###### 28

###### آزاد.jpeg

###### دانشگاه آزاد اسلامي

###### واحد تهران مرکز

**موضوع:**

**امنیت پایگاه‌ داده، رمزنگاری، طراحی سیستم و بررسی موانع**

**فهرست مطالب**

[فصل 1 كليات 3](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310516)

[فصل 2 امنيت كلاسيك 6](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310517)

[2-1 مقدمه 6](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310518)

[2-2 امنیت پایگاه‌ داده 7](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310519)

[2-3 تهدید امنیت در پایگاه داده 7](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310520)

[2-4 کنترل امنیت پایگاه داده 8](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310521)

[2-4-1 کنترل انتشار 8](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310522)

[2-4-2 کنترل استنباط 8](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310523)

[2-4-3 کنترل دسترسی 9](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310524)

[2-4-3-1 ارتباط کنترل دسترسی با سایر سرویس‌های امنیتی 12](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310525)

[2-4-3-2 ماتریس دسترسی 14](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310526)

[2-4-3-3 سیاست‌های کنترل دسترسی 15](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310527)

[2-4-3-3-1 سياست تشخیص 16](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310528)

[2-4-3-3-2 سیاست اجباری 18](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310529)

[2-4-3-3-3 سیاست مبتنی بر نقش 22](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310530)

[2-5 مديريت تفويض اختيار 24](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310531)

[2-6 جمع‌بندي 25](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310532)

[فصل سوم بررسي امنيت در نرم‌ افزار SQLServer2005 26](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310533)

[3-1 مقدمه 26](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310534)

[3-2 هویت شناسی 27](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310535)

[3-2-1 مد هویت شناسی ویندوزی (WAM) 27](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310536)

[3-2-2 مد ترکیبی (MM) 28](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310537)

[3-3 Logins 30](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310538)

[3-3-1 Login‌های ویندوز و کاربران پایگاه‌داده 30](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310539)

[3-3-1-1 ایجاد گروه در ویندوز 30](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310540)

[3-3-1-2 ارتباط گروه‌های ویندوز با کاربران SQLServer با استفاده از GUI 32](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310541)

[3-3-1-3 ارتباط گروه‌های ویندوز با کاربران SQLServer با استفاده از کد‌های T-SQL 36](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310542)

[3-3-2 Login‌های سرویس دهنده و کاربران پایگاه‌داده 38](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310543)

[3-3-2-1 ایجاد Login در سطح سرویس دهنده با استفاده از GUI 38](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310544)

[3-3-2-2 ایجاد Login در سطح سرویس دهنده با استفاده از کد T-SQL 40](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310545)

[3-3-3 Sa Login 40](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310546)

[3-4 کنترل دسترسی(Access Control) 41](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310547)

[3-5 نقش‌ها 42](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310548)

[3-5-1 نقش‌های ثابت سرویس دهنده (FSR) 42](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310549)

[3-5-2 نقش‌های پایگاه‌داده‌ای (DBR) 44](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310550)

[3-5-3 نقش‌های برنامه‌ای (APR) 50](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310551)

[3-6 شِما 53](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310552)

[3-7 Principal 55](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310553)

[3-8 Securable 56](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310554)

[3-9 Permission 57](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310555)

[3-10 رمز نگاری 60](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310556)

[3-10-1 رمزنگاری با استفاده از کلمه عبور کاربر 61](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310557)

[3-10-2 رمزنگاری کلید متقارن 62](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310558)

[3-10-3 رمزنگاری کلید نامتقارن 63](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310559)

[3-10-4 رمزنگاری با استفاده از گواهینامه 64](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310560)

[3-11 جمع بندي 66](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310561)

[فصل چهارم طراحي سيستم پرسنلي 67](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310562)

[4-1 مقدمه 67](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310563)

[4-2 UseCase 68](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310564)

[4-2-1 شرح UseCase 68](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310565)

[4-3 نمودار توالی 70](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310566)

[4-4 Class Diagram 74](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310567)

[4-5 واژه‌نامه داده‌ای 74](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310568)

[فصل پنجم معرفي نرم افزار و بررسي موانع هنگام برنامه نويسي 76](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310569)

[5-1 مقدمه 76](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310570)

[5-2 رشته ارتباط 77](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310571)

[5-3 ارتباط برنامه با نقش برنامه‌ای(APR) 78](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310572)

[5-4 معرفی فرم پرسنل 83](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310573)

[5-5 رمز نمودن اطلاعات 87](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310574)

[5-6 کار با استثناها 88](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310575)

[5-7 جمع بندی 92](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310576)

[فصل ششم نتیجه‌گیری و راهکارهای آینده 93](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310577)

[منابع و ماخذ 95](file:///G:\پایان%20نامه\پایان%20نامه%20کامپیوتر\امنیت%20پایگاه‌%20داده\امنیت%20پایگاه‌%20داده.doc#_Toc62310578)

# فصل 1 كليات

امنیت اطلاعات یکی از مهمترین مفاهیم ،از آغاز زندگی بشر تاکنون بوده است. انسان‌های ادوار گذشته از اهمیت این موضوع مطلع بودند و بسیاری از شکست‌های انسان‌های گذشته در جنگ‌ها فاش شدن اطلاعات مهم و سری بوده است. در ضمن آنها اطلاعات حساس را به رمز تبدیل کرده و برای رد و بدل کردن این اطلاعات از زبان رمزی استفاده می‌کردند.

با پیشرفت علم و جوامع بشری اهمیت این موضوع بیش از پیش آشكار شده و فاش شدن اطلاعات نظامی و یا سیاسی ممکن است منجر به نابودی یک جامعه بیانجامد. سرقت‌های میلیاردی که گاها از بانک‌ها می‌شود مثالی دیگر از اهمیت این موضوع است.

برای امن کردن جامعه مدرن باید از امکانات مدرن نیز استفاده شود زیرا سارقان اطلاعات از امکانات پیشرفته برای دستیابی به اطلاعات استفاده می‌کنند. در این پایان نامه به بررسی امنیت در محیط پایگاه داده می‌پردازیم. این محیط بر مشکلاتی نظیر افزونگی داده و ناسازگاری داده که در سیستم فایل مشکل ساز بوده ، فائق آمده و با به اشتراک گذاشتن داده‌ها ، امکان استفاده بیشتر از اطلاعات را مهیْا ساخته است. در این محیط امکان مدیریت تعداد زیادی کاربر تعبیه شده است. کاربر زیاد مساوی است با درد سر زیاد ! ممکن است کاربری عمدی یا غیر عمدی به داده های محرمانه دست یابد و سیستم را مختل سازد. برای تامین امنیت در چنین محیط‌هایی که همواره با پیچیدگی‌های زیادی نیز برخوردار است لازم است در ابتدا موضوع امنیت را بصورت کلاسیک بررسی کنیم. آشنایی با مفاهیمی همچون تهدید ، صحت داده و انتشار داده ، ما را در شناخت مدل‌های امنیت یاری می‌کند. تامین امنیت در پایگاه داده با شناسایی تهدید آغاز می‌شود. از دیگر واژه‌های مهم در این موضوع کنترل دسترسی است. هدف کنترل دسترسی محدود کردن فعالیت‌هایی است که کاربر مجاز می‌تواند بر روی سیستم‌های کامپیوتری انجام دهد. کنترل دسترسی شامل سیاست‌های مختلفی است. سیاست‌های تشخیص ، اجباری و مبتنی بر نقش از آن جمله هستند. این سیاست‌ها هر يك با اعمال محدودیتی خاص دسترسی کاربر را محدودتر می‌کنند و در تناقض با یکدیگر نیستند ،به عبارت دیگر جهت حرکت همه آنها یکی است.

امنیت کلاسیک را در فصل 2 بررسی می کنیم. سپس به بررسی امنیت در نرم افزار SQLServer2005 می‌پردازیم. رنگ امنیت کلاسیک در تمامی مولفه‌های امنیتی SQLServer2005 به چشم می‌خورد. در این فصل با مفاهیمی همچون مدل هویت شناسی و تفویض اختیار در SQLServer2005 آشنا می شویم. انواع کنترل دسترسی ، انواع نقش ها ، شما و بسیاری دیگر از واژه‌ها و مفاهیم را در فصل 3 بررسی می‌کنیم. رمز نگاری که در نسخه SQLServer2000 نبوده به SQLServer2005 اضافه شده و این نرم افزار را از لحاظ امنیت بسیار پرقدرت ساخته است. در واقع در فصل 3 مدل امنیتی SQLServer2005 به طور کامل بررسی شده است. در فصل 4 یک محیط عملی طراحی و پیاده سازی شده است. در فصل 5 بامشکلاتی که در حین پیاده سازی چنین سیستمی با آن مواجه هستیم را بررسی می‌کنیم. اهمیت این پایان نامه از این جهت است که تعداد بسیار کمی از افراد متخصص این موضوع را در SQLServer2005 بررسی کرده و آن را بصورت عملی پیاده سازی کرده‌اند. بسياري از سيستم‌هاي طراحي شده از لحاظ امنيتي ناكارامد هستند و مکانیزم‌‌هاي امنيتي به كار رفته در اين سيستم‌ها داراي نواقص و كمبودهاي بسياري است.

# 

# فصل 2 امنيت كلاسيك

## 2-1 مقدمه

در محیط پایگاه‌داده ، برنامه‌ها و کاربران مختلف سازمان به یک مجموعه اطلاعات واحد و یکپارچه در DBMS دسترسی دارند. مشکلاتی نظیر ناسازگاری و افزونگی داده‌ها که در سیستم‌های گذشته نمایان بودند از بین رفته و در عوض مسأله تامین امنیت در پایگاه‌داده اهمیت بسیاری پیدا کرده ‌است. تامین امنیت در محیط پایگاه ‌داده یعنی شناسایی تهدید‌هایی[[1]](#footnote-1) که امنیت آن را به خطر می‌اندازند و همچنین انتخاب سیاست‌ها و مکانیسم‌های مناسب برای مقابله با آن. یکی از راههای مبارزه با تهدید‌ها ، کنترل دسترسی است. هدف كنترل دسترسي[[2]](#footnote-2)، محدود كردن اعمال و فعاليت‌هايي است كه كاربر مجاز ، مي‌تواند بر روي سيستم كامپيوتري انجام دهد. كنترل دسترسي ، آنچه را كه كاربر و يا برنامه تحت كنترل او مي‌تواند انجام دهد را كنترل مي‌كند. در اين راستا ، كنترل دسترسي ، مانع از انجام فعاليت‌هايي مي‌شود كه امنيت سيستم را تهدید مي‌كنند.

در اين فصل پس از بیان چند مفهوم پایه در رابطه با امنیت پایگاه‌داده ، به بررسي كنترل دسترسي و رابطه آن با ساير سرويس‌‌هاي امنيتي از جمله سرويس هویت شناسی[[3]](#footnote-3)، سرويس حسابرسي[[4]](#footnote-4) و سرويس مديريت[[5]](#footnote-5) مي‌پردازیم. سپس ماتريس دسترسي[[6]](#footnote-6) و چگونگي پياده‌سازي آن در محيط‌هاي كاربردي را بررسي مي‌كنیم. در پايان به مطالعه سياست‌هاي كنترل دسترسي و مختصري درباره چگونگي مديريت آنها مي‌پردازد.

## 2-2 امنیت پایگاه‌ داده

امنیت اطلاعات در پایگاه‌داده دارای سه بخش اصلی است :

**محرمانگی**[[7]](#footnote-7) : تضمین محرمانگی اطلاعات شامل جلوگیری از فاش شدن غیر مجاز اطلاعات و شناسایی و تحذیر عوامل آن می‌باشد.

**صحت**[[8]](#footnote-8) : تضمین صحت اطلاعات شامل جلوگیری از تغییر غیر مجاز اطلاعات و شناسایی وتحذیر عوامل آن می‌باشد.

**دسترس پذیری** : تضمین در دسترس پذیری اطلاعات شامل جلوگیری از رد غیر مجاز دسترسی به سرویس‌های ارائه شده توسط سیستم و شناسایی و تحذیر عوامل آن می‌باشد.

## 2-3 تهدید امنیت در پایگاه داده

در اینجا لازم است تا تعریف مناسبی از تهدید در پایگاه‌داده ارائه شود. تهدید به معنی تجاوز تصادفی ، یا عمدی و برنامه‌ریزی شده به پایگاه‌داده ، به منظور فاش‌سازی و یا تغییر اطلاعات مدیریت شده توسط سیستم می‌باشد. تجاوز به پایگاه‌داده و تهدید امنیت آن شامل خواندن ، تغییر و حذف غیر مجاز و نادرست اطلاعات می‌باشد. عوامل ایجاد کننده تجاوز در پایگاه‌داده تهدید نامیده می‌شوند. نتایج تجاوز به پایگاه‌داده مختصرا در ذیل آورده شده است :

**انتشار نامناسب اطلاعات**[[9]](#footnote-9) : خواندن عمدی و یا غیر عمدی اطلاعات توسط کاربر غیر مجاز که موجب انتشار غیر مجاز اطلاعات می‌شود.

**تغییر نامناسب داده**[[10]](#footnote-10) : تغییر نامناسب داده شامل تمام تجاوز‌هایی می‌شود که صحت داده را به خطر می‌اندازند.

**عدم پذیرش سرویس‌ها** : عدم پذیرش سرویس‌ها شامل تمام اعمالی است که مانع دسترسی کاربر به داده‌ها و یا استفاده از منابع می‌شود.

1. Threat- [↑](#footnote-ref-1)
2. - access control [↑](#footnote-ref-2)
3. - authentication [↑](#footnote-ref-3)
4. - auditing [↑](#footnote-ref-4)
5. administration- [↑](#footnote-ref-5)
6. access matrix- [↑](#footnote-ref-6)
7. - Secrecy [↑](#footnote-ref-7)
8. Integrity- [↑](#footnote-ref-8)
9. Improper release of information- [↑](#footnote-ref-9)
10. Improper modification of data- [↑](#footnote-ref-10)