بسم الله الرحمن الرحیم

ارائه سمینار تحقیق و تتبع نظری

عنوان سمینار:

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

ارائه سمینار تحقیق و تتبع نظری

استاد راهنما:

دکتر سیدعلی رضوی

نگارنده:

سمیه کرباسی راوری

تابستان ۱۴۰۰

ارائه سمینار تحقیق و تتبع نظری

فهرست

تعریف مسئله و اهداف تحقیق

تعریف مسئله

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.

اهداف تحقیق

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.

نکته

NIST

The National Institute of Standards and Technology

به معنای

موسسه ملی استاندارد و فناوری

در ایالات متحده آمریکا

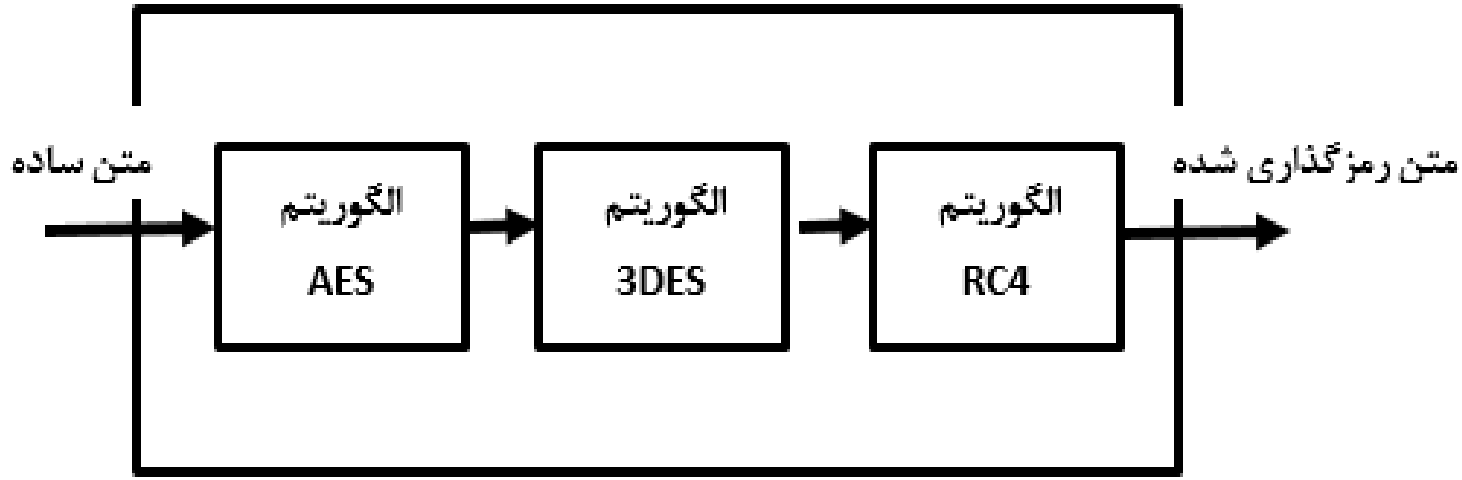
ارائه سمینار تحقیق و تتبع نظری

مقدمه و بررسی مفاهیم

سرویس امنیتی برای رمزنگاری داده‌های مراقبت های بهداشتی

- محرمانه بودن
- جامعیت
- اعتبار

رمزگذاری چندلایه



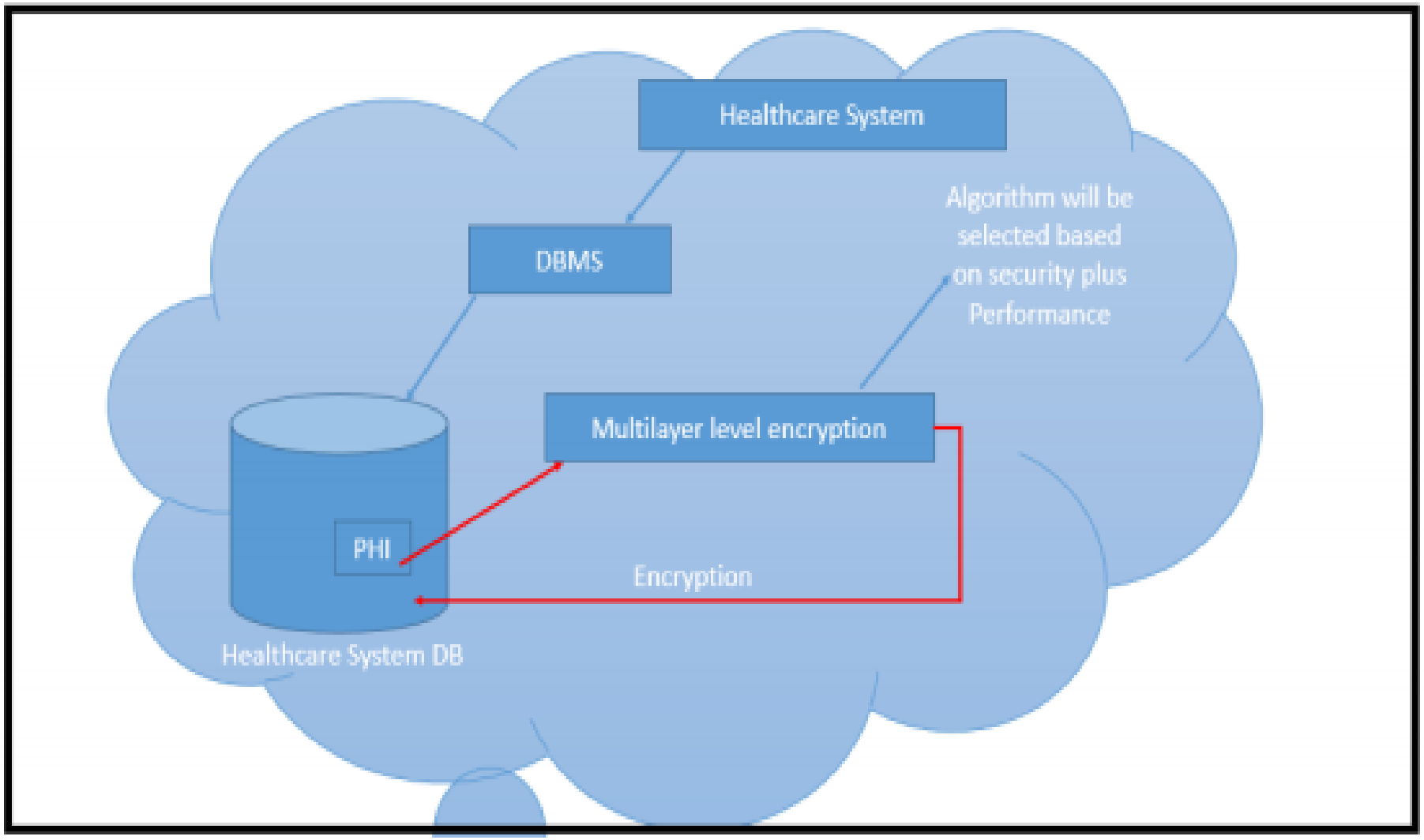
مروری بر کارهای انجام شده در پایان‌نامه

ارائه سمینار تحقیق و تتبع نظری

راه‌اندازی آزمایشی طرح پیشنهادی

برای توسعه طرح یک مجموعه داده ساختگی(برای ایمنی بیمار) از حدود ۵۰۰ بیمار انتخاب کرده؛ اسلاید بعد 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.



ارائه سمینار تحقیق و تتبع نظری

فیش ارائه شده به بیمار
MR no , password , address

Receipt #: 1-2020-01-20390 **Date:** 28/01/2020 **Visit:** 8

MR No: 1-2018-23524 **Name:** MUSHTAQ AHMAD S/O MUHAMMAD MASKIN **Category:** Free

CNIC: 3740616044471()

Contact No: 03005049139 **Clinic:** GLAUCOMA CLINIC (G-8) **Age:** 65 Yrs

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

Next Follow-up: _____/_____/_____

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

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

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

نکته

MR no

Medical Record no

Password

رمز تصادفی پیچیده

Web Address

آدرس

اساس الگوریتم چند لایه پایان‌نامه

الگوریتم رمزگذاری متقارن *AES* را با ترکیب کلیدهای مختلف و *3DES* بر روی داده‌ها اعمال می‌کنیم

کلید در *RDBMS* ذخیره می‌شود و توسط سرور *Microsoft SQL* محافظت می‌شود و از رمز عبور محافظت می‌کند.

فرآیند رمزگذاری و رمزگشایی در RDBMS

مرحله ۱ : ایجاد کلید اصلی

مرحله ۲ : ایجاد گواهی (جهت محافظت از کلید اصلی)

مرحله ۳ : ساخت کلید

مرحله ۴ : رمزگذاری ستون‌ها

سخت‌افزار مورد نیاز

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

سیستم عامل و نرم‌افزار مورد نیاز

- ویندوز ۱۰ یا بالاتر
- *Visual Studio* ۱۲ یا ۱۵
- *SQL Server 2014* یا بالاتر
- *Framework* ۴.۵

ارائه ایده برای ادامه کار

- 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

باتشکر از توجه شما