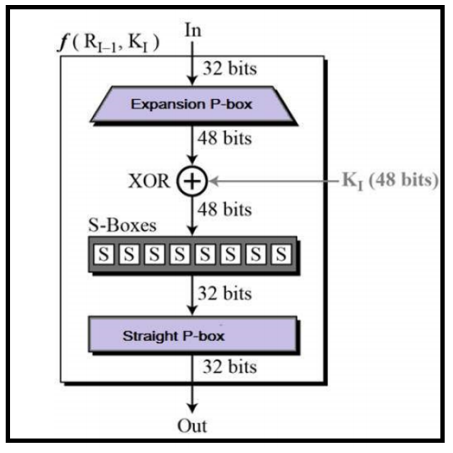
*اندازه بلوک و اندازه کلید این الگوریتم 64 بیت است اما طول کلید 56 بیت است و 8 بیت در رمزگذاری استفاده نمی‌شود. از عملیات زیر در DES استفاده می‌شود.*

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

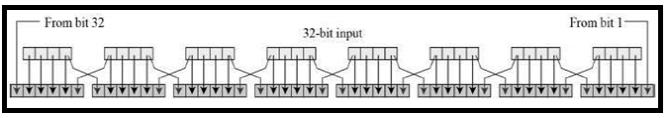
*جایگشت  اولیه: برای فهم جایگشت اولیه شکل*[*1.6*](#شکل1و6) *را مشاهده کنید.*

*عملکرد Round: عملکرد دور هسته اصلی عملکرد DES است. این عملکرد از کلید 48 بیتی تشکیل شده‌است. 32 بیت کلید که درست‌ترین حالت هستند، خروجی 32 بیتی را تولید می‌کند. جزئیات در شکل 1.7  نشان داده شده است.*

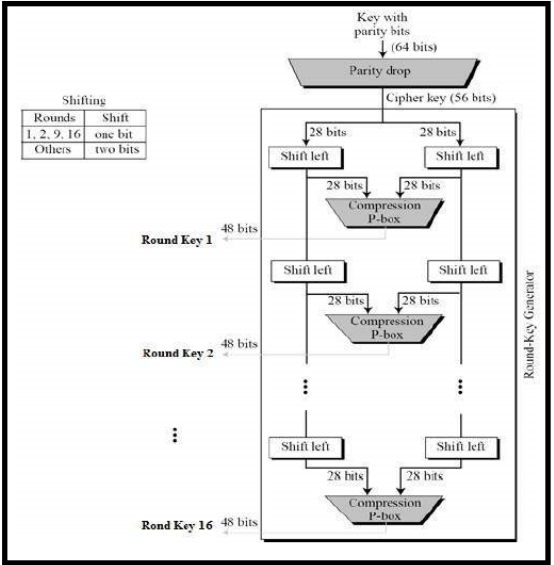
*گسترش جعبه جایگشت: در کلید دور 48 بیت است و ورودی 32 بیت از سمت راست 48 بیت است. نمودار این فرآیند شکل 1.8 نشان داده شده است.*

**

شکل ‏1‑7: تابع Round

**

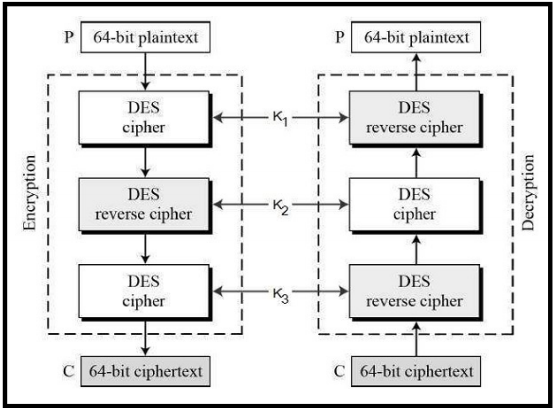
شکل ‏1‑8:  گسترش جعبه جایگزینی[[6]](#footnote-6)

**

شکل ‏1‑9: تولید کلید[[7]](#footnote-7)

*تولید کلید: تابع Round الگوریتم DES ، 16 بلوک از کلیدهای 48 بیتی کلید رمزگذاری 56 بیتی ما را ایجاد می‌کند. این فرایند در شکل*[*1.9*](#شکل1و9) *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 3DES ارتقا می‌یابد.*

*کار الگوریتم 3DES : شکل*[*1.10*](#شکل1و10)*را ببینید؛ اولین گام سه کلید K1، K2، K3.  تولید می‌کند. اندازه هر کلید 56 بیت است و اندازه کل 3 کلید برابر با 3 \* 56 = 168 بیت است و مراحل رمزگذاری در زیر شرح داده شده است:*

**

شکل ‏1‑10: نمودار معماری 3DES [[8]](#footnote-8)

*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 پيشرفته رمزگذاری: NIST یک الگوریتم متقارن الگوریتم دیگری با نام AES معرفی کرد؛ به شکل*[*1.11*](#شکل1و11) *مراجعه کنید. وینسنت ریجمن، جوآن دیمن این الگوريتم را در سال 1998 منتشر كردند. در آن از سه اندازه كليد 128و192و256 بیت و اندازه بلوك 256 بيت استفاده می‌شود.  ویژگی های اصلی AES به شرح زیر است:*

* *این رمزنگاري بلوكي است.*
* *الگوریتم کلید متقارن (رمزگذاری و رمزگشایی را می‌توان با تنها یک كليد انجام داد).*
* *اندازه‌های مختلف کلید را می‌توان با توجه به نیاز استفاده کرد. به عنوان مثال 128و192و256 56 اما اندازه کلید 256 ایمن‌تر است.*
* *قدرت محاسبه سریع‌تر است.*
* *معماری باز است و می‌تواند به راحتی به هر زبان رایانه‌ای طراحی شود.*

كار الگوريتم 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 جايگشت و جایگزینی در هر دور کار می‌کند.*

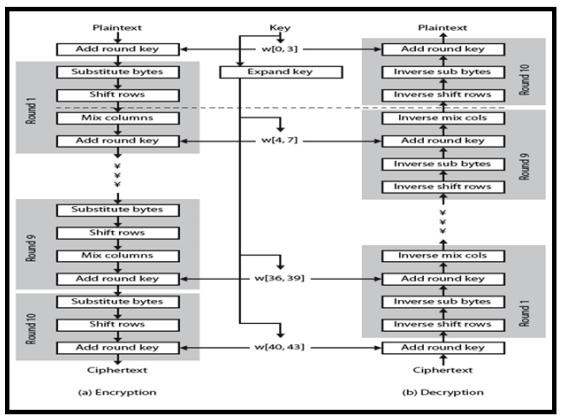
*کلید اصلی به مجموعه ای از چهل و چهار 32 بیت کلمه تقسیم شده است. چهار كلمه مشخص با اندازه 128 بیت برای کلید Round در هر دور استفاده می‌شود.*

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

* + *بایت های جایگزین: از s-box برای اعمال بایت بایت و جايگشت روی بلوک استفاده می‌کند.*
  + *Shift Rows Operation : این یک عملیات جایگزینی ساده است .*
  + *Mix Columns Operation: در این عملیات از روش GF (28) براي جايگزيني استفاده می‌شود.*
  + *افزودن عملكرد كليد Round : بيتي كه با بخشي از كليد منبسط شده در بلوك جاري XOR مي‌شود.*
  + *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 تشكيل 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، مشكلي 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 جايگزيني بایت‌ها فعال مي‌شود، ردیف های Shift و مخلوط می‌شوند. تابع معكوس می‌تواند با استفاده از XOR در همان دور کلید دور در بلوک به دست آيد.*
  + *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 يكسان 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 نياز است كه قابل برگشت باشد.*

## *7.1  قانون HIPAA و GDPR چیست؟*

*HIPAA [**[10](#ش10)] مخفف قانون قابلیت حمل و پاسخگویی بیمه درمانی است. این مصوبه در سال 1996 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 كند.*

**

شکل ‏1‑11: معماري الگوريتم AES [[9]](#footnote-9)

*قوانین مختلفی در مورد دسترسی به داده‌ها و محافظت از داده‌ها با توجه به حساسیت داده‌ها ارائه می‌دهد. 18 ویژگی زیر اعمالي كه بايد محافظت شوند را مشخص مي‌كند* [*11*](#ش11)*:*

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

*GDPR**[*[*12*](#ش12)*]  (مقررات عمومی حفاظت از داده ها) مقررات اتحادیه اروپا است که در سال 2016 پذیرفته شده است. پس از سال 2018 این قانون برای کلیه سازمان های کشورهای اتحادیه اروپا اجباری شده است که ذخيره اطلاعات شخصی فرد را باید مطابق با GDPR باشد.*

## *8.1  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 بيمار علیه آن سازمان شکایت می‌کنند، دادگاه آن سازمان را جریمه می‌کند. بنابراین، دو نوع از دست دادن در اینجا اتفاق می افتد. يک 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.*

## *9.1  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.*

## *10.1  سوالات تحقیق*

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

*1: چه نوع تکنیک‌های محرمانگي داده برای محیط مبتنی بر ابر در دسترس است؟*

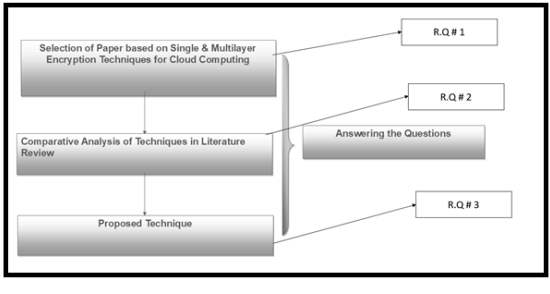
*2: عمده‌ترین ایرادات و نقایص موجود در این تکنیک‌ها چیست؟*

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

## *11.1  روش تحقیق*

*روش تحقیق نقش بسیار مهمی برای دستیابی به هدف دارد. از  روش نشان داده شده در شکل*[*1.12*](#شكل1و12)*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 45 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 ‏1‑12:  نمودار روش تحقیق

## *12.1 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**. [*[*13*](#ش13)*]*

*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.*

## *13.1 اهمیت پایان‌نامه*

*لیست زیر اهمیت پایان‌نامه را نشان می‌دهد:*

*این مطالعه سطح محرمانگي اطلاعات مربوط به بيمار 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.*

|  |  |
| --- | --- |
| *مشکل* | *محرمانگي داده ها ، حریم خصوصی* |
| *تأثیر می گذارد* | *بیمارستان‌ها، بیمار، محيط رایانش ابری*  *، بیمه درمانی و*  *سازمان‌های مرتبط* |
| *تأثیر آن است* | *ممکن است منجر به مرگ يك بيمار شود، ضرر زیادی برای سازمان مرتبط با سلامتی ايجاد شود، حریم خصوصی شخصی خدشه‌دار مي‌شود. اطلاعات از بین خواهد رفت.* |
| *یک راه حل موفق* | *محرمانگي داده‌ها، داده‌های بیمار بايد به طور دائم ایمن، مطمئن و در دسترس باشد.* |
| *ارائه خواهد شد* |

جدول ‏1‑2: اهمیت پایا‌ن نامه

## *14.1  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؟*

## *15.1 سازمان پایان‌نامه*

*فصل‌های این پایان‌نامه به صورت ذیل مرتب شده است:*

* *فصل 2 درباره مرور ادبیات است که در آن ما تکنیک‌های مختلف پیشنهادی را شرح داده‌ایم و یک تحلیل مقایسه‌ای درباره این تکنیک‌ها انجام داده‌ایم.*
* *فصل 3 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 4، نیازهای سخت افزاری و نرم افزاری برای نصب آزمایشی، نحوه انجام آزمایشی و بحث درباره نتایج، ارائه شده است.*
* *فصل 5 درباره نتیجه‌گیری و کارهای آینده است.*

*فصل 2*

# *بررسی ادبیات*

*برای ارائه یک راه حل جامع از مسئله بحث‌شده در فصل 1، 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 كدام است؟*

*قدرت تکنیک‌های مورد استفاده کاربران، در چه حدي 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 2.1 فنون روش تحقیق را نشان می‌دهد. بخش 2.2 کارهای مربوطه را نشان می دهد. بخش 2.3 بررسی‌های مهم بررسی ادبیات و 2.4 نتایج ادبیات را نشان می‌دهد.*

## *2.1  کار مرتبط*

*در [*[*11*](#ش11)*] 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 3DES و تابع مقدار هش را معرفی کرده‌ اند. نویسندگان از اندازه کلید 193 بیت برای لایه 1 و 129 بیت تا 192 بیت برای لایه 2 و 112 تا 128 برای لایه 3 و 80 تا 111 بیت برای لایه 4 استفاده کرده‌اند. کار اصلی نویسندگان بر روی الگوریتم 3DES است. و از الگوریتم منفرد برای رمزگذاری و رمزگشایی استفاده می‌شود.*

*در [*[*12*](#ش12)*] 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 [*[*13*](#ش13)*] 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 [*[*14*](#ش14)*] 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 [*[*15*](#ش15)*] 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 [*[*16*](#ش16)*] نویسندگان الگوریتم DES ، AES ، 3DES ، 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 [*[*17*](#ش17)*] نقصی در [*[*18*](#ش18)*] برای اجرای USB MSD (دستگاه ذخیره‌سازی انبوه) بیان می‌شود. سپس یک ERP جدید برای سیستم مراقبت‌های بهداشتی هوشمند معرفی می‌شود که ایمن تر از [*[*17*](#ش17)*] است.*

*در [*[*19*](#ش19)*] 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 [*[*20*](#ش20)*] نویسندگان به خوبی مدل مراقبت‌های بهداشتی جدیدی را برای ذخیره داده‌های ابری در نظر گرفته‌اند. آن‌ها RBE (رمزنگاری مبتنی بر نقش) را اعمال کرده‌اند. ابتدا، آن‌ها مدل PCEHR (سوابق الکترونیکی کنترل الکترونیکی شخصی) را که توسط دولت استرالیا معرفی شده شرح داده‌اند. سپس PCEHR در RBE برای امنیت داده استفاده می‌شود. آن‌ها ساختار آرم دادهها و ویژگی‌هایش را بر اساس رمزگذاری طراحی می‌کنند و ادعا كردند كه رویكرد آنها كنترل انعطاف‌پذیری در ذخیره‌سازی داده‌ها را فراهم می‌كند.*

*در [*[*21*](#ش21)*] 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 [*[*22*](#ش22)*] 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 [*[*23*](#ش23)*] 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 [*[*24*](#ش24)*] 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 [*[*25*](#ش25)*] ، 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 [*[*26*](#ش26)*] 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 می‌كند. آن‌ها ادعا کردند که تکنیک آن‌ها با ترکیبی از رمزنگاری و استگانوگرافی امنیت بهتری را فراهم می‌کند.*

*در [*[*27*](#ش27)*] 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 اهميت و اهميت بالا اعمال کردند.*

*در [*[*28*](#ش28)*] نویسندگان رویکرد مبتنی بر رمزگذاری ستونی و رمزگشایی مطرح كرده‌اند. 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 درگير خواهند شد نه همه‌شان. آزمایش های مختلفی را روی داده‌های حساس انجام دادند و بهترین روش را بيان كردند اما فقط رمزگذاری تک نوع روي اطلاعات حساس در آن انجام می‌شود.*

*در [*[*29*](#ش29)*] 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 [*[*30*](#ش30)*] نویسندگان ایده ای به نام مدل MIDEA را پیشنهاد کردند. فرآیند رمزگذاری به سرور ابری اختصاص داده شده است. آنها بيان کردند که مقیاس‌پذیری افزایش می‌يابد 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 [*[*31*](#ش31)*] 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 لايه‌بندي یک‌زمانه، استفاده کردند. ماتریس مربع پلی بیوس را پیاده سازی کردند و همچنین تعداد دورها را برای محافظت از داده‌ها افزایش دادند.*

*در [*[*32*](#ش32)*] 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 8 بیت معرفی کردند. آنها بيان کردند که این روش از مصرف برق کم با بهره‌وری بیشتر از منابع استفاده می‌کند.*

*در [*[*33*](#ش33)*] 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 [*[*34*](#ش34)*] 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 [*[*35*](#ش35)*] 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 [*[*36*](#ش36)*] 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 52٪ 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 [*[*37*](#ش37)*] 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 [*[*38*](#ش38)*] 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 [*[*39*](#ش39)*] نویسندگان تشخیص و گزارش پزشکان را در تصاویر اسکن شده اعمال کردند و سپس از استگانوگرافی و رمزنگاری استفاده کردند.*

*در [*[*40*](#ش40)*] 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 [*[*41*](#ش41)*] 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 [*[*42*](#ش42)*] 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 [*[*43*](#ش43)*] 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 [*[*44*](#ش44)*] 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 [*[*45*](#ش45)*] 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 [*[*46*](#ش46)*] 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 [*[*47*](#ش47)*] 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 [*[*48*](#ش48)*] 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 [*[*49*](#ش49)*] نویسندگان الگوریتم‌های همومورف را مقایسه کرده‌اند. آن‌ها فقط توضیح داده‌اند که کلیدهای رمزگذاری و رمزگشایی بر روی ابر چگونه کار می‌کنند.*

*در [*[*50*](#ش50)*] 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 [*[*51*](#ش51)*] الگوریتم‌های مختلف رمزگذاری برای امنیت داده‌ها در ابر بررسی شده‌اند. نویسندگان سطح امنیتی الگوریتم‌های مختلف استانداردها را مقایسه کرده‌اند.*

*در [*[*52*](#ش52)*] چالش‌های مختلف محیط ابر برجسته شده است. نویسندگان برای امنیت داده‌ها، پیشنهادات مختلفی را به ارائه‌دهندگان مختلف ابر ارائه داده‌اند.*

*در [*[*53*](#ش53)*] 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 [*[*54*](#ش54)*] امنیت داده مورد بحث است. ECC نیز از اهمیت برخوردار است و بحث می‌شود.*

*در [*[*55*](#ش55)*] چالش‌های مختلف امنیتی رایانش ابری بازنگری شده،  تکنیک‌های مختلف امنیت داده مورد بحث قرار گرفت که قابلیت اطمینان را ایجاد می‌کند.*

## 2.2 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 2.1 مراجعه 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. اين امر باعث افزایش سطح امنیت می شود.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *کاغذ* | *رویکرهای چند لایه* | *امنیت هدف* | *نقاط قوت* | *نقاط ضعف* |
| *[*[*11*](#ش11)*]* | *بله* | *محرمانگی اطلاعات* | *3DES و الگوریتم هش* | *چگونگی کلیدهای به اشتراک گذاشته شده، استاندارهای HIPAA و GDPR* |
| *[*[*12*](#ش12)*]* | *خیر* | *محرمانگی اطلاعات* | *الگوریتم چند لایه* | *چگونگی کلیدهای به اشتراک گذاشته شده، استاندارهای HIPAA و GDPR*  *و RDBMS تعبیه شده* |
| *[*[*13*](#ش13)*]* | *خیر* | *محرمانگی اطلاعات* | *الگوریتم ECC* | *روش رمزگذاری منفرد استفاده شده است ، از هر استانداردی استفاده نکرده است.* |
| *[*[*14*](#ش14)*]* | *خیر* | *محرمانگی اطلاعات* | *الگوریتم AES* | *روش رمزگذاری منفرد استفاده شده است. از هر استانداردی مانند HIPAA ، GDPR پیروی نکرده است.* |
| *[*[*15*](#ش15)*]* | *بله* | *محرمانگی اطلاعات* | *جفت سازی دوخطی و کلید احراز هویت* | *مسائل کلیدی مدیریت وانطباق HIPAAوGDPR* |
| *[*[*16*](#ش16)*]* | *خیر* | *محرمانگی اطلاعات* | *نظرسنجی روی الگوریتم‌های AESوDESو3DES* | *پیاده‌سازی ندارد.* |
| *[*[*17*](#ش17)*] [*[*18*](#ش18) *]* | *خیر* | *محرمانگی اطلاعات* | *محافظت USB برای داده‌های مراقبت بهداشتی* | *رمزنگاری تک لایه* |
| *[*[*19*](#ش19)*]* | *بله* | *محرمانگی اطلاعات* | *EPR و LSB* | *رمزگذاری مبتنی بر تصویر از هیچ استانداردی مانند GDPR,IPAA پیروی نمی‌کند.* |
| *[*[*20*](#ش20)*]* | *خیر* | *محرمانگی اطلاعات* | *رمزگذاری مبتنی بر نقش* | *از هیچ استانداردی مانند HIPAAوGDPR پیروی نمی‌کند.* |
| *[*[*21*](#ش21)*]* | *بله* | *محرمانگی اطلاعات* | *مبتنی بر اینترنت اشیا* | *رمزگذاری منفرد* |
| *[*[*22*](#ش22)*]* | *خیر* | *محرمانگی اطلاعات* | *الگوریتمElgmal* | *رمزگذاری منفرد* |
| *[*[*23*](#ش23)*]* | *خیر* | *محرمانگی اطلاعات* | *ECC* | *رمزگذاری منفرد* |
| *[*[*24*](#ش24)*]* | *خیر* | *محرمانگی اطلاعات* | *بلاکچین* | *از هیچ استانداردی مانند HIPAAوGDPR پیروی نمی‌کند.* |
| *[*[*25*](#ش25)*]* | *بله* | *محرمانگی اطلاعات* | *DES و فایستل و مدیریت*  *WBAN* | *از هیچ استانداردی مانند HIPAAوGDPR پیروی نمی‌کند.* |
| *[*[*26*](#ش26)*]* | *بله* | *محرمانگی اطلاعات* | *الگوریتم AES,LSB* | *به عنوان رمزگذاری مبتنی تصویر استفاده می‌شود.* |
| *[*[*27*](#ش27)*]* | *بله* | *محرمانگی اطلاعات* | *نشانه گذاری روی داده‌ها* | *از هیچ استانداردی مانند HIPAAوGDPR پیروی نمی‌کند.* |
| *[* [*28*](#ش28) *]* | *خیر* | *محرمانگی اطلاعات* | *پارتیشن‌بندی داده‌ها و اعمال رمزگذاری منفرد داده‌ها* | *بدون رمزگذاری چند لایه* |
| *[* [*29*](#ش29) *]* | *خیر* | *محرمانگی اطلاعات* | *پارتیشن‌بندی عمودی و فعال‌سازی رمزگذاری* | *رمزگذاری منفرد* |
| *[*[*30*](#ش30)*]* | *خیر* | *محرمانگی اطلاعات* | *مدل MIDEA برای رمزگذاری و رمزگذاری مبتنی بر MAC* |  |
| *[*[*31*](#ش31)*]* | *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 ميشوند.* |
| *[*[*32*](#ش32)*]* | *بله* | *محرمانگی اطلاعات* | *AES128 بیتی و بلاکچین* | *پیاده‌سازی روی  RDBMS و از هیچ استانداردی مانند HIPAA ، GDPR پیروی نمی‌کند.* |
| *[*[*33*](#ش33)*]* | *بله* | *محرمانگی اطلاعات* | *رمزگذاری مبتنی بر ویژگی و کلید قابل لغو* | *پیاده‌سازی روی  RDBMS و از هیچ استانداردی مانند HIPAA ، GDPR پیروی نمی‌کند.* |
| *[*[*34*](#ش34)*]* | *خیر* | *محرمانگی اطلاعات* | *نظر سنجی* |  |
| *[*[*35*](#ش35)*]* | *خیر* | *محرمانگی اطلاعات* | *رمزگذاری منفرد* |  |
| *[*[*36*](#ش36)*]* | *خیر* | *محرمانگی اطلاعات* | *مهاجمان خودی از خارجی خطرناک‌تر هستند.* |  |
| *[*[*37*](#ش37)*]* | *بله* | *محرمانگی اطلاعات* | *استگانوگرافی با استفاده از LSB و تبدیل به تصویر* | *روی خصوصیات PHI ممکن نیست.* |
| *[*[*38*](#ش38)*]* | *بله* | *محرمانگی اطلاعات* | *AES با کمی تغییر و سپس LSB* | *تبدیل به داده‌های مبتنی بر تصویر* |
| *[*[*39*](#ش39)*]* | *خیر* | *محرمانگی اطلاعات* | *استگانوگرافی* | *رمزگذاری منفرد* |
| *[*[*40*](#ش40)*]* | *بله* | *محرمانگی اطلاعات* | *الگوریتم فایستل*  *ریتم با تغییر S-box و*  *DES* | *استفاده از تکنیک های قدیمی* |

جدول ‏2‑1: مرور آنالیز ادبیات

## *3.2 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 داديم 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.*

## *4.2  خلاصه*

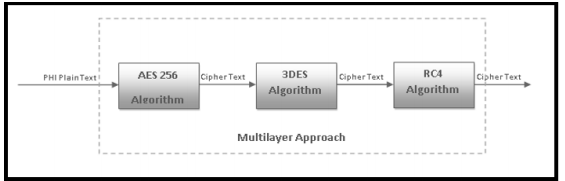
*در مجموع 45 مقاله تحقیقاتی را مرور کردیم که 8 مقاله در اینجا نشان داده شده است. در ادبیات ما 8-10 تکنیک مبتنی بر الگوریتم های رمزنگاری منفرد است که 5-6 نویسنده بر روی داده‌های مبتنی بر تصویر کار کرده‌اند و داده‌ها را به تصاویر تبدیل کرده‌اند و 2 نویسنده نیز بر روی رمزگذاری بر اساس نقش کار کرده اند، 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 3*

# 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 3.1 نحوه دستیابی به مجموعه داده را توصیف می‌کند، بخش 3.2 نحوه رمزگذاری داده‌ها را توصیف می‌کند، بخش 3.3 معماری متد را توصیف می‌کند ، بخش 3.4 توضیح می‌دهد که امکانات رمزگذاری در پایگاه داده سرور SQL برای تبلیغ رمزگذاری موجود است. بخش 3.5 نتیجه‌گیری است.*

**

شکل ‏3‑1: تکنیک محافظت از چند لایه

## *1.3  انتخاب مجموعه داده‌ها*

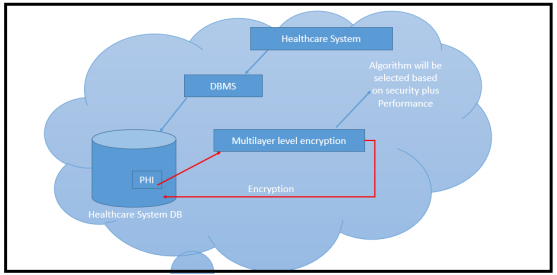
*برای توسعه طرح و تجزیه و تحلیل هدف، یک مجموعه داده ساختگی( برای ایمنی بیمار) از حدود 500 بیمار را انتخاب کرده‌ایم و از نمودار زیر برای رمزگذاری PHI هر ویژگی استفاده کرده‌ایم.*

## *2.3  لایه رمزگذاری PHI Attribut ES*

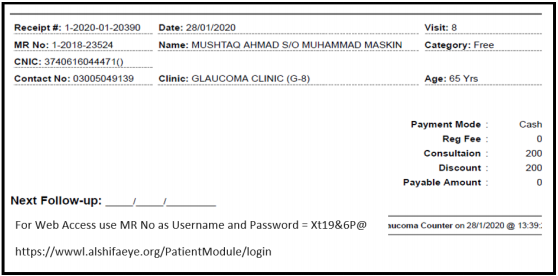
*شکل*[*1.3*](#شکل3و1) *نشان می‌دهد که یک ویژگی از داده‌های PHI به شکل متن ساده انتخاب شده است. این ویژگی به یک الگوریتم منتقل می‌شود. به عنوان مثال AES256 با یک کلید و سپس خروجی این الگوریتم که متن رمزگذاری شده‌ای است و با یک کلید دیگر به الگوریتم 3DES منتقل می‌شود. این مفهوم رمزگذاری چند لایه است که از داده‌ها محافظت می‌کند و سطح محرمانگی را افزایش می‌دهد.*

## *3.3  معماری روش*

*شکل*[*2.3*](#شکل3و2)*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 ‏3‑2:  نمودار معماری روش‌شناسی

**

شکل ‏3‑3:  فیش ورود به سیستم برای بیمار

*برای دسترسی در وب سایت( به شکل*[*3.3*](#شکل3و3) *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 3DES بر روی داده‌ها اعمال مي‌كنيم 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.*

## *4.3  فرآیند رمزگذاری و رمزگشایی در RDBMS ( (Microsoft SQL Server)*

*سرور SQL با استفاده از کلید نامتقارن یا متقارن ارائه شده 3DES 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. ويژگی دیگر این است که چندین کلید متقارن می‌توانند همزمان باز شوند و رمزگذاری و رمزگشایی از این طریق انجام می‌شود.*

### *1.4.3  چگونه رمزگذاری در SQL Server انجام می‌شود؟*

*شکل*[*4.3*](#شكل3و4) *روند رمزگذاری کلی از SQL Server بر روی يك ستون از یک جدول را نشان می‌دهد.*

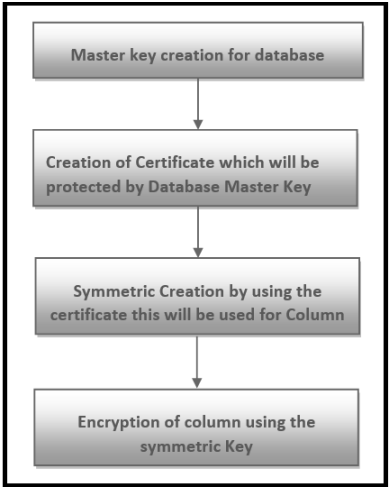
*هدف اصلی کلید اصلی پایگاه‌داده، محافظت از کلیدها و گواهینامه‌های خصوصی است که در پایگاه‌داده ذخیره می‌شوند كه بر اساس روش متقارن است. این کلید توسط رمز عبور در زمان ایجاد محافظت می‌شود.*

#### 1.1.4.3  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.*

#### 2.1.4.3  ایجاد گواهی

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

**

شکل ‏3‑4:  فرآیند رمزگذاری کلی

#### 3.1.4.3 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.*

#### 4.1.4.3  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.*

## *5.3  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 درRDBMS*
* *مفهوم کلید اصلی چیست؟*
* *هدف از گواهی‌نامه چیست؟*
* *کلید متقارن در RDBMS چگونه کار می‌کند؟*
* *گواهی و کلیدها چگونه ایجاد می‌شوند؟*

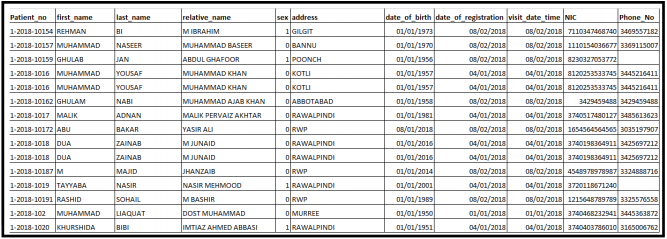
*فصل 4*

# *تجزیه و تحلیل آزمايشي 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 4 به بخش‌های مختلف تقسیم شده است. بخش 1.4 در مورد داده ها و اطلاعات بحث می‌کند. بخش 2.4 تنظیمات آزمایشی را توصیف می‌کند. بخش 3.4 فرآیند رمزگذاری را تشريح می‌کند. بخش 4.4 روند رمزگشایی را توصیف می‌کند و آخرین بخش 4.5 مربوط به بخش تجزیه و تحلیل نتایج است.*

## *1.4  انتخاب مجموعه داده*

*ما یک مجموعه داده ساختگی از 500 بیمار را برای هدف‌ آزمایش آماده کرده‌‌ايم. نمونه مجموعه داده در شکل*[*1.4*](#شكل4و1) *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 محرمانگي، ما خصوصیات ویژه  PHI را برای رمزگذاری و رمزگشایی در نظر گرفته‌ایم.*

**

شکل ‏4‑1: نمونه مجموعه داده‌های ساختگی

## *2.4  نصب پیکربندی سخت‌افزار و نرم‌افزار*

*برای پیاده‌سازی از سخت‌افزار و نرم‌افزار زیر استفاده می‌شود.*

### *1.2.4  سخت‌افزار مورد نياز*

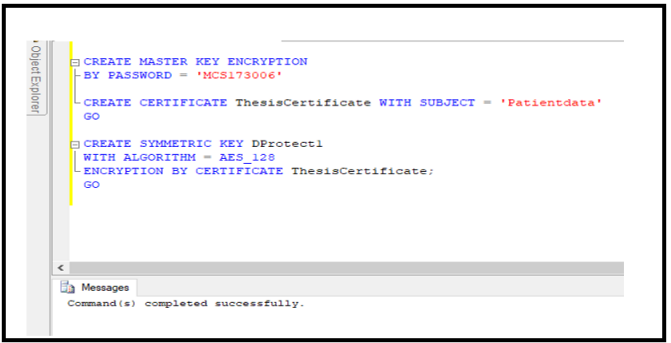
*برای ساخت چارچوب از سخت‌افزار زیر استفاده می‌شود.*

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

### *2.2.4  سیستم عامل و نرم‌افزار توسعه*

*برای ساخت چارچوب از نرم‌افزارهاي زیر استفاده می‌شود:*

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

**

شکل ‏4‑2:  ایجاد کلیدها و گواهینامه ها

## *3.4  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*[*2.4*](#شكل4و2) *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) ,*

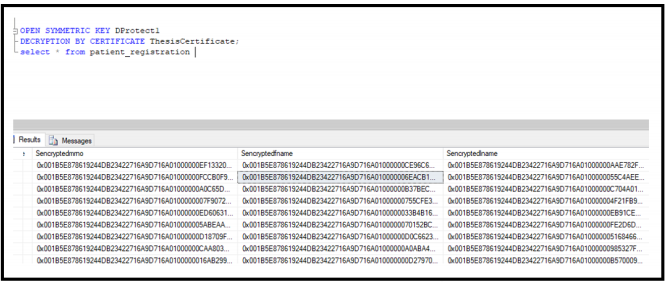
*Sencryptedregamount=EncryptByKey(Key GUID(’DProtect1’), regamount)*

*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*[*3.4*](#شكل4و3)*نشان داده شده، ذخیره می‌شوند.*

**

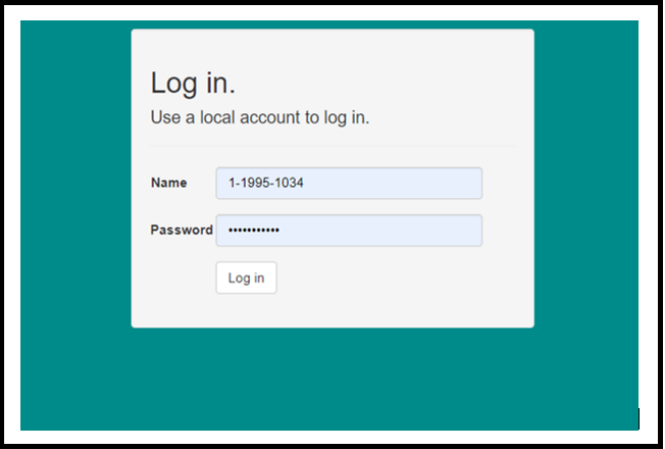
شکل ‏4‑3: فرم رمزگذاری شده داده‌ها

## *4.4 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* [*4.4*](#شكل4و4) *و شکل*[*5.4*](#شكل4و5)*نشان داده شده است.*

## *5.4 تحلیل نتایج*

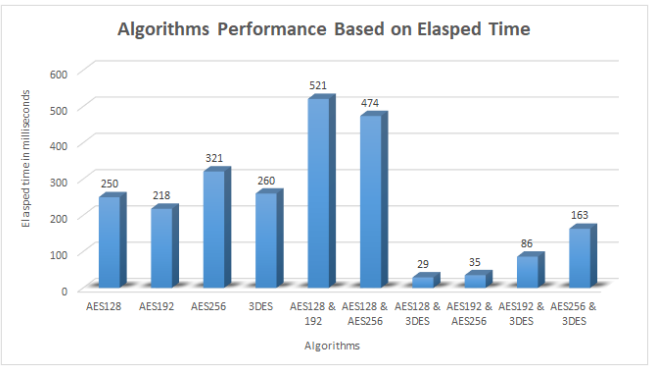
*در این بخش نتایج بدست آمده با روش‌های منفرد و ترکیبی مقایسه می‌شود. نمودارهای زیر در شکل*[*6.4*](#شكل4و6) *و شکل* [*7.4*](#شكل4و7) *و شکل*[*8.4*](#شكل4و8)*؛ نتایج زمان سپری شده، زمان پردازنده و ظرفیت ذخیره‌سازی داده‌های الگوریتم‌های رمزگذاری شده مختلف را نشان می‌دهد. شکل*[*7.4*](#شكل4و7) *زمان سپری شده روی 500 رکورد با الگوریتم‌های رمزگذاری منفرد نشان می‌دهد.*

**

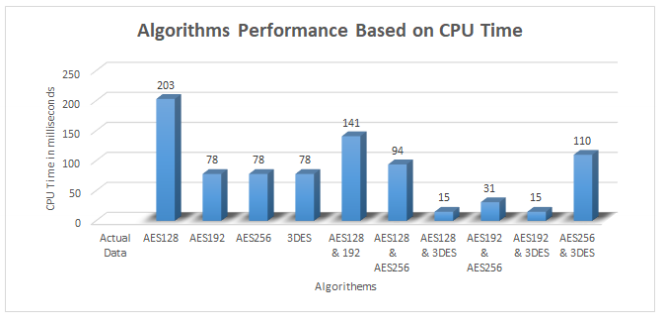
شکل ‏4‑4: : صفحه ورود به سیستم برای ورود بیمار

**

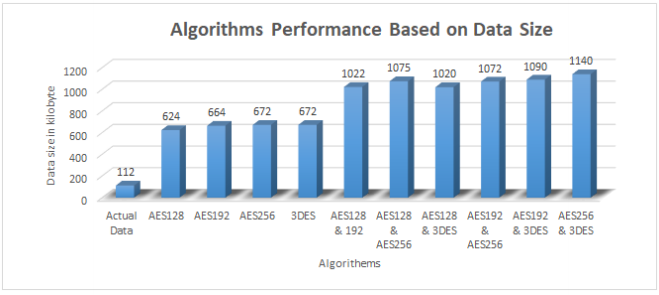
شکل ‏4‑5: جزئیات پرونده پزشکی یک بیمار

**

شکل ‏4‑6 : نمای گرافیکی زمان سپری شده الگو

**

شکل ‏4‑7 :  نمای گرافیکی زمان CPU زمان الگوریتم رمزگذاری چندلایه و منفرد

**

شکل ‏4‑8: نمای گرافیکی اندازه جدول پایگاه داده بعد از ذخیره‌سازی

* *اگر الگوریتم رمزگذاری منفرد AES با اندازه کلید 128 بیتی اعمال شود، کل زمان سپری شده 250 میلی‌ثانیه خواهدبود.*
* *اگر AES با اندازه کلید 192 بیتی اعمال شود، کل زمان سپری شده 21 میلی‌ثانیه خواهد‌بود.*
* *اگر AES با اندازه کلید 218 بیتی اعمال شود، کل زمان سپری شده 321 میلی‌ثانیه خواهدبود.*
* *اگر 3DES به تنهایی اعمال شود، کل زمان سپری شده 260 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 192 استفاده شود؛ زمان سپری شده 521 میلی‌ثانیه خواهدبود.*
* *اگر ترکیبی از AES128 و 256 استفاده شود؛ زمان سپری شده 474 میلی‌ثانیه خواهدبود.*
* *اگر ترکیبی از AES128 و 3DES استفاده شود، زمان سپری شده 29 میلی‌ثانیه خواهدبود.*
* *اگر ترکیبی از AES192 و AES256 استفاده شود، مدت زمان سپری شده 35 میلی ثانیه خواهد بود.*
* *اگر ترکیبی از AES192 و 3DES استفاده شود، مدت زمان سپری شده 86 میلی‌ثانیه خواهدبود.*
* *اگر ترکیبی از AES256 و 3DES استفاده شود، مدت زمان سپری شده 163 میلی ثانیه خواهدبود.*

*شکل*[*8.4*](#شكل4و8) *زمان پردازنده را در میلی‌ثانیه برای 500 رکورد با الگوریتم‌های رمزگذاری منفرد به ما ارائه می‌دهد.*

* *AES128 زمان پردازنده 203 میلی ثانیه را می‌گیرد.*
* *AES192 زمان پردازنده 78 میلی‌ثانیه است.*
* *AES256 ، 72میلی‌ثانیه طول می‌کشد.*
* *3DES، 78 میلی‌ثانیه طول می‌کشد.*

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

* + *AES128 و 192، 141 میلی‌ثانیه طول می‌کشد.*
  + *AES128 و AES256 ، 94 میلی‌ثانیه طول می‌کشد.*
  + *AES192 و AES256 31 میلی‌ثانیه طول می‌کشد.*
  + *AES192 و 3DES ، 15 میلی‌ثانیه طول می‌کشد.*
  + *AES256 و 3DES ، 110 میلی‌ثانیه طول می‌کشد.*

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *AES256* | *3DES* | *چند لایه*  *AES128*  *& 3DES* | *چند لایه*  *AES192*  *& 3DES* | *چند لایه*  *AES256*  *& 3DES* |  |
| *کم* | *کم* | *متوسط* | *متوسط* | *بالا* | *سطح محرمانه بودن*  *[*[*56*](#ش56)*]* |
| *سریع* | *سریع* | *سریع* | *متوسط* | *متوسط* | *سرعت رمزگذاری*  *و رمزگشایی*  *[*[*56*](#ش56)*]* |
| *تک کلید* | *تک کلید* | *دو کلید* | *دو کلید* | *دو کلید* | *تعداد کلید*  *استفاده شده [*[*56*](#ش56)*]* |
| *دشوار* | *دشوار* | *سخت* | *سخت* | *خیلی سخت* | *امکان*  *حمله [*[*56*](#ش56)*]* |
| *12* | *48* | *12* | *48* | *60* | *تعداد دورها [*[*56*](#ش56)*]* |
| *256* | *128و192* | *256* | *128و192* | *متفاوت* | *طول کلید برحسب بایت [*[*56*](#ش56)*]* |

جدول ‏4‑1: مفایسه الگوریتم‌های منفرد و ترکیبی 3DES و AES256

*در جدول*[*1.4*](#جدول4و1) *مقایسه الگوریتم‌های مختلف را با یک لایه و چند لایه انجام داده‌ایم. سطح محرمانگي 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 محرمانگي 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 محرمانگي، 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 محرمانگي بسیار بالا خواهد بود. ردیف دوم جدول*[*1.4*](#جدول4و1)*در مورد سرعت الگوریتم متفاوت است. سرعت AES256 و 3DES متوسط ​​است، سرعتAES192 و 3DES نیز متوسط ​​است اما سرعت AES256 و 3DES به تنهایی بهتر از الگوریتم‌های چند لایه است. تنها نقطه ضعف الگوریتم 3DES سرعت است. به همین دلیل است که وقتی با الگوریتم دیگری استفاده میشود روند تركيبي را نیز کند می‌کند. دلیل این امر 48 دور آن است. ردیف سوم جدول*[1.4](#جدول4و1) *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.*

## *6.4  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 5*

# *نتیجه‌گیری و آینده کار*

## *1.5  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.*

## *2.5 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

[1] 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.“, 10th International Conference on EUropean Transnational Education (ICEUTE 2019), 2019.

[2] S. M and Altowaijri, “An architecture to improve the security of cloud computing in the healthcare sector,” in Smart Infrastructure and Applications. Springer, pp.249–266,2020.

[3] “https://tutorialspoint.com/cloud-computing/cloud-computing-overview.htm/“

[4] “https://timesofcloud.com/cloud-tutorial/characteristics-of-cloud-computing-as-per-nist/“

[5] 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. 20, no. 7, p. e10041, 2018.

[6] Z. Yan, R. H. Deng, and V. Varadharajan, “Cryptography and data security in cloud computing,” 2017.

[7] T. M. Damico, “A brief history of cryptography,” Inquiries Journal, vol. 1, no. 11, 2009.

[8] “https://www.garykessler.net/library/crypto.html/ “

[9] Babatunde, A. O., A. J. Taiwo, and E. G. Dada., “Information Security in Health Care Centre Using ryptography and Steganography.,” arXiv preprint arXiv:1803.05593,2018.

[10] 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. 239, no. 6, p. 772, 2004.

[11] R. Sulaiman, D. Sharma, W. Ma, and D. Tran, “A new security model using multilayer approach for e-health services,” Journal of Computer Science, vol. 7, no. 11, pp. 1691–1703, 2011.

[12] K. Sudheep and S. Joseph, “Review on securing medical big data in healthcare cloud,” in 2019 5th nternational Conference on Advanced Computing & Communication Systems (ICACCS). IEEE, 2019, pp. 212–215.

[13] V. S. V. Hema and R. Kesavan, “Ecc based secure sharing of healthcare data in the health cloud environment,” Wireless Personal Communications, vol. 108, no. 2, pp. 1021–1035, 2019.

[14] M. M. Kiah, M. S. Nabi, B. Zaidan, and A. Zaidan, “An enhanced security solution for electronic medical records based on aes hybrid technique with soap/xml and sha-1,” Journal of medical systems, vol. 37, no. 5, p. 971, 2013.

[15] E. Shanmugapriya and R. Kavitha, “Medical big data analysis: preserving security and privacy with hybrid loud technology,” Soft Computing, vol. 23, no. 8, pp. 2585–2596, 2019.

[16] F. Shahbodin, A. Azni, T. Ali, and C. K. N. C. K. Mohd, “Lightweight cryptography techniques for mhealth cybersecurity,” in Proceedings of the 2019 Asia Pacifific Information Technology Conference, 2019, pp. 44–50.

[17] 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. 60, no. 1, pp. 30–37, 2014.

[18] K. Renuka, S. Kumari, and X. Li, “Design of a secure three-factor authentication scheme for smart healthcare,” Journal of medical systems, vol. 43, no. 5, p. 133, 2019.

[19] S. A. Parah, A. Bashir, M. Manzoor, A. Gulzar, M. Firdous, N. A. Loan, and J. A. Sheikh, “Secure and reversible data hiding scheme for healthcare system using magic rectangle and a new interpolation technique,” in Healthcare Data Analytics and Management. Elsevier, 2019, pp. 267–309.

[20] L. Zhou, V. Varadharajan, and K. Gopinath, “A secure role-based cloud storage system for encrypted patient-centric health records,” The Computer Journal, vol. 59, no. 11, pp. 1593–1611, 2016.

[21] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. Rodrigues, “Authentication in cloud-driven iot-based big data environment: Survey and outlook,” Journal of Systems Architecture, vol. 97, pp. 185–196, 2019.

[22] K. J. Modi and N. Kapadia, “Securing healthcare information over cloud using hybrid approach,” in Progress in advanced computing and intelligent engineering. Springer, 2019, pp. 63–74.

[23] 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. 50, no. 1, pp. 73–80, 2019.

[24] H. Jin, Y. Luo, P. Li, and J. Mathew, “A review of secure and privacypreserving medical data sharing,” IEEE Access, vol. 7, pp. 61 656–61 669, 2019.

[25] Y. S. Lee, E. Alasaarela, and H. J. Lee, “An effiffifficient encryption scheme using elliptic curve cryptography (ecc) with symmetric algorithm for healthcare system,” International journal of security and its applications, vol. 8, no. 3, pp. 63–70, 2014.

[26] 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.

[27] G. Garkoti, S. K. Peddoju, and R. Balasubramanian, “Detection of insider attacks in cloud based e-healthcare environment,” in 2014 International Conference on Information Technology. IEEE, 2014, pp. 195–200.

[28] 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. 43, no. 5, p. 124, 2019.

[29] A. M. Elmisery and H. Fu, “Privacy preserving distributed learning clustering of healthcare data using cryptography protocols,” in 2010 IEEE 34th Annual Computer Software and Applications Conference Workshops. IEEE, 2010, pp. 140–145.

[30] 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. 8, no. 2, p. 171, 2019.

[31] Jammu, Aashmeen, and Harjinder Singh, “Improved AES for Data Security in E-Health IEEE,” International Journal of Advanced Research in Computer Science 8.5 2017.

[32] K.-L. Tsai, Y.-L. Huang, F.-Y. Leu, I. You, Y.-L. Huang, and C.-H. Tsai, “Aes-128 based secure low power communication for lorawan iot environments,” IEEE Access, vol. 6, pp. 45 325–45 334, 2018.

[33] A. Michalas and N. Weingarten, “Healthshare: Using attribute-based encryption for secure data sharing between multiple clouds,” in 2017 IEEE 30th International Symposium on Computer-Based Medical Systems (CBMS). IEEE, 2017, pp. 811–815.

[34] A. Michalas, N. Paladi, and C. Gehrmann, “Security aspects of e-health systems migration to the cloud,” in 014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom). IEEE, 2014,

pp. 212–218.

[35] H. Asri, H. Mousannif, H. Al Moatassime, and T. Noel, “Big data in healthcare: Challenges and opportunities,” in 2015 International Conference on Cloud Technologies and Applications (CloudTech). IEEE, 2015, pp. 1–7.

[36] J. Oltsik, “Vormetric/ESG Insider Threat Report: Profifile on HealthCare, 2014, pp. 1–7. [37] V Mahalakshmi, S Satheeshkumar and Dr. S Sivakumar, “Performance of steganographic methods in medical imaging, International Journal of Computational and Applied Mathematics Vol. 12, no. 1, pp 549-556,2017.

[38] PratikshaSethi and V Kapoor, “A Secured System for Information Hiding in Image Steganography using enetic algorithm and Cryptography, International Journal of Computer Applications, Vol. 144, No. 9Et.al.,2016.

[39] “Steganography and cryptography approaches combined using medical digital images,” International Journal of Engineering Research & Technology (IJERT), vol. 4, 2015.

[40] 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. 23, pp. 1030-1036,2010

[41] C. Jiang, B. Li, and H. Xu, “An effiffifficient scheme for user authentication in wireless sensor networks,” IEEE, pp. 438–442, 2007.

[42] L. Chen and D. B. Hoang, “Novel data protection model in healthcare cloud,” IEEE, pp. 550–555, 2011.

[43] 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. 4752.,2010

[44] 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. 11 676–11 686, 2018.

[45] 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. 24, no. 1, pp. 131143, Jan.2013.

[46] H. Kaur, H. P. S. Gill, and D. Sarmah, “Multiphase and multiple encryption,” IEEE, pp. 1–8.

[47] Kumar, Vishal, et al. ”Multiple Encryption using ECC and its Time Complexity Analysis.” International Journal of Computer Engineering In Research Trends 3.11, pp. 568-572, 2016.

[48] Tebaa, Maha, and Said El Hajji., ”Secure cloud computing through homo morphic encryption.” empharXiv preprint arXiv:1409.0829, (2014).

[49] Sarhan, Akram, and LeszekLilien, ”An Approach to Identity Management in Clouds without Trusted Third Parties.” empharXiv preprint arXiv:1904.00880, (2019).

[50] R. Arora, A. Parashar, and C. C. I. Transforming, “Secure user data in cloud computing using encryption algorithms,” pp. 1922–1926, 2013.

[51] 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) 1.2”, : pp. 136-146,2011.

[52] 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. 261–265, 2013.

[53] Albugmi, Ahmed, et al., ”Data security in cloud computing.”, 2016 Fifth International Conference on Future Generation Communication Technologies (FGCT). IEEE, 2016.

[54] V. Gampala, S. Inuganti, and S. Muppidi, “Data security in cloud computing with elliptic curve cryptography,” pp. 138–141, 2012.

[55] Ahamed, Farhad, SeyedShahrestani, and AthulaGinige., ”Cloud computing: security and reliability issues.”, Communications of the IBIMA 2013, 2013.

[56] Babatunde, AO and Taiwo, AJ and Dada, EG, ”Information Security in Health Care Centre Using Cryptography and Steganography”, arXiv preprint

arXiv:1803.05593, 201.

1. https://medium.com/@outrightsystems/cloud-computing-in-business-ab19f308221d [↑](#footnote-ref-1)
2. <https://timesofcloud.com/cloud-tutorial/characteristics-of-cloud-computing-as-per-nist/> [↑](#footnote-ref-2)
3. https://www.tutorialspoint.com/cryptography/cryptosystems.htm [↑](#footnote-ref-3)
4. https://www.tutorialspoint.com/cryptography/cryptosystems.htm [↑](#footnote-ref-4)
5. https://www.tutorialspoint.com/cryptography/cryptosystems.htm [↑](#footnote-ref-5)
6. 7https://www.tutorialspoint.com/cryptography/cryptosystems.htm [↑](#footnote-ref-6)
7. https://www.tutorialspoint.com/cryptography/cryptosystems.htm [↑](#footnote-ref-7)
8. https://www.tutorialspoint.com/cryptography/cryptosystems.htm [↑](#footnote-ref-8)
9. http://pranav-mnit.tripod.com/aes.htm [↑](#footnote-ref-9)