

**دانشکده فنی و مهندسی**

**گروه مهندسی کامپیوتر و فناوری اطلاعات**

**گزارش سمینار كارشناسي ارشد رشته مهندسي كامپيوتر نرم‌افزار(M.Sc)**

**عنوان سمينار:**

**مدل رمزگذاری چند لایه برای محافظت از داده‌های مراقبت‌هاي بهداشتی در محیط ابري( بررسي و مرور)**

**استاد راهنما:**

**دکتر سيدعلي رضوي**

**نگارنده:**

**سميه كرباسي راوري**

مرداد 1400

**BISM2**

فهرست مطالب

[چکیده 1](#_Toc79284505)

[کلمات کلیدی 1](#_Toc79284506)

[1. مقـدمـه 2](#_Toc79284507)

[۱-۱ تعريف مسئله و بيان سؤال‌های اصلي تحقيق 5](#_Toc79284508)

[1-2 ضرورت تحقیق 5](#_Toc79284509)

[۱ – ۳ هدف‌ها 5](#_Toc79284510)

[1-4 چه كاربردهايي از انجام اين تحقيق متصور است؟ 6](#_Toc79284511)

[1-5 روش و مراحل انجام تحقیق 6](#_Toc79284512)

[1-6 سازمان پایان‌نامه  مورد بررسی 6](#_Toc79284513)

[1-7 ساختار گزارش تحقیق 6](#_Toc79284514)

[2. مفـاهیـم عمـومـی رمزگذاری و پيشينه تحقيق 7](#_Toc79284515)

[2-1 انواع طرح‌های رمزنگاری 7](#_Toc79284516)

[2-1-1 رمزگذاري متقارن 7](#_Toc79284517)

[2-1-2 رمزگذاري نامتقارن 7](#_Toc79284518)

[2-2 سرویس امنیتی برای رمزنگاری برای مراقبت های بهداشتی 8](#_Toc79284519)

[2-3 رمزگذاری چند لایه 9](#_Toc79284520)

[2-4 کار الگوریتم‌های مورد استفاده در طرح پیشنهادی 9](#_Toc79284521)

[2-5 پیشینه تحقیق 14](#_Toc79284522)

[3. مروری بر کارهای انجام‌شده 17](#_Toc79284523)

[3-1 مقدمه 17](#_Toc79284524)

[3-2 راه‌اندازی آزمایشی طرح پیشنهادی 17](#_Toc79284525)

[3-2-1 فرآیند رمزگذاری و رمزگشایی در RDBMS 19](#_Toc79284526)

[3-3 تجزیه و تحلیل طرح پیشنهادی 19](#_Toc79284527)

[4-3 نصب پیکربندی سخت‌افزار و نرم‌افزار 20](#_Toc79284528)

[3-4-1 سخت‌افزار مورد نياز 20](#_Toc79284529)

[3-4-2 سیستم عامل و نرم‌افزار مورد نیاز 20](#_Toc79284530)

[3-5 ایجاد کلیدها و گواهینامه‌ها و رمزگذاری داده‌ها 20](#_Toc79284531)

[3-6 رمزگشایی داده‌ها 22](#_Toc79284532)

[3-7 تحلیل نتایج 23](#_Toc79284533)

[4. کاربرد الگوريتم‌هاي چندگانه رمزگذاري روي داده‌هاي مراقبت بهداشتي-مزایا و معایب 26](#_Toc79284534)

[4-1 مقدمه 26](#_Toc79284535)

[4-2 دستورالعمل‌های موجود 26](#_Toc79284536)

[4-3 آینده کار 27](#_Toc79284537)

[4-4 مزایا و معايب استفاده از تکنیک‌های پیشنهادی 27](#_Toc79284538)

[4-4-1 مزايا 27](#_Toc79284539)

[4-4-2 معايب 28](#_Toc79284540)

[4-5 پاسخ به سوالات تحقیق 28](#_Toc79284541)

[4-6 جمع بندی 29](#_Toc79284542)

[5. جمع‌بندی و پیشنهادها 30](#_Toc79284543)

[5-1 مقدمه 30](#_Toc79284544)

[۵ – 2 نتایج حاصل از تحقیق 30](#_Toc79284545)

[5-3 پيشنهادها 31](#_Toc79284546)

[5-4 ارائه ایده برای پایان‌نامه‌های جدید تکمیلی 31](#_Toc79284547)

[5-5 جمع‌بندی و نتیجه‌گیری 32](#_Toc79284548)

[مراجع 33](#_Toc79284549)

[واژه‌نامه 34](#_Toc79284550)

[Abstract 36](#_Toc79284551)

**فهرست اشکال**

[شکل ‏1‑1: رایانش ابری 3](#_Toc79284662)

[شکل ‏1‑2: رمزنگاری استگانوگرافي(Shah,2020) 4](#_Toc79284663)

[شکل ‏2‑1: رمزگذاری نامتقارن کلید 8](#_Toc79284664)

[شکل ‏2‑2: روش رمزگذاری چند لایه (Shah,2020) 9](#_Toc79284665)

[شکل ‏2‑3: جایگزینی اولیه(Shah,2020) 10](#_Toc79284666)

[شکل ‏2‑4: تابع Round(Shah,2020) 10](#_Toc79284667)

[شکل ‏2‑5 : گسترش جعبه جایگزینی 10](#_Toc79284668)

[شکل ‏2‑6 : تولید کلید 11](#_Toc79284669)

[شکل ‏2‑7: نمودار معماری 3DES 12](#_Toc79284670)

[شکل ‏2‑8 : معماري الگوريتم AES (Shah,2020) 14](#_Toc79284671)

[شکل ‏3‑1: تکنیک محافظت از چند لایه (Shah,2020) 17](#_Toc79284672)

[شکل ‏3‑2: نمودار معماری روش‌شناسی(Shah,2020) 18](#_Toc79284673)

[شکل ‏3‑3: فیش ورود به سیستم برای بیمار (Shah,2020) 18](#_Toc79284674)

[شکل ‏3‑4 : فرآیند رمزگذاری کلی(Shah,2020) 19](#_Toc79284675)

[شکل ‏3‑5 : نمونه مجموعه داده‌های ساختگی(Shah,2020) 20](#_Toc79284676)

[شکل ‏3‑6 : ایجاد کلیدها و گواهینامه‌ها(Shah,2020) 21](#_Toc79284677)

[شکل ‏3‑7 : فرم رمزگذاری شده داده‌ها(Shah,2020) 21](#_Toc79284678)

[شکل ‏3‑8 : صفحه ورود به سیستم برای ورود بیمار(Shah,2020) 22](#_Toc79284679)

[شکل ‏3‑9 : جزئیات پرونده پزشکی یک بیمار(Shah,2020) 22](#_Toc79284680)

[شکل ‏3‑10 : نمای گرافیکی زمان سپری شده الگو (Shah,2020) 23](#_Toc79284681)

[شکل ‏3‑11 : نمای گرافیکی زمان CPU زمان الگوریتم رمزگذاری چندلایه و منفرد(Shah,2020) 23](#_Toc79284682)

[شکل ‏3‑12 : نمای گرافیکی اندازه جدول پایگاه داده بعد از ذخیره‌سازی(Shah,2020) 24](#_Toc79284683)

**فهرست جداول**

[جدول ‏1‑1 : مقایسه بین رمزنگاری کلاسیک و مدرن(Shah,2020) 4](#_Toc79283324)

[جدول ‏4‑1 : مفایسه الگوریتم‌های منفرد و ترکیبی 3DES و AES256(Shah,2020) 28](#_Toc79283325)

**فهرست علائم اختصاری**

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

# 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 پایگاه داده رابطه‌ای و فریم‌ورک 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. (Shah,2020)

کلمات کلیدی**:** رايانش ابري[[1]](#footnote-1)، داده‌ هاي مراقيت‌هاي بهداشتي[[2]](#footnote-2)، رمزگذاري، كليد

فصـل اول

# مقـدمـه

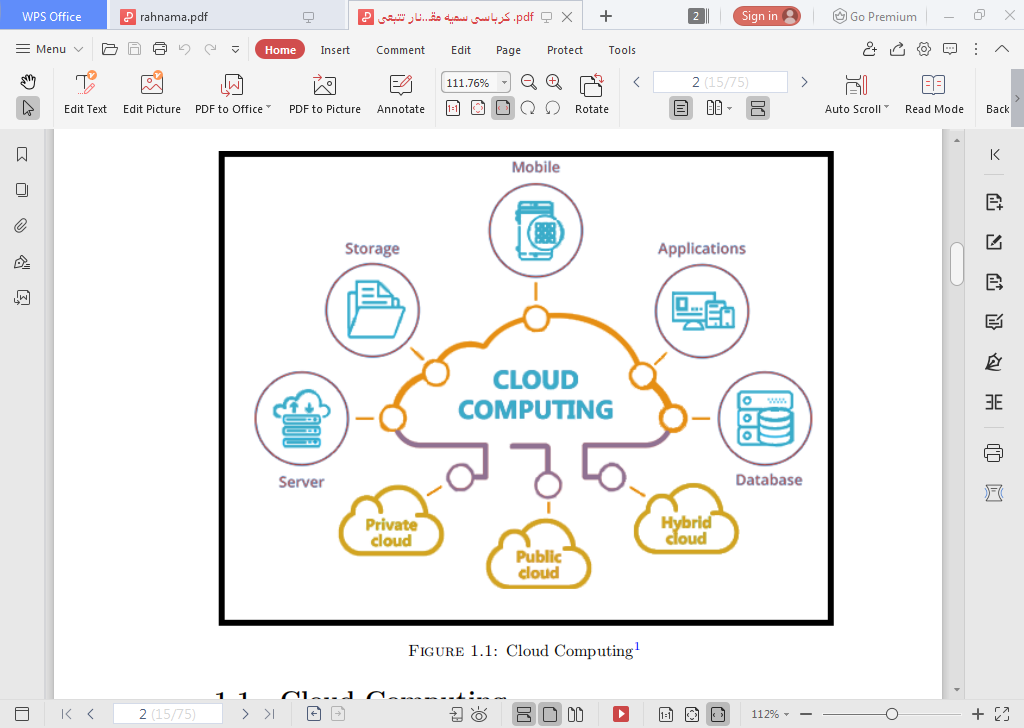
محیط مبتنی بر ابر روز به روز در حال پیشرفت است و بسیاری از سازمان‌ها به سمت محیط ابر تغییر مسیر می‌دهند. به همین ترتیب، بخش مراقبت‌های بهداشتی مبتنی بر فناوری اطلاعات به دلیل مزایایی که دارد، به عنوان مثال در دسترس بودن در هر مکان، هر زمان و منابع اندازه گیری شده، به سمت محیط ابر در حال حرکت است. داده‌های بیمار در قالب الکترونیکی در فضای ابری ذخیره می‌شود. برای مشاوره و درمان بیشتر می‌توان از طریق اینترنت در دسترس بود. بیمار می‌تواند از هر دکتری که در اینترنت در دسترس است؛ از هر نقطه از جهان، مشاور بگیرد. داده‌های دیجیتال بستری را برای پزشکان فراهم می‌کنند که بتوانند بیماران خود را تحت نظر بگیرند. بنابراین با اختراع اینترنت و رایانش ابری، کیفیت خدمات بخش بهداشت و درمان مبتنی بر فناوری اطلاعات نیز روز به روز بهبود می‌یابد. اما حملاتی مانند سرقت اطلاعات محافظت شده/ حساس، DoS 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 و به همین دلیل HIPAA و GDPR برای محافظت از صفات PHI  نقش دارند.( Shah,2020)

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

**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. (Shah,2020)

براي درك مفهوم رايانش ابري شكل 1-1 بسيار مفيد است كه منبع اصلي شكل را در پاورقي ذكر كرده‌ام.



شکل ‏1‑1: رایانش ابری[[3]](#footnote-3)

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.[[4]](#footnote-4)

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. (Gao,Thiebes, Sunyaev,2018)

اين خدمات شامل نرم‌افزار به عنوان سرويس، بسترهاي نرم‌افزاري به عنوان سرويس، زيرساخت به عنوان سرويس مي‌شود كه در مقاله اصلي به آن پرداخته شده است و در اين پايان‌نامه هركدام مختصرا توضيح داده شدهاند.

رمزنگاری، رمزگذاری تبدیل متن ساده به متن مخفی برای ایجاد امنیت بیشتر است. داده‌های ذخیره‌شده بیمار در ابر به حفاظت نیاز دارند و لذا می‌توان با تکنیک‌های رمز گذاری، سطح محرمانگی داده‌های مربوط به بیمار را بهبود بخشید. رمز نگاری از تکنیک‌های ریاضی استفاده می‌کند که مقاله"تاریخچه مختصری از رمزگذاری"[[5]](#footnote-5) به آن پرداخته است؛ این تکنیک‌های بر مبنای کلید است.

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.



شکل ‏1‑2: رمزنگاری استگانوگرافي(Shah,2020)

مقایسه مختصری بین رمزنگاری کلاسیک و مدرن در جدول 1-1 نشان داده شده است.

جدول ‏1‑1 : مقایسه بین رمزنگاری کلاسیک و مدرن(Shah,2020)

|  |  |
| --- | --- |
| **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 |

## ۱-۱ تعريف مسئله و بيان سؤال‌های اصلي تحقيق

*در مورد محرمانگی داده‌های مراقبت‌های بهداشتی ( PHI ) هنگامی که در محیط ابر ذخیره می‌شوند، سیاست‌های درستی باید اعمال شود. این اطلاعات می‌تواند به دلیل ذخیره‌سازی در قالب ساده یا با استفاده از الگوریتم‌های رمزگذاری ضعیف، به خطر بیفتد.*

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

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. *رویکردهای پذیرفته شده در ادبیات كدام است؟*
4. *چگونه می‌توان از روش‌های رمزگذاری مبتنی بر چند لایه برای حفظ محرمانه بودن داده‌های مراقبت‌های بهداشتی استفاده کرد؟*

## 1-2 ضرورت تحقیق

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

1. ضرر مالی و از دست دادن اطلاعات بیمار، مثلا در مورد بیمار ممکن است با سرقت رفتن کارت اعتباری و رمزهای وارد شده در سیستم، پول خود را از دست بدهد.
2. در صورت شکایت بیمار، اعتبار سازمان خدشه دار می‌شود.

*پس موضوع این تحقیق برای مدیریت و پیشگیری از بروز خطرات فوق ضروری است.*

## **۱ – ۳ هدف‌ها**

*هدف اصلی این گزارش ارائه یک الگو و روش مطمئن برای حفظ محرمانگی داده‌های بیماران است. چون داده‌ها، به صورت همیشگی در محیط ابری در دسترس هستند. این امر با رمزگذاری و رمزگشایی داده‌ها به صورت چند لایه به دست می‌آید. الگوریتم‌هایی که برای رمزگذاری استفاده خواهیم کرد؛ الگوریتم‌های استاندارد هستند که توسط NIST توصیه می‌شوند**. در این‌جا هدف استفاده از الگوریتم‌های چندگانه برای حفظ محرمانگی داده‌ها است.*

## 1-4 چه كاربردهايي از انجام اين تحقيق متصور است؟

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

## 1-5 روش و مراحل انجام تحقیق

روش انجام این تحقیق به‌صورت کتابخانه­ای است. منابع مورداستفاده شامل پایان نامه، مقالات، تحقیقات علمی و پژوهشی، کتب و جستجوهای اینترنتی درزمینه‌ی الگوریتم‌های رمزگذاری و حفظ امنیت داده‌های مراقبت بهداشتی است.

در این راستایک پایان‌نامه انتخاب شد (Shah,2020) و با بررسی ساختار پایان نامه و منابع مرجع، توانستم موضوع درک و تجزیه و تحلیل وبیان کنم.

## 1-6 سازمان پایان‌نامه  مورد بررسی

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.( Shah,2020)

## 1-7 ساختار گزارش تحقیق

فصل اول به تعریف و مقدمه و دلایل نیاز به طرح ارائه‌شده پرداخته می‌شود.

فصل دوم به مفاهیم عمومی رمرگذاری پرداخته می شود.

فصل سوم مروری است بر کارهای انجام شده طرح پیشنهادی پایان‌نامه

فصل چهارم به کاربردها و مزایا و معایب الگوریتم‌های رمزگذاری پرداخته می‌شود.

فصل پنجم نیز به جمع‌بندی و نتیجه‌گیری پرداخته می‌شود.

فصـل دوم

# مفـاهیـم عمـومـی رمزگذاری و پيشينه تحقيق

## 2-1 انواع طرح‌های رمزنگاری

*الگوريتم‌هاي رمزگذاري به دو دسته تقسيم مي‌شوند:*

* *رمزگذاری كليد متقارن*
* *رمزگذاری كليد نامتقارن*

### 2-1-1 رمزگذاري متقارن

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

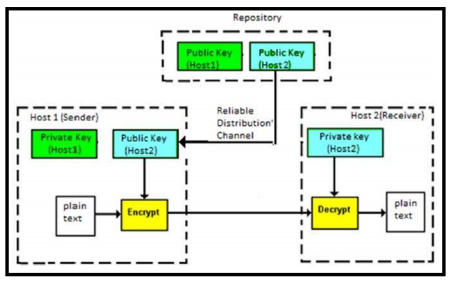
*این کلید دارای ویژگی‌های زیر است:*

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

### 2-1-2 رمزگذاري نامتقارن

*در اين حالت يك فرستنده و يك گيرنده داريم. كليد عمومي براي همه شناخته شده است ولي كليد خصوصي براي رمزگشايي استفاده مي‌شود و داراي ويژگي‌هاي زير است.*

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

**

شکل ‏2‑1:  رمزگذاری نامتقارن کلید[[6]](#footnote-6)

## 2-2 سرویس امنیتی برای رمزنگاری داده‌هاي مراقبت های بهداشتی

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

**محرمانه بودن**

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

**جامعيت**

*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.*

**اعتبار**

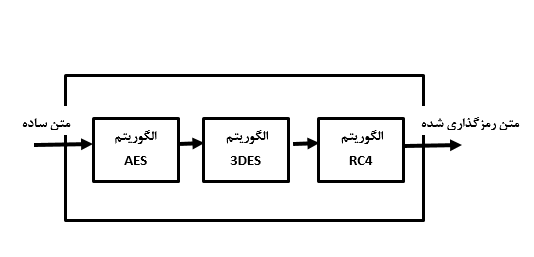
*اصالت اطلاعات را از طرف فرستنده تضمین می‌دهد و به گیرنده اطمینان می‌دهد که اطلاعات دریافتی از کاربران واقعی است که شامل دو نوع است:*

*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.*

## 2-3 رمزگذاری چند لایه

*متن ساده را به یک الگوریتم با کلید منتقل خواهیم کرد و خروجی آن الگوریتم با کلید متفاوت به الگوریتم دوم منتقل می شود. چنین لایه‌هایی می‌توانند شامل دو یا چند الگوریتم باشند. بنابراین، می‌توان به یک سطح محرمانگی دست یافت. شكل 2-2 روش رمزگذاري چندلايه را نشان مي‌دهد.*



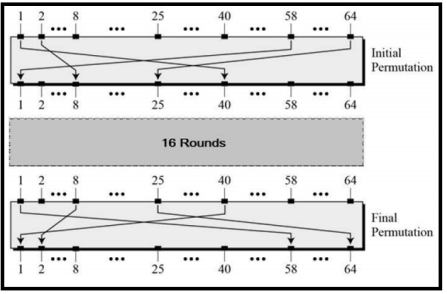
شکل ‏2‑2: روش رمزگذاری چند لایه

## 2-4 کار الگوریتم‌های مورد استفاده در طرح پیشنهادی

*اولين الگوريتمي كه توسط NIST نيز مطرح است و در اين‌جا به آن توجه شده است. استاندارد رمزگذاری داده‌ها(DES) یک الگوریتم متقارن است. پیاده‌سازی الگوريتم DES براساس رمزگذاری فایستل است که در 16 دور انجام می‌شود . اندازه بلوک و اندازه کلید الگوریتم 64 بیت است 56 بیت براي رمزگذاري و 8 بیت اضافه براي مصارف ديگر. از عملیات زیر در DES استفاده می‌شود:*

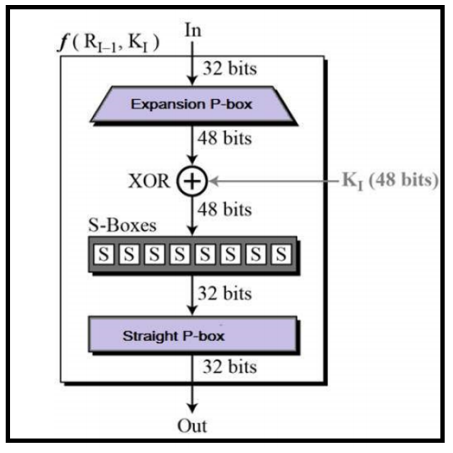
* *جایگزینی اولیه*
* *عملکرد Round*
* *گسترش جعبه جايگشت*
* *توليد كليد*

***جایگشت  اولیه: در شكل 2-3 اين مفهوم نشان داده شده است:***

**

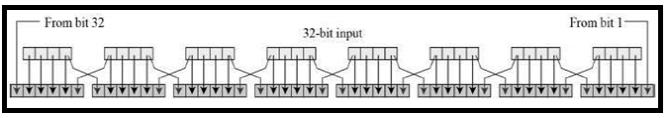
شکل ‏2‑3:  جایگزینی اولیه(Shah,2020)

*عملکرد Round: اين عملکرد يك عملكرد مهم در دور هسته اصلی الگوريتم DES است. همان‌طور كه در شكل 2-4 نمايش داده شده است كلا 48 بيت داريم كه 32 بيت آن در حالت درست هستند.*

**

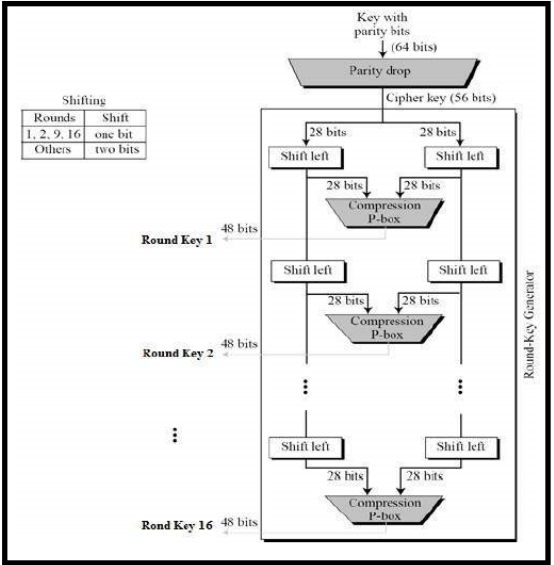
شکل ‏2‑4:  تابع Round(Shah,2020)

*گسترش جعبه جایگشت: توجه داشته باشيد كه کلید دور 48 بیت است و براي ايجاد ورودي 32 بیت از سمت راست آن 48 بیت استفاده مي‌كنيم. در شكل2-5 مفهوم گسترش نشان داده شده است.*

**

شکل ‏2‑5 :   گسترش جعبه جایگزینی[[7]](#footnote-7)

*تولید کلید: بخش نهايي و مهم اين الگوريتم توليد كليد است. تابع Round كه بالاتر مطرح شد؛ 16 بيت كليد را ايجاد مي‌كند كه در پايان نامه با شكل 2-6 به وضوح نشان داده شده است.*

**

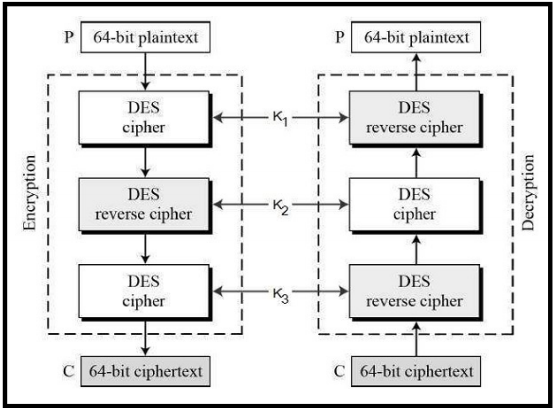
شکل ‏2‑6 :  تولید کلید[[8]](#footnote-8)

*الگوریتم 3DES : فرایند رمزگذاری و رمزگشایی به شرح زیر است:*

* *K1 متن ساده را رمزگذاری می‌کند.*
* *خروجی اول توسط K2 رمزگشایی می‌شود.*
* *و در آخرین مرحله خروجی بلوک دوم دوباره با K3 رمزگشایی می‌شود.*
* *این متن رمز نهایی است.*
* *رمزگشایی فرایند معکوس است.*

*اگر کلیدهای K1 ، K2 ، K3 یکسان استفاده شود، مانند DES کار می‌کند. (Shah,2020)*

*اين الگوريتم در نشان 2-7 نشان داده شده است.*

**

شکل ‏2‑7:  نمودار معماری 3DES [[9]](#footnote-9)

*استاندارد پيشرفته رمزگذاری AES : 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.( Shah,2020)*

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. براي درك بيشتر مطلب، از كتاب پايگاه داده پيشرفته دكتر احمدفراهي استفاده مي‌گنم.*

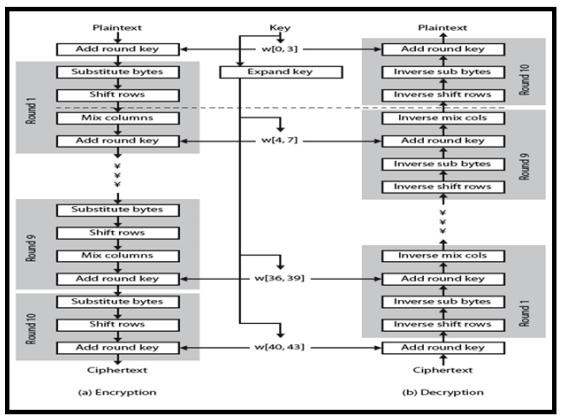
*اين الگوريتم بايت به بايت كار مي‌كند و ورودي اصلي را با كليد رمزنگاري در يك ماتريس جفت مي‌كند.كليد به طريقي تقسيم يا برنامه‌ريزي شده است كه بتواند در مراحل مختلف تكرار به تدريج تزريق شود. اولين قسمت كليد قبل از شروع پروسه‌ي 10 مرحله‌اي تزريق مي‌شود. در هر كدام از اين مراحل، بايت‌ها جابجا مي‌شوند، رديف‌ها نوبت پيدا مي‌كنندو ستون‌ها تركيب مي‌شوند.(فراهي،1398)*

*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.( Shah,2020)*

*ساختار الگوريتم AES در شكل 2-8 نشان داده شده است.*

**

شکل ‏2‑8 :  معماري الگوريتم AES (Shah,2020)

## 2-5 پیشینه تحقیق

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

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

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

در سال 2010 مایکروسافت Azure توسط مایکروسافت منتشر شد.

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

*در سال 2011 دكتر سلیمان و همكاران*[[10]](#footnote-10) *در مقاله‌اي، روش چندلایه‌ای را برای خدمات سلامت الکترونیکی مطابق با سند ISO 17799 تعریف کرده و اطلاعات را به سه دسته اطلاعات سری، بسیار محرمانه و خصوصی تقسیم کرده؛ الگوریتم‌های رمزگذاری متقارن، 3DES و تابع مقدار هش را معرفی کرده‌ اند. نویسندگان از اندازه کلید 193 بیت برای لایه 1 و 129 بیت تا 192 بیت برای لایه 2 و 112 تا 128 برای لایه 3 و 80 تا 111 بیت برای لایه 4 استفاده کرده‌اند. کار اصلی نویسندگان روی الگوریتم 3DES است. و از يك الگوریتم برای رمزگذاری و رمزگشایی استفاده می‌شود.*

*در سال 2013 کیا و همکاران*[[11]](#footnote-11) *در مقاله‌ای با استفاده از SOAP / XML داده‌ها را با AES رمزگذاری کرده اند.*

*در سال 2016 ژو و همکاران*[[12]](#footnote-12) *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 سال 2019 سودهیپ و همکار*[[13]](#footnote-13) *در مقاله‌ای رمزگذاری مبتنی بر ویژگی سیاست رمزگذاری (CP-ABE) را معرفی کرده‌اند. کلید رمزگذاری شامل خط‌مشی‌هایی است و آن‌ها می‌گویند اگر کلید هک شده‌باشد، آن‌دسته از سوابق رمزگشایی می‌شوند که کلید آن‌ها هک می‌شود اما بقیه موارد همچنان محافظت می‌شوند.*

*در سال 2019 هما و همکار*[[14]](#footnote-14)*، درباره روش رمزنگاری منحنی بیضوی بحث کردند و روش‌های تولید کلید اصلی شخص ثالث را معرفی کردند. مالک داده را برای درخواست کلید و رمزگذاری سند به صورت آنلاین به بخش دیگر ارسال می‌کند. شخص ثالث رمز را رمزگذاری و به صاحب داده ارسال و مالک تاریخ را در سرور ابری بارگذاری می‌کند و کلید را برای استفاده در آینده نگه می‌دارد.*

*در سال 2019 پارا و همکاران*[[15]](#footnote-15) *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 سال 2019 وزيد و همكاران*[[16]](#footnote-16) *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.*

فصـل سـوم

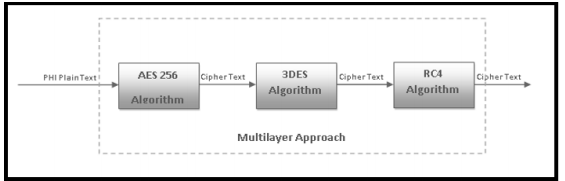
# مروری بر کارهای انجام‌شده

## 3-1 مقدمه

*در فصل 3 پایان‌نامه مورد بررسی راه‌اندازی آزمایشی طرح پیشنهادی مدنظر قرار گرفته شده؛ روش‌های پیشنهادی را تجزیه و تحلیل کرده؛ طرح اخیر بر مفاهیم و اصول رمزگذاری و رمز گشایی متمرکز است. طرح پیشنهادی با الگوریتم چندلایه رمزگذاری، داده‌های PHI را رمزگذاری و محافظت می‌کند. داده‌های رمزگذاری شده در سرور ابری قابل اعتماد که احتمالا مورد نیاز بیمار در آینده، در دسترس خواهد بود. با استفاده از معماری کلاینت/ سرور و از طریق شبکه منتقل شود، طرح فوق توسعه داده شده است و در فصل4 پایان‌نامه مورد بررسی، طرح پیشنهادی تجزیه و تحلیل می‌شویم که در ادامه به تفکیک توضیح ميدهم.*

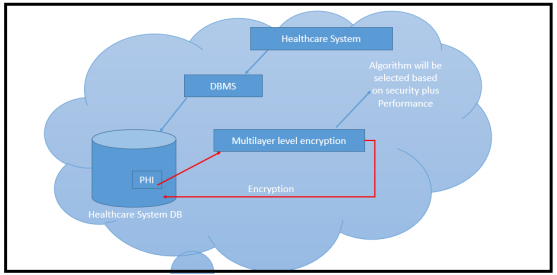
## 3-2 راه‌اندازی آزمایشی طرح پیشنهادی

*ابتدا به تکنیک چندلایه رمزگذاری ( شکل3-1) توجه کنید؛ در این حالت متنی که باید محافظت شود؛ وارد سیستم الگوریتم چندگانه می‌شود. داخل سیستم الگوریتم چندگانه در این مورد خاص، 3 الگوریتم AES و 3DES و RC4 وجود دارد. خروجی هر الگوریتم، به صورت رمزگذاری شده و دوباره توسط الگوریتم بعدی طبق شکل، رمزگذاری می‌شود و خروجی نهایی با رمزگذاری چندلایه و ایمنی بالا ایجاد می‌شود.*

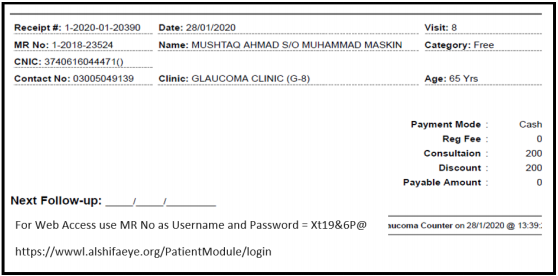
**

شکل ‏3‑1: تکنیک محافظت از چند لایه (Shah,2020)

*برای توسعه طرح یک مجموعه داده ساختگی( برای ایمنی بیمار) از حدود 500 بیمار انتخاب کرده؛ شکل 3-2 یک سیستم مراقبت‌های بهداشتی به همراه سیستم مدیریت پایگاه‌داده را نشان می‌دهد. روی داده‌ها، الگوریتم‌های رمزگذاری موجود در RDBMS اعمال می‌شوند و داده‌ها در محیط ابری ذخیره می‌شوند.*



شکل ‏3‑2:  نمودار معماری روش‌شناسی(Shah,2020)

**

شکل ‏3‑3:  فیش ورود به سیستم برای بیمار (Shah,2020)

*در آغاز ثبت نام بیماران، شماره MR با رمز عبور پیچیده‌ای که به طور تصادفی ایجاد شده است، برای اطلاعات بیمار اختصاص می‌یابد. برای دسترسی در وب سایت( شکل 3-3 )، 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. کلید در RDBMS ذخیره می‌شود و توسط سرور Microsoft SQL محافظت می‌شود و از رمز عبور محافظت می‌کند. بنابراین برای رمزگذاری و رمزگشایی نیازی به ارائه رمز برای رمزگذاری و رمزگشایی بیمار نیست.( Shah,2020)*

### 3-2-1 فرآیند رمزگذاری و رمزگشایی در RDBMS

*فرایند رمزگذاری کلی با استفاده از SQL Server بر روی يك ستون از یک جدول در شکل 3-4 نشان داده شده است. کلید اصلی در پایگاه‌داده، براساس روش متقارن محافظت می‌شود.*

**مرحله 1 :  ایجاد کلید اصلی**

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

**مرحله 2 : ایجاد گواهی**

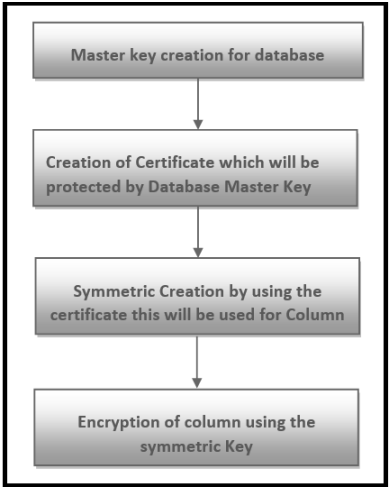
*گواهینامه دیجیتالی جهت محافظت از کلید اصلی پایگاه‌داده ایجاد می‌شود.*

**مرحله 3 : ساخت کلید متقارن**

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

**مرحله 4 : رمزگذاری ستون‌ها**

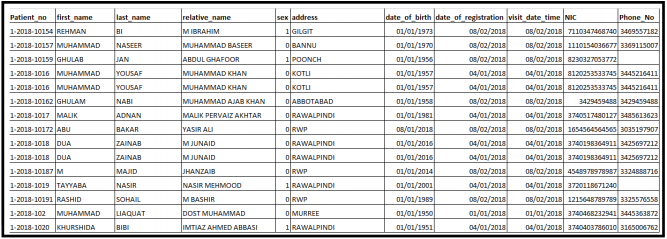
*شمای جدول و فیلدهای را رمزگذاری می‌کنیم.*

**

شکل ‏3‑4 : فرآیند رمزگذاری کلی(Shah,2020)

## 3-3 تجزیه و تحلیل طرح پیشنهادی

*ما یک مجموعه داده ساختگی از 500 بیمار را برای هدف‌ آزمایش آماده کرده‌‌ايم. نمونه مجموعه داده در شکل3-5 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.( Shah,2020)*

**

شکل ‏3‑5 : نمونه مجموعه داده‌های ساختگی(Shah,2020)

## 4-3 نصب پیکربندی سخت‌افزار و نرم‌افزار

### 3-4-1 سخت‌افزار مورد نياز

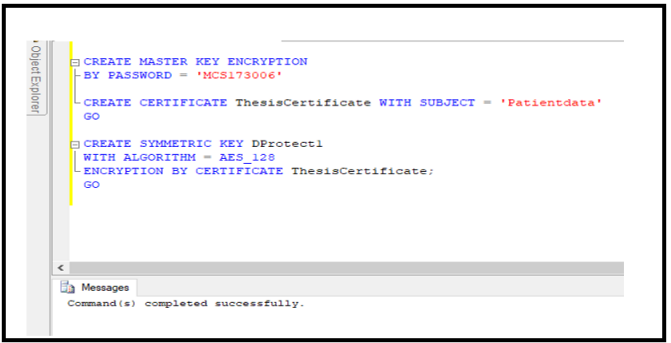
* *پردازنده Intel Core i7-6500U Processor*
* *Ram 8 گیگابایتی*
* *هارد دیسک 500 گیگابایتی*

### 3-4-2 سیستم عامل و نرم‌افزار مورد نیاز

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

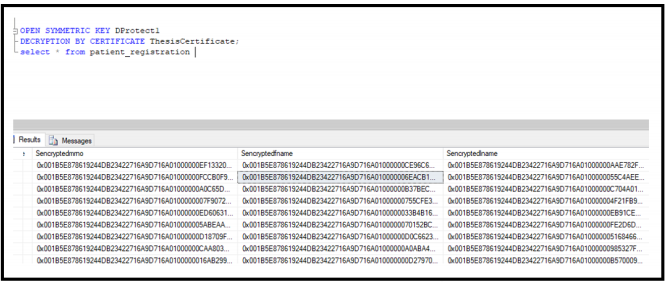
## 3-5 ایجاد کلیدها و گواهینامه‌ها و رمزگذاری داده‌ها

ایجاد کلید و گواهینامه‌ها با دستورات SQL و مطابق شکل 3-6 انجام می‌شود.

**

شکل ‏3‑6 : ایجاد کلیدها و گواهینامه‌ها(Shah,2020)

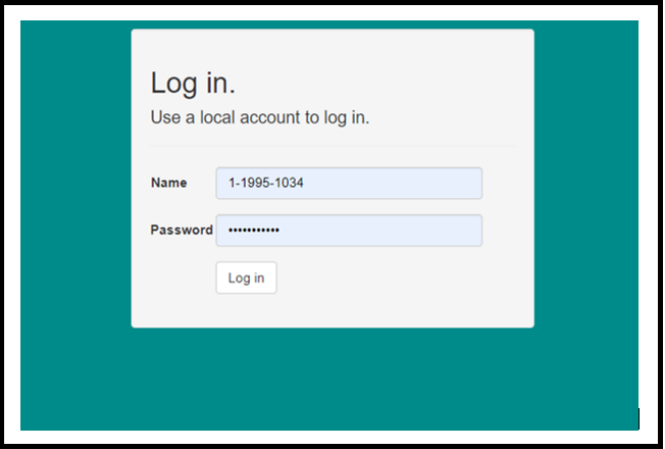
*داده‌های مربوط به بیمار که باید روی ابر بارگذاری شوند؛ تهیه شده و فرآیند رمزگذاری روی آن اعمال می‌شود. داده‌ها در جدول پایگاه‌داده با فرمت شکل 3-7، ذخیره می‌شوند.*

**

شکل ‏3‑7 : فرم رمزگذاری شده داده‌ها(Shah,2020)

## 3-6 رمزگشایی داده‌ها

*بیمار وارد سایت مورد نظر می‌شود که در برگه ثبت نام چاپ شده است و از شماره پرونده پزشکی به عنوان نام کاربری و رمز عبور استفاده می‌کند و بر روی ورود کلیک می‌کند. ورود بیمار در شکل 3-8  و جزئیات پرونده پزشکی بیمار در شکل 3-9 نشان داده شده است.*

**

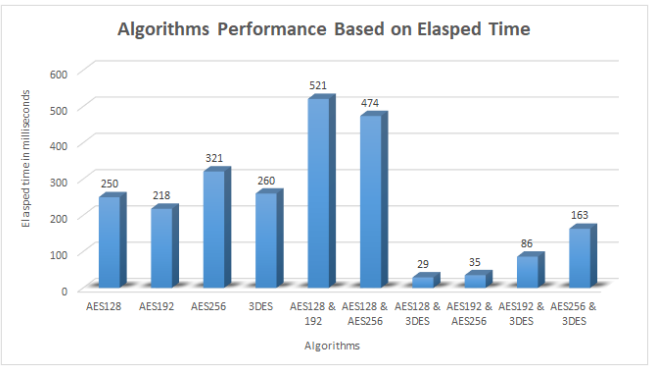
شکل ‏3‑8 :  صفحه ورود به سیستم برای ورود بیمار(Shah,2020)

**

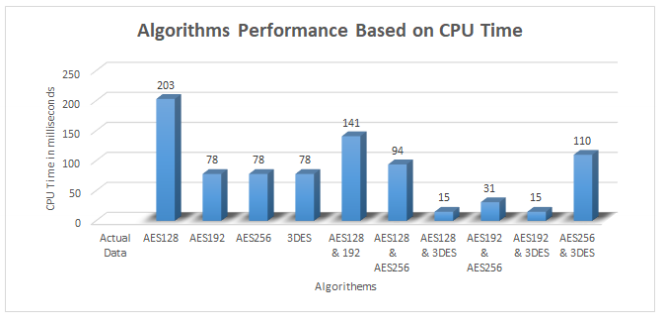
شکل ‏3‑9 : جزئیات پرونده پزشکی یک بیمار(Shah,2020)

## 3-7 تحلیل نتایج

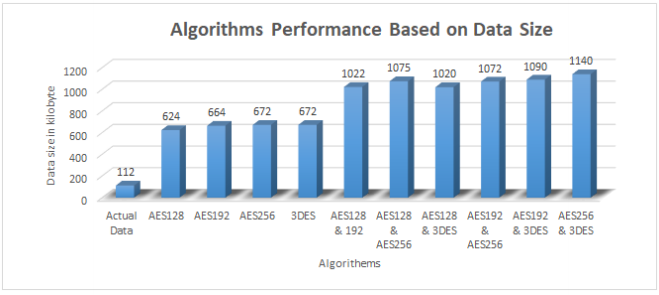
*در این بخش نتایج بدست آمده با روش‌های مختلف مقایسه می‌شود. نمودارهای زیر در شکل 3-10 و شکل 3-11 و شکل 3-12؛ نتایج زمان سپری شده، زمان پردازنده و ظرفیت ذخیره‌سازی داده‌های الگوریتم‌های رمزگذاری شده مختلف را نشان می‌دهد.*

**

شکل ‏3‑10 :  نمای گرافیکی زمان سپری شده الگو (Shah,2020)

**

شکل ‏3‑11 :  نمای گرافیکی زمان CPU زمان الگوریتم رمزگذاری چندلایه و منفرد(Shah,2020)

**

شکل ‏3‑12 :  نمای گرافیکی اندازه جدول پایگاه داده بعد از ذخیره‌سازی(Shah,2020)

* *اگر الگوریتم رمزگذاری منفرد AES با اندازه کلید 128 بیتی اعمال شود، کل زمان سپری شده 250 میلی‌ثانیه خواهدبود.*
* *اگر AES با اندازه کلید 192 بیتی اعمال شود، کل زمان سپری شده 21 میلی‌ثانیه خواهد ‌بود.*
* *اگر AES با اندازه کلید 218 بیتی اعمال شود، کل زمان سپری شده 321 میلی‌ثانیه خواهد بود.*
* *اگر 3DES به تنهایی اعمال شود، کل زمان سپری شده 260 میلی‌ثانیه خواهد بود.*

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

* *اگر ترکیبی از AES128 و 192 استفاده شود؛ زمان سپری شده 521 میلی‌ثانیه خواهد بود.*
* *اگر ترکیبی از AES128 و 256 استفاده شود؛ زمان سپری شده 474 میلی‌ثانیه خواهد بود.*
* *اگر ترکیبی از AES128 و 3DES استفاده شود، زمان سپری شده 29 میلی‌ثانیه خواهد بود.*
* *اگر ترکیبی از AES192 و AES256 استفاده شود، مدت زمان سپری شده 35 میلی ثانیه خواهد بود.*
* *اگر ترکیبی از AES192 و 3DES استفاده شود، مدت زمان سپری شده 86 میلی‌ثانیه خواهد بود.*
* *اگر ترکیبی از AES256 و 3DES استفاده شود، مدت زمان سپری شده 163 میلی ثانیه خواهدبود.*

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

* *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 مناسب است.*

فصـل چهارم

# کاربرد الگوريتم‌هاي چندگانه رمزگذاري روي داده‌هاي مراقبت بهداشتي-مزایا و معایب

## 4-1 مقدمه

*حفاظت از اطلاعات بیمار به دلیل نياز به امنیت و نگهداري آن‌ها درفضاي مناسب جهت استفاده احتمالي بيمار در آينده مسئله مهمي است كه امروزه به‌عنوان علم روز و تكنولوژي جديد مورد نياز بيمارستان‌ها و مراكز مربوطه است. تکنیک‌های معرفی شده در چارچوب ادبیات بررسی شد. یافتن تکنیک جدید نیاز به دقت و تست دارد. تکنیک‌های رمزگذاری چند لایه می‌توانند برای محافظت از داده‌های بیمار مفید باشند. این رویکرد مدل رمزگذاری چند لایه برای داده‌های مراقبت‌های بهداشتی در محیط ابر بر روی داده‌های بیمار اعمال شده و اثرات آن مورد تجزیه و تحلیل قرار گرفت.*

## 4-2 دستورالعمل‌های موجود

**قانون HIPAA و GDPR**

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

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

* *نام و نام خانوادگی بیمار*
* *آدرس شامل کد پستی، شهر، کشور*
* *همه تاریخ‌ها*
* *شماره تلفن*
* *نمابر*
* *شناسه ایمیل*
* *SSNo (شماره بيمه)*
* *سوابق پزشکی شماره*
* *اطلاعات کارت سلامت*
* *حساب بانکی بدون/ اطلاعات کارت اعتباری*
* *گواهینامه یا گواهینامه رانندگی*
* *شماره خودرو*
* *شناسه دستگاه و شماره سریال*
* *آدرس وب*
* *آدرس پروتکل اینترنت (IP)*
* *بیومتریک*
* *هر نوع تصویری*
* *هر مشخصه دیگری که بتواند منحصراً فرد را شناسایی کند.(* Sulaiman, Sharma, Ma, Tran,2011*)*

*GDPR* *(مقررات عمومی حفاظت از داده ها) مقررات اتحادیه اروپا است که در سال 2016 پذیرفته شده است. پس از سال 2018 این قانون برای کلیه سازمان های کشورهای اتحادیه اروپا اجباری شده است که ذخيره اطلاعات شخصی فرد را باید مطابق با GDPR باشد.(* Sudheep,Joseph,2019*)*

## 4-3 آینده کار

*در ادامه كار و جهت پيشرفت‌هاي بيشتر مي‌توان روي موضوعات زير كار كرد*

* *انتخاب الگوریتم رمزگذاری به صورت تصادفی*
* *استانداردهای الگوریتم بیشتری اضافه شود.*
* *افزایش سرعت رمزگذاری*
* *پیاده سازی الگوریتم‌های چند لایه روی داده‌های مبتنی بر تصویر (*
* *Shah,2020)*

## 4-4 مزایا و معايب استفاده از تکنیک‌های پیشنهادی

### 4-4-1 مزايا

* *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.( Shah,2020)*

### 4-4-2 معايب

*معايبي كه وجود دارد در برابر مزايا، ارزش هزينه و زمان را دارد. مشخص است كه تركيب چند الگوريتم با اينكه مي‌تواند سطح محرمانگي و سرعت را بالا ببرد ولي در مواردي ممكن است سرعت و پيچيدگي كار به نسبت وجود يك الگوريتم بالا رود كه به مراتب خدمات و قدرت بالاتري خواهد داشت و لذا ارزش آن را دارد. تنها مي‌توان بهترين تركيب چند لايه را تست كرد كه تلاش اين پايان‌نامه همين بوده است . همچنين يكي از كمبودهايي كه مينواند در ادامه كار پايان‌نامه و در جايي ديگر رفع شود؛ به نظر من توجه بيشتر به داده‌هاي تصويري و ... است كه بايد امنيت بيشتري داده باشند.*

## 4-5 پاسخ به سوالات تحقیق

اکنون می‌توان با توجه به مطالب بیان شده به سوالات که فصل اول این گزارش مطرح شده بود؛ پاسخ داد

**جواب سوال 1:** انواع الگوریتم متقارن و نامتقارن و غیره رمزگذاری وجود دارد.

**جواب سوال 2:** هر کدام معایب و مزایای خاص خود در زمینه‌های مختلف داشته که در جدول زیر این مقایسه‌ها ذکر می‌شود.

جدول ‏4‑1 : مفایسه الگوریتم‌های منفرد و ترکیبی 3DES و AES256(Shah,2020)

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

**جواب سوال3 :** الگوریتم‌های DESوAESو3DES و ترکیب این الگوریتم‌ها به عنوان یک الگوریتم چندلایه که امنیت بالاتر را ایجاد کند.

**جواب سوال 4:** با توجه به مقایسات مطرح شده باید از چند الگوریتم رمزگذاری که ترکیب آن‌ها با یکدیگر بیشترین مزایا و کمترین معایب را داشته باشد؛ استفاده کرد. ورودی به سیستم الگوریتم رمزگذاری چندلایه، همان متن ساده است که لازم است برای استفاده مجدد در آینده و ذخیره‌سازی روی فضای ابری رمزگذاری شود و در الگوریتم، رمزگذاری متناسب انجام و به عنوان ورودی الگوریتن بعدی داده می‌شود و درنهایت خروجی نهایی، تحویل داده می‌شود.

## 4-6 جمع ­بندی

الگوريتم‌هاي چند لايه بررسي شده در اين پايان‌نامه داراي كارايي موثر بوده‌اند. هر چند معايبي مانند سرعت دارند كه باز به توجه به مزايا و بخصوص محرمانگي بيشتر به صرفه است. مي‌توان براي بالارفتن سرعت از استاندردهاي ديگري در ادامه كار استفاده كرد و آن را تست نمود. مطلبي ديگر كه در اين پايان نامه زياد تاكيد نشده؛كار الگوريتم‌هاي رمزگذاري چندگانه روي داده هاي تصوير و ... است كه نياز به كار بيشتر دارد.

فصـل پنجم

# جمع‌بندی و پیشنهاد­ها

## 5-1 مقدمه

در این بخش به نتایج حاصل از تحقیق با توجه به استفاده از الگوريتم‌هاي رمزگذاري چندگانه روي داده‌هاي مراقبت‌هاي بهداشتي، به نتیجه‌گیری و ارائه پیشنهاد در خصوص بهبود طرح پرداخته می‌شود. و نهایتاً نتیجه‌گیری بر اساس مزایا و قابلیت‌های طرح مذکور ارائه می‌گردد.

## ۵ – 2 نتایج حاصل از تحقیق

​در كل و به عنوان نتيجه تحقيق، 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. 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. به دلیل ترکیب کلید، سطح اطمینان نیز افزایش می‌یابد زیرا داده‌ها با چندین کلید رمزگذاری می‌شوند. در نتیجه، روش چند لایه به دلیل رمزگذاری لایه ای از سرعت کمی برخوردار است اما از نظر محرمانه بودن از سطح بالایی برخوردار است.( Shah,2020)

## 5-3 پيشنهادها

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

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

*موردی که جای کار بیشتر دارد و مورد نیاز است توجه به داده‌های غیرمتنی بیمار است که با تکنیک‌های بروز رمزگذاری، ایمن‌تر باشند.*

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

## 5-4 ارائه ایده برای پایان‌نامه‌های جدید تکمیلی

* بررسی و تست بهترین ترکیب الگوریتم‌های رمزگذاری از لحاظ سرعت،هزینه،کارایی و ... روی داده‌های مراقبت‌های بهداشتی برای رسیدن به مطلوب‌ترین نتیجه
* پیاده‌سازی الگوریتم‌های رمزگذاری بومی ایران روی داده‌های مراقبت‌های بهداشتی
* رمزگذاری چندلایه کارا روی داده‌های تصویری مراقبت‌های بهداشتی
* ساخت برنامه امنیتی Open Source رمزگذاری چند لایه روی انواع سیستم ها

## 5-5 جمع‌بندی و نتیجه‌گیری

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

این گزارش شامل 5 فصل است. فصل اول به تعریف و مقدمه، فصل دوم مفاهیم عمومی رمرگذاری، فصل سوم مروری است بر کارهای انجام شده طرح پیشنهادی پایان‌نامه، فصل چهارم کاربردها و مزایا و معایب الگوریتم‌های رمزگذاری و فصل پنجم نیز جمع‌بندی و نتیجه‌گيري نهايي است

پس ار درك موضوع و تجزيه و تحليل آن‌ها در راستاي ادامه كار موضوعات پيشنهادي بيان شد و به خصوص جهت بومي‌سازي اين طرح در ايران پيشنهادهايي مطرح شد.

# مراجع

* فراهي، احمد. (1398). «پايگاه داده پيشرفته» ،تهران: دانشگاه پيام‌نور 400 ص
* Babatunde, A. O., A. J. Taiwo, and E. G. Dada., “Information Security in Health Care Centre Using Cryptography and Steganography.,” arXiv preprint arXiv:1803.05593,2018.
* T. M. Damico, “A brief history of cryptography,” Inquiries Journal, vol. 1, no. 11, 2009.
* F. Gao, S. Thiebes, and A. Sunyaev, “Rethinking the meaning of cloud computing for health care: A taxonomic perspective and future research directions,” Journal of medical Internet research, vol. 20, no. 7, p. e10041, 2018.
* 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.
* M. M. Kiah, M. S. Nabi, B. Zaidan, and A. Zaidan, “An enhanced security solution for electronic medical records based on aes hybrid technique with soap/xml and sha-1,” Journal of medical systems, vol. 37, no. 5, p. 9971, 2013.
* [Outright Systems](https://medium.com/@outrightsystems?source=post_page-----ab19f308221d--------------------------------).(2019). Cloud Computing in Business Retrieved from <https://medium.com/@outrightsystems/cloud-computing-in-business-ab19f308221d>
* 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
* H.A.Shah. (2020). “A Multilayer Encryption Model To Protect Healthcare Data in Cloud Environment”. (Unpublished master’s thesis). University of Islamabad
* K. Sudheep and S. Joseph, “Review on securing medical big data in healthcare cloud,” in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*. IEEE, 2019, pp. 212–215
* 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.
* Vrema.sushil.(2019). characteristics-of-cloud-computing-as-per-nist Retrieved <https://timesofcloud.com/cloud-tutorial/characteristics-of-cloud-computing-as-per-nist>
* M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. Rodrigues, “Authentication in cloud-driven iot-based big data environment: Survey and outlook,” Journal of Systems Architecture, vol. 97, pp. 185-196, 2019.
* Z. Yan, R. H. Deng, and V. Varadharajan, “Cryptography and data security in cloud computing,” 2017
* 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.

# واژه‌نامه

**واژه‌نامه فارسی به انگلیسی**

|  |  |
| --- | --- |
| ارتباط | Communication |
| تاريخچه | History |
| تركيب | Combination |
| چندلايه | Multilayer |
| رايانش ابري | Cloud computing |
| رمزگذاري | Cryptography |
| متقارن | Symmetric |
| مراقبت‌هاي بهداشتي | Healthcare |
| معماري | Architecture |
| هزينه | Cost |

**واژه‌نامه انگلیسی به فارسی**

|  |  |
| --- | --- |
| معماري | Architecture |
| رايانش ابري | Cloud computing |
| تركيب | Combination |
| ارتباط | Communication |
| هزينه | Cost |
| رمزگذاري | Cryptography |
| مراقبت‌هاي بهداشتي | Healthcare |
| تاريخچه | History |
| چندلايه | Multilayer |
| متقارن | Symmetric |

## **Abstract**

This is the era of cloud computing and it has become an integral part for any

organization. It is equally suitable for all the organizations e.g. education, gov

ernment, public sector, health care department. Main features of cloud computing

are broad network, shared resources, rapid elasticity and pay per use. Cloud com

puting is also providing highly potential services to IT based healthcare sector. In

cloud computing model a patient can get consultancy from any doctor available

in the world. There are two types of patient information i.e. protected/sensi

tive health information and general information. Protected information (Phone

no, ATM, Security no, MR no etc.) requires more confifidentiality as compared

to general information. Therefore, for some protected health information without

patient association (general disease name, symptoms) will be very helpful for re

search experiments. Health information is protected by achieving confifidentiality,

integrity and availability, when data is stored in cloud environment.

There can be many types of attacks possible on protected health information

stored on cloud e.g. if patient credit card information is hacked by a hacker than

he may lose his all money. Similarly, if the disease information of a celebrity

is leaked out than he/she may lose the career. Thats why protected/sensitive

information requires protection in cloud environment. Cryptography methods

provide difffferent techniques to protect the data stored in cloud environment. In

this thesis, we have suggested a multilayer encryption technique to ensure the

confifidentiality of data stored in cloud environment. This suggested technique

will improve the security of cryptographic techniques when used in multilayered

format. We have set up a local system for the experiment. We have used the

RDBMS (Microsoft SQL Server) and Framework 4.5. A set of 500 dummy patient

records is used to test the proposed techniques. The experiment was performed

to check the confifidentiality of the suggested techniques. This experiment shows

us that multilayer encryption techniques is more suitable for public health sectors

when data is in cloud environment.

**Keywords**

Cloud computing , healthcare , Encryption , key

****

**Payam Noor University**

**Department of Computer Engineering and Information Technology**

**Seminar Report (M.Sc)**

Title:

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

**Supervisor:**

**Dr. Ali Razavi**

**By:**

**Somayeh Karbasy**

August 2021

1. Cloud computing [↑](#footnote-ref-1)
2. healthcare [↑](#footnote-ref-2)
3. <https://medium.com/@outrightsystems/cloud-computing-in-business-ab19f308221d> [↑](#footnote-ref-3)
4. [https://timesofcloud.com/cloud-tutorial/characteristics-of-cloud-computing-as-per-nist](https://timesofcloud.com/cloud-tutorial/characteristics-of-cloud-computing-as-per-nist/) [↑](#footnote-ref-4)
5. **T. M. Damico, “A brief history of cryptography,” Inquiries Journal, vol. 1, no. 11, 2009.**  [↑](#footnote-ref-5)
6. https://www.tutorialspoint.com/cryptography/cryptosystems.htm/ [↑](#footnote-ref-6)
7. 7https://www.tutorialspoint.com/cryptography/cryptosystems.htm [↑](#footnote-ref-7)
8. https://www.tutorialspoint.com/cryptography/cryptosystems.htm [↑](#footnote-ref-8)
9. https://www.tutorialspoint.com/cryptography/cryptosystems.htm [↑](#footnote-ref-9)
10. R.sulaiman.D.Sharma,W.Ma and D.Tran [↑](#footnote-ref-10)
11. M.M.Kian,M.S.Nabi,B.Zaidan and A.Zaidan [↑](#footnote-ref-11)
12. L. Zhou, V. Varadharajan, and K. Gopinath [↑](#footnote-ref-12)
13. K.Sudheep and Joseph [↑](#footnote-ref-13)
14. V.S.V Hema and R.Kesavan [↑](#footnote-ref-14)
15. S. A. Parah, A. Bashir, M. Manzoor, A. Gulzar, M. Firdous, N. A. Loan, and J. A. Sheikh [↑](#footnote-ref-15)
16. M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. Rodrigues [↑](#footnote-ref-16)