امنیت در رایانش ابری

اتوسا طغیانی
دانشکده فنی و مهندسی، دانشگاه لرستان، خرم اباد، ایران
Atousa.toghyani@gmail.com

چکیده- ابر برای اتصال ارزان، مسیریابی و مدیریت در هر زمان و مکانی بسیار کارآمد خواهد بود. داده های ابر با کمک خدمات ارائه-شده توسط ارائه‌دهندگان خدمات ابری در یک سرور از راه دور ذخیره می‌شوند و قابل‌دسترسی هستند. تامین امنیت یک نگرانی اساسی است، زیرا داده‌ها از طریق یک کانال (اینترنت) به سرور از راه‌دور منتقل می‌شوند. امنیت داده‌ها درسرور پایگاه داده ابری، منطقه اصلی نگرانی در پذیرش ابر است. برای محافظت از داده ها "رمزگذاری" یکی از روش‌های مهم است.

واژه‌های کلیدی: رایانش ابری ، محاسبات ابری ، امنیت ، رمزنگاری ،AES ، IaaS ، PaaS ، SaaS

۱- مقدمه

رایانش ابری، یک مدل مبتنی بر اینترنت است که برای ایجاد دسترسی به دریایی از منابع محاسباتی است. این منابع می‌توانند: شبکه، سرور، سرویس و یا اپلیکیشن باشند.

محاسبات، به معنای توان‌پردازشی است که از سوی خدمات ابری ارائه می‌شود و هر چه توان محاسباتی بیشتر باشد به همان نسبت عملکرد بهتر است.

سرویس‌دهی در ابر به سه صورت است: نرم‌افزار به‌عنوان سرویس (SaaS)[1] ، پلتفرم به‌عنوان سرویس(PaaS)[2] و زیرساخت به‌عنوان سرویس(IaaS)[3].

بزرگان این حوزه آمازون (AWS)، مایکروسافت (Microsoft Windows Azure)، گوگل(GCP)، آی بی ام (IBM) و به‌تازگی علی بابا (Alibaba) هستند.

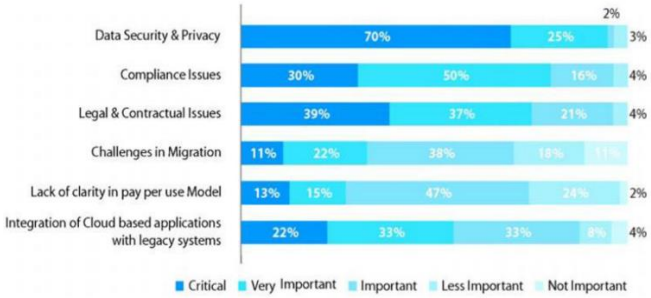
با توجه به‌نوظهور بودن این فناوری اما هیچ‌گونه نشانی دال بر اینکه بازار این بخش از دنیای فناوری ممکن است با رکورد یا پسرفت همراه باشد، وجود ندارد.

امنیت و حفظ حریم‌خصوصی به دلیل داشتن اطلاعات حساس و مهم ذخیره شده در ابر برای مشتریان، به عنوان یک مسئله مهم در محیط محاسبات ابری مطرح می‌شود.

امنیت یک چالش اساسی است، که به خطر افتادن ان باعث از بین‌رفتن اطلاعات مخفی کاربر، نشت داده‌ها و افشای حریم خصوصی داده‌های شخصی است .

قبل از اجرای رایانش ابری در یک سازمان، ابتدا باید با چالش امنیتی روبه‌رو شد.

در شکل (۱) مشخص است، که امنیت داده‌ها و حریم خصوصی مهم‌ترین عامل هستند.[3]



شکل ۱- امنیت داده‌ها و حریم‌خصوصی [3]

سه گونه خطر داده‌ها را تهدید میکند: سوءاستفاده از خدمات دهنده ابزارداده‌ها، نفوذ کاربران به زیرساخت ابر و نفوذ خرابکاران به لینک ارتباطی بین کاربر و ابر.

نتیجه هر سه مورد برای کاربر یکسان است و باعث از دست‌دادن امنیت و حریم شخصی می‌شود.

I. بخش اول: شیوه‌های سرویس‌دهی در ابر: [2]

شیوه‌های سرویس‌دهی در ابر به سه صورت است: نرم‌افزار به عنوان سرویس(SaaS)، پلتفرم به عنوان سرویس(PaaS)، زیرساخت به عنوان سرویس(IaaS).

1) IaaS :

درمدل IaaS تمام زیرساخت‌ها توسط ارائه‌دهنده سرویس‌های ابر(CSP) ارائه و نگهداری می‌شود، که شامل: سرورها، ذخیره‌سازها ، شبکه ها و... است.

نمونه ایی از خدمات فروشنده های این مدل: cloud Amazon، Go Grid، Rackspace Cloud

ویژگی ها و مؤلفه های IaaS شامل:

- توافق‌نامه سطح خدمات (SLA)
- مقیاس‌گذاری پویا
- اتوماسیون وظایف اداری
- خدمات سرویس محاسبات و مدل صورت‌حساب
- اتصال اینترنتی
- مجازی‌سازی دسک‌تاپ

خطرات و آسیب پذیری‌های مجازی سازی‌شده که به‌ویژه برمدل تحویل IaaS تأثیر می‌گذارند، عبارتند از:

۱- خطرات و آسیب پذیری های مدل IaaS :

۱-۱) تهدیدات امنیتی ناشی از میزبان:

نقطه کنترلی در محیط‌های مجازی دستگاه میزبان وجود دارد که به میزبان اجازه می‌دهد تا vm[۴] نظارت و ارتباط برقرار کند. بنابراین محافظت از ماشین‌های میزبان از محافظت vm ضروری‌تر است.

میزبان میتواند برترافیک شبکه vm های میزبان خود نظارت کند. این می‌تواند ویژگی‌های مفیدی را برای میزبان درنظر بگیرد و آنها ممکن است از آن استفاده‌کنند؛ مانند: کلیپ‌بورد مشترک که اجازه می‌دهد تا داده‌ها را با استفاده از برنامه مخرب در vms با vm میزبان انتقال دهند. بنابراین محیط میزبان باید نسبت به ماشین-های مجازی فردی ایمن‌تر باشد.

میزبان میتواند از طریق روش‌های زیر روی vm ها تاثیر بگذارد:

- میزبان میتواند vm ها را روشن، خاموش، توقف و راه‌اندازی مجدد کند.
- نظارت و پیکربندی منابعی که دراختیار vm است، شامل:
  - Cpu ، حافظه، دیسک و استفاده از شبکه vm.
- تعداد Cpu ها، میزان حافظه، میزان و تعداد دیسک‌های مجازی و تعدادی رابط شبکه مجازی را که در دسترس vm است، تنظیم کند.
- نظارت بر برنامه‌هایی که داخل vm کار می‌کند.
- داده‌های ذخیره‌شده در دیسک‌های مجازی vm را مشاهده، کپی و احتمالاً اصلاح کند.

متاسفانه، مدیر سیستم یا هرکاربر مجاز که کنترل ممتازی روی داده‌ها داشته باشد، می‌تواند از این رویه‌ها سوءاستفاده کند.

۱-۲) تهدیدات امنیتی دیگر:

الف) نظارت بر vm می‌تواند امنیت و حریم خصوصی را نقض کند؛ اما معماری جدید Cpu ها که با یک ویژگی محافظت از حافظه ادغام شده‌اند؛ می‌توانند از نقص امنیت و حریم خصوصی جلوگیری کنند.

ب) از مهم‌ترین موضوعاتی که تبادل اطلاعات بین ماشین‌های مجازی را تهدید می‌کند، نحوه استقرار آنها است.

به اشتراک گذاشتن منابع بین vm ها ممکن است، امنیت هر vm را برای همکاری با استفاده از برنامه‌هایی مانند :کلیپ‌بورد مشترک که امکان تبادل داده‌ها بین vmها و میزبان را که به برنامه‌های مخرب در vmها کمک می‌کند، را سلب کند.

یک مخرب vm میتواند از طریق حافظه shard به سایر vm ها دسترسی داشته باشد.

ج) حمله DOS[۵] : تلاشی برای خارج کردن ماشین و منابع شبکه از دسترس کاربران مجاز می‌باشد، به‌عنوان مثال: کاربران برای وارد شدن به سایت تلاش می‌کنند، اما قادر به دیدن سایت و مشاهده خطا نیستند.

این اتفاق وقتی می‌افتد که تعداد درخواست‌هایی که توسط سرور قابل دستیابی است از ظرفیت آن فراتر رود.

استفاده از سیستم تشخیص نفوذ (IDS)[۶] یکی از روش‌های مفید دفاع در برابر این نوع حملات است.

۱-۳) حملات اتصال به شبکه و اینترنت:

راه‌حل‌ها و تکنیک‌های عملی برای از بین‌بردن این حملات یا کاهش اثرات آن‌ها به شرح زیر است:

- تقسیم بندی شبکه منطقی
- اجرای فایروال‌ها
- رمزگذاری ترافیک
- نظارت بر شبکه

۲) مدل PaaS:

راهی برای اجاره سخت‌افزار از طریق اینترنت است. توانایی مدیریت برنامه‌ها را بدون نصب هیچ پلتفرم یا ابزار روی دستگاه-های محلی خود امکان پذیر می‌کند. در این مدل پلتفرم در اختیار کاربران قرارمی‌گیرد تا برنامه‌های مورد نیاز خود را روی آن نصب کنند.

نمونه‌ایی از خدمات فروشنده‌های این مدل: Google App Engine, Amazon Web Service Elastic , Microsoft Windows Azure Beanstalk

۲-۱) مزایا :

- OS[۷] ، سیستم‌عامل در هر زمان می‌تواند تغییرکرده و به‌روز شود.
- به تیم‌های توزیع‌شده جغرافیایی اجازه می‌دهد تا اطلاعات را برای توسعه پروژه‌های نرم‌افزاری به اشتراک بگذارند.

برای برنامه‌نویسانی که می‌خواهند کد خود را توسعه دهند بسیار مفید است.

در PaaS از ماشین‌مجازی استفاده می‌شود، ماشین‌های مجازی باید در برابر حملات مخرب، مانند: بدافزارهای ابری محافظت شوند. بنابراین حفظ یکپارچگی برنامه‌ها و همچنین اجرای دقیق تأیید هویت در هنگام انتقال داده‌ها درکل کانال‌های شبکه، امری اساسی است.

۲-۲) تهدیدهای امنیتی:

a) مکان داده‌ها :

پلتفرم واقعی در یک میزبان واحد نیست؛ این پلتفرم را می‌توان به عنوان گروه میزبان‌های خوشه فکرکرد؛ در واقع مکان داده‌ها را نمی‌توان به بخش خاص در میزبان اختصاص داد؛ این امر نیازمند ایجاد امنیت بیشتری است، تا جایی که تامین امنیت یک مکان واحد نسبت به بسیاری از آنها راحت‌تر است.

مسئله امنیتی دیگر این است، تکثیر داده‌ها در دسترس‌بودن زیادی از داده‌ها را برای توسعه‌دهندگان و کاربران ایجاد می‌کند، که این داده‌های توزیع‌شده مانند سایر داده‌ها است و تفاوت عمده این مورد در ناشناخته‌بودن مکان دقیق انها است.

b) دسترسی ممتاز :

از محبوب‌ترین ویژگی‌های PaaS، اجازه استفاده توسعه‌دهندگان نرم‌افزار برای اشکال‌زدایی (Debug) است. در اشکال‌زدایی به توسعه‌دهندگان اجازه دسترسی به داده‌ها و مکان‌های حافظه داده می‌شود تا در صورت لزوم بتوانند مقادیر را تغییر دهند.

c) سیستم‌های توزیع‌شده:

PaaS معمولاً بسیار توزیع‌شده است.گره‌ها می‌توانند مستقل باشند؛ در حالی که ارائه‌دهنده خدمات ابری (CSP)[۸] دارای خوشه است. بنابراین به احتمال زیاد مسیرهای پیکربندی استاندارد وجود خواهد داشت.

CSP باید بتواند امنیت لازم را تأمین کند؛ اما مسئولیت تأیید این امر به مشتری تعلق دارد.

راه حل‌ها و تکنیک‌های عملی برای از بین‌بردن این حملات یا کاهش اثرات آن‌ها:

- محصورکردن سیاست‌های کنترل دسترسی با اشیا می‌تواند یکی از راه‌حل‌های حل دسترسی خصوصی باشد.
- نقاط اجرای سیاست PEP[۹] : یک نقطه اجرای سیاست (PEP) یک نهاد منطقی یا مکانی است که بر روی سرور ایجاد می‌شود و در صورت درخواست کاربر،کنترل می‌شود و در مورد پذیرش درخواست کاربرکه می‌خواهد به یک منبع روی یک رایانه یا سرور شبکه دسترسی پیداکند، تصمیم‌گیری می‌کند.

Trusted Computing Base (TCB) : مجموعه‌ای از کدهای اجرایی و پرونده‌های پیکربندی است که فرض می‌شود امن است. TCB برای نقص‌های امنیتی کاملاً مورد تجزیه و تحلیل قرارگرفته است و به عنوان یک‌لایه بر روی سیستم‌عامل نصب شده و یک API[۱۰] را برای اشیا کاربر فراهم می‌کند.

به نظر می‌رسد، رمزگذاری بهترین راه‌حل ممکن است.

۳) مدلSaaS :

در مدل SaaS کاربران با استفاده از مرورگرهای وب از طریق اینترنت، به نرم افزارهای کاربردی سرویس دسترسی پیدا می‌کنند. بنابراین امنیت مرورگرهای وب از اهمیت حیاتی برخوردار است. افسران امنیت اطلاعات باید روش‌های مختلفی را برای تأمین امنیت برنامه های SaaS در نظر بگیرند.

گزینه های موجود که برای اجرای حفاظت از داده های منتقل شده از طریق اینترنت استفاده می شود، شامل:

امنیت خدمات وب، رمزگذاری گسترده زبان نشانه‌گذاری (XML)[۱۱] ، Secure Socket Layer (SSL) و ...

SaaS در اصل برای اتوماسیون نیروی فروش و مدیریت ارتباط با مشتری (CRM) Salefoece.com مستقر شد. نمونه‌ایی دیگر از خدمات فروشنده‌های این مدل : Google Docs , Google Gmail در این مدل امکان کارگروهی روی پروژه وجود دارد.ارائه‌دهندگان خدمات باید تاییدکنند،که چندکاربر بودن آنها باعث نقض حریم خصوصی سایر کاربران نمی‌شود.

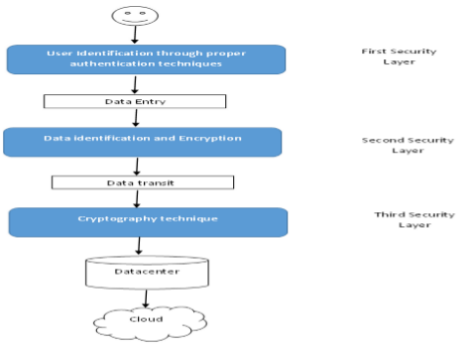
تهدید های امنیتی در مدل SaaS:

- احراز هویت و مجوز
- محرمانه بودن داده‌ها
- امنیت اطلاعات
- دسترسی به داده‌ها
- نقض داده‌ها
- مدیریت هویت و ورود به فرایند

Navneet Singh : راه‌حل‌های عملی را برای ارزیابی تهدیدهای امنیتی درSaaS ارائه می‌دهد، که در آن باید از مشتری سوال شود:
از چه معیارهایی برای گزارش استفاده می شود؟
سطح کنترل دسترسی چقدر است؟
آیا داده‌های ارائه‌شده به‌راحتی در ابزارهای نظارت داخلی قابل انطباق است؟
داده‌های مشترک چقدر مهم هستند؟

مدل پیشنهادی:

مدل امنیتی ابر ارائه شده از سه لایه تشکیل شده است:
در لایه اول : شناسایی کاربر از طریق تکنیک های مناسب و تأیید صحت ان بررسی می‌شود.
امنیت در لایه دوم: به شناسایی داده‌ها و رمزگذاری بستگی دارد.
در آخرین لایه :از روش رمزنگاری برای اطمینان از انتقال داده‌ها استفاده می‌شود. معماری مدل پیشنهادی در شکل (۲) نشان داده شده است.**[2]**

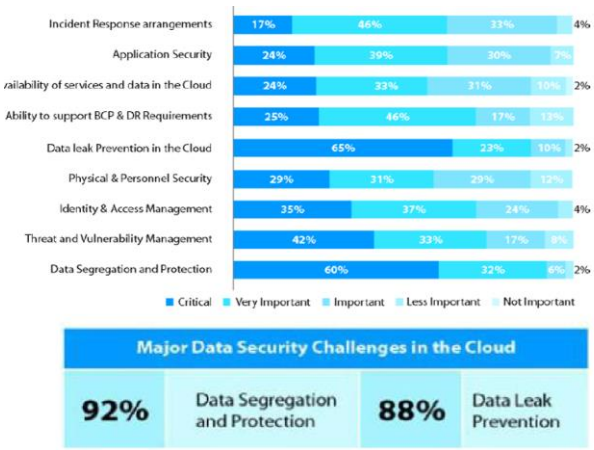


شکل ۲ – مدل پیشنهادی: [2]

II. بخش ۲: چالش‌های امنیت داده :[3]

برای تقویت امنیت در رایانش‌ابری، تهیه تأیید اعتبار، مجوز و کنترل دسترسی برای داده‌های ذخیره‌شده در ابر مهم است.
سه حوزه اصلی در امنیت داده‌ها عبارتند از:
- محرمانه‌بودن: جلوگیری از افشای اطلاعات به افراد غیرمجاز و همچنین محدود کردن دسترسی به اطلاعات و سیستم‌ها.
- تمامیت: جلوگیری از تغییر داده‌ها به‌طور غیرمجاز و حفظ یکپارچگی داده‌ها.
- دسترسی: اطلاعات باید زمانی که مورد نیاز افراد مجاز هستند، در دسترس باشند.

از دست‌دادن داده یا نشت داده‌ها می‌تواند تأثیر جدی بر تجارت، برند و اعتماد یک سازمان داشته باشد. همان‌طور که در شکل (۳) مشاهده می شود؛ نشت داده‌ها با ۸۸٪ از مهم‌ترین عامل‌ها در چالش‌های امنیتی است؛ هم‌چنین تفکیک و محافظت از داده‌ها ۹۲٪ بر چالش‌های امنیتی تاثیر می‌گذارد. [3]



شکل ۳- چالش های امنیت داده‌ها[3]

۲-۱) محل:

در محاسبات ابری، داده‌ها در مناطق مختلفی توزیع می‌شوند و یافتن مکان داده‌ها دشوار است. وقتی داده‌ها به مکان‌های مختلف جغرافیایی منتقل می‌شوند، قوانین حاکم برآن داده‌ها نیز می‌تواند، تغییرکند. بنابراین یک مسئله پیروی از قوانین و حفظ حریم خصوصی داده‌ها در محاسبات ابری است. مشتریان باید موقعیت مکانی اطلاعات خود را بدانند و این امکان باید از طرف ارائه‌دهنده خدمات تضمین شود.

۲-۲) امنیت:

سیستم باید امنیت را به‌گونه‌ای حفظ‌کند که داده‌ها فقط توسط شخص مجاز اصلاح شوند.
در محیط مبتنی بر ابر، باید یکپارچگی داده‌ها به‌درستی حفظ شود تا از دست‌رفتن داده‌ها جلوگیری شود. به طورکلی، هر تراکنش در رایانش ابری باید خصوصیات ACID[۱۲] را برای حفظ یکپارچگی داده‌ها دنبال کند.

۲-۳) دسترسی:

دسترسی به داده‌ها عمدتا به سیاست‌های امنیتی داده اشاره دارد. در دسترس بودن مهمترین مسئله در سازمان‌های مختلف است که به عنوان یک مسئله مهم در مواجهه با خرابی با ان مواجهه‌هستند. در یک سازمان، بخشی از کارمندان براساس سیاست‌های امنیتی شرکت خود، به‌بخشی از داده‌ها دسترسی پیدا می‌کنند و سایرکارمندان شاغل در همان سازمان نمی‌توانند به همان داده‌ها دسترسی پیداکنند.

ازآنجا که دسترسی از طریق اینترنت برای همه کاربران ابری فراهم شده است؛ لازم است دسترسی ممتاز برای کاربر فراهم شود.کاربر می‌تواند از مکانیسم‌های رمزگذاری و محافظت از داده‌ها برای جلوگیری از خطر امنیتی استفاده کند.

۲-۴) محرمانه بودن:

داده‌ها روی سرورهای از راه‌دور توسط کاربران‌ابری ذخیره می‌شوند و محتوا شامل:داده‌ها، فیلم‌ها و .... می‌توانند در اختیار ارائه دهندگان یک یا چند ابر قرارگیرد.

هنگامی که داده ها در سرور راه دور ذخیره می‌شوند؛ محرمانه بودن داده‌ها یکی از ملزومات‌مهم است. برای محرمانه نگه‌داشتن، اطلاعات رمزنگاری می‌شوند و در طی انتقال یا جاهایی که ممکن است ذخیره شود، رمزشده باقی می‌ماند.

۲-۵) نقض می‌کند[۱۳]:

شکستن داده‌ها مسئله مهم امنیتی دیگری است که باید در ابر بررسی شود.

از آنجا که داده‌های بزرگ کاربران مختلف در ابر ذخیره می‌شود، امکان دارد کاربر مخرب وارد ابر شود به گونه‌ای که کل محیط ابر مستعد حمله باشد.

نقض می‌تواند به دلیل مشکلات مختلف انتقال، تصادف یا به دلیل حمله خودی رخدهد.

۲-۶) تفکیک:

یکی از ویژگی‌های اصلی محاسبات ابری چنداجاره‌ایی بودن ان است. از آنجا که چنداجاره‌ایی بودن ابر، اجازه می‌دهد تا داده‌ها توسط چندین کاربر در سرورهای ابری ذخیره شود، امکان نفوذ وجود دارد. با واردکردن کد مشتری یا با استفاده از هر برنامه‌ایی، می‌توان داده ها را مورد حمله قرارداد؛ بنابراین این یک ضرورت است که داده‌های مشتری به صورت جداگانه ذخیره شود.

آسیب پذیری‌های که با تفکیک داده‌ها ایجاد می‌شود را می‌توان با استفاده از تست‌هایی مانند علائم تزریق SQL[۱۴] ، اعتبارسنجی داده‌ها و ذخیره ناامن کشف کرد.

۲-۷) ذخیره سازی:

برای بررسی داده‌های ذخیره‌شده در ماشین‌های مجازی، موارد بسیاری وجود دارد که یکی از این موارد قابلیت اطمینان در ذخیره‌سازی داده‌ها است.

ماشین‌های مجازی باید در یک مکان فیزیکی ذخیره‌شوند که ممکن است باعث ایجاد خطر امنیتی شود.

III. بخش ۳: تامین امنیت رایانش ابری با استفاده از رمز نگاری [4]

رمزنگاری در روزگار مدرن،گروه بندی سه نوع الگوریتم است:

۱. الگوریتم کلید متقارن:

در این الگوریتم از یک کلید محرمانه (خصوصی) استفاده می‌کنند؛ که برای ارسال‌کننده و دریافت‌کننده شناخته شده است. از همان کلید خصوصی برای رمزگزاری و رمزگشایی استفاده می‌شود. شامل: استاندارد رمزگذاری داده‌ها (DES)[۱۵] ، استاندارد رمزگشایی پیشرفته (AES)[۱۶]، Triple Desi، Blowfish.

۲. الگوریتم کلید نامتقارن :

از یک جفت کلید برای رمزنگاری استفاده می‌کند، یک کلید عمومی برای رمزنگاری و یک کلید خصوصی برای رمزگشایی.

این الگوریتم هزینه محاسباتی بالا و سرعت پائینی دارد.

از الگوریتم های مختلفی مانند: Adleman ، Shamir, Rivest (RSA)[۱۷]، الگوریتم امضای دیجیتال (DSA), منحنی ایپیتیک، EL Gama Diffi-Hillman (DH) , Elliptic Curve (Ec) و ... استفاده میکند.

۳. توابع هش:

از یک انتقال ریاضی غیرقابل برگشت، برای تبدیل داده‌ها به یک مقدار فشرده استفاده می‌کند؛ شامل الگوریتم هایی مثل: پیام Digest، الگوریتم Secure Hash است.

رمزگذاری متقارن به عنوان راه‌حل انتخاب می‌شود؛ زیرا دارای سرعت و راندمان محاسباتی بالا برای رمزگذاری حجم زیادی از داده‌ها است.

زمان لازم برای شکستن یک الگویتم رمزگذاری، ارتباط مستقیم با طول کلید مورد استفاده برای برقراری ارتباط دارد، هر چه طول کلید طولانی‌تر باشد، رمزگذاری قوی‌تر است.

الگوریتم AES :

AES مخفف " Advanced Encryption Standard " است.
AES، استاندارد رمزگذاری پیشرفته، یک الگوریتم رمزگذاری متقارن است؛ این الگوریتم توسط دو رمزنگار بلژیکی جوآن دمن و وینسنت رجمن تهیه شده است.
AES امروزه الگوریتم رمزگذاری متداول است؛که مبتنی بر چندین تعویض، جایگشت و تحولات خطی است که هر یک در بلوک‌های داده ۱۶بایت اجرا می‌شوند. هنگامی که می خواهیم متن محرمانه-ای را با فرمت رمزگشایی، رمزگذاری کنیم این الگوریتم مفید است. برای مثال: وقتی می خواهیم داده‌های حساس را از طریق نامه الکترونیکی ارسال کنیم.
رمزگشایی متن رمزگذاری شده فقط درصورتی امکان‌پذیر است که رمز عبور مناسب را بدانیم.
الگوریتم AES، حداقل زمان را برای رمزگذاری مصرف می‌کند و RSA طولانی‌ترین زمان رمزگذاری را مصرف می‌کند.
هیچ حمله عملی علیه AES وجود ندارد؛ بنابراین بهترین الگوریتم رمزگذاری برای دولت‌ها، بانک‌ها و سیستم‌های نیازمند امنیت بالا در سراسرجهان است.
این الگوریتم مبتنی‌بر "شبکه جایگزینی - جایگشت" است.
این مجموعه شامل یک‌سری عملیات مرتبط است که برخی از آنها شامل جایگزین کردن ورودی‌ها با خروجی‌های خاص (تعویض) و برخی دیگر شامل جابجایی بیت‌های اطراف است.

۱) قدم اول :

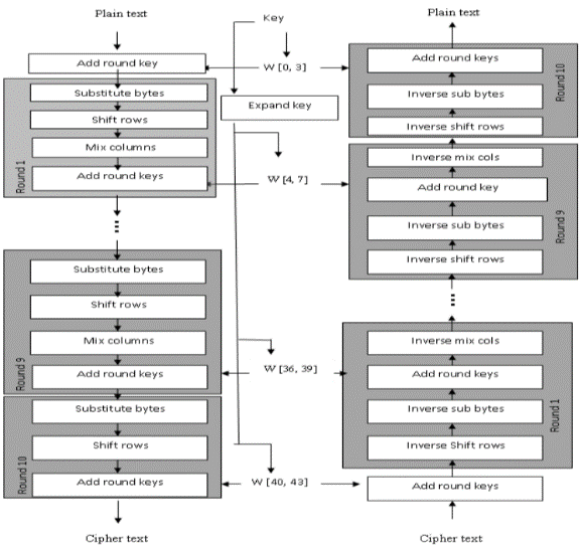
- Add Round Key

۲) چهار کارکرد زیر تکرار می شوند :

- Sub Bytes
- Shift Rows
- Mix Columns
- Add Round Key

۳) مرحله نهایی:

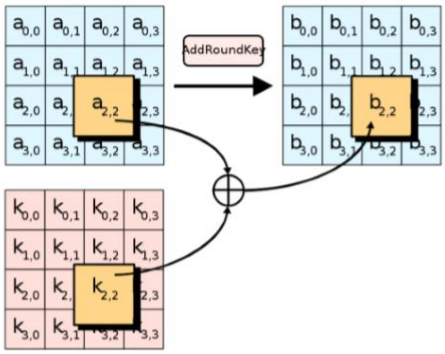
- Sub Byte
- Shift Row
- Add Round Key



شکل ۴ - رمزگذاری و رمزگشایی در AES [3]

۴) تعویض بایت (Sub Bytes):

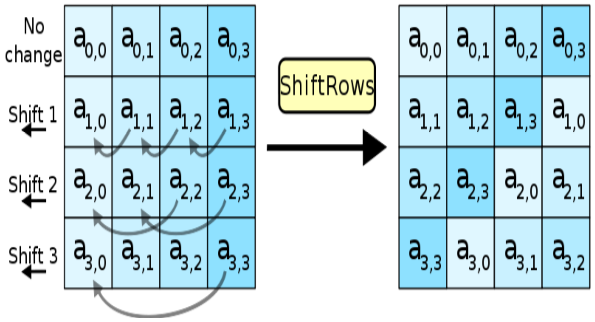
۱۶ بایت ورودی با جستجو در یک جدول ثابت (جعبه S) ارائه‌شده در طراحی جایگزین می‌شوند؛ نتیجه یک ماتریس است؛ که شامل: چهار ردیف و چهار ستون است.



شکل ۵ – تعویض بایت[4]

۵) جابه‌جایی سطرها (Shift Rows):

هر یک از چهار ردیف ماتریس به سمت چپ منتقل می‌شوند.
هر ورودی که "سقوط کند" در سمت راست سطر دوباره وارد می‌شود.



شکل ۶ – جابه‌جایی سطرها[4]

شیفت به شرح زیر انجام می شود:
- ردیف اول جابه‌جا نمی‌شود.
- ردیف دوم یک موقعیت (بایت) به سمت چپ منتقل می‌شود.
- ردیف سوم دو موقعیت به سمت چپ منتقل می‌شود.
- ردیف چهارم سه موقعیت به سمت چپ منتقل می‌شود.

نتیجه یک ماتریس جدید است که از همان ۱۶ بایت تشکیل شده‌است اما مکان داده‌ها تغییر کرده‌است.

۶) ستون‌ها ادغام می‌شوند (Mix Columns):

هر ستون از چهار بایت تشکیل شده است؛ که با استفاده از یک عملکرد ویژه ریاضی به اعداد دیگر تبدیل می‌شوند. این عملکرد چهار بایت یک ستون را وارد می کند و چهار بایت کاملاً جدید را جایگزین ستون اصلی می کند.

نتیجه یک ماتریس جدید دیگر است،که از ۱۶ بایت جدید تشکیل شده‌است.

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

شکل ۷ – ادغام ستون‌ها[4]

۷) Add Round key :

۱۶ بایت ماتریس اکنون ۱۲۸ بیت در نظر گرفته شده است و با ۱۲۸ بیتی از round key (کلید گرد)، XOR شده است.

اگر این آخرین دور باشد؛ خروجی متن رمزگذاری می‌شود.

درغیر این‌صورت، ۱۲۸ بیت حاصل به عنوان ۱۶ بایت تعبیر می‌شود و دور مشابه دیگری را شروع می‌شود.

IV. بخش چهارم: بررسی مسائل امنیتی بانک در محاسبات ابری [1]

مدیریت ریسک محاسبات ابری، شامل: فرآیندهای محاسباتی ، روش ها و تکنیک‌هایی است که برای کاهش خطرات محاسبات ابری مفید هستند؛ همچنین به مدیر پروژه و تیم نرم‌افزار کمک می‌کند تا تصمیم‌گیری‌های بهتری را برای کاهش خطرات محاسبات ابری انجام دهند.

مدیریت ریسک امنیتی در بسیاری از مناطق مرتبط با فناوری اطلاعات (IT) قابل توجه می‌باشد، به‌عنوان مثال: ارتباطات از راه دور، سیستم های اطلاعات بانکی، محاسبات ابری.

چهارچوب مدل سازی محاسبات ابری به پنج مرحله تقسیم میشود :

- تحرک و برنامه بانکی
- مدل‌های استقرار ابری (CDM)
- مدل‌های مدیریت ریسک ابر (CRMM)
- مدل‌های سرویس ابر (CSM)
- مدل امنیتی ابر (CSM)

۱) مدل امنیتی ابر (CSM) شامل مراحل زیر است:

۱-۱) تحرک مربوط به امکان جابجایی در مکان‌های متنوع و استفاده از هرنوع وسیله قابل حمل مانند: تلفن‌های هوشمند، دستیاران دیجیتال شخصی (PDA)[۱۸] و لپ‌تاپ‌های بی‌سیم است.

با این وجود، بانکداری تلفن همراه مربوط به هر عملیاتی است که به خدمات بانکی مربوط است، مانند: چک، پرداخت، دریافت پیامک بانکی از طریق دستگاه تلفن همراه و معاملات حساب .

۱-۲) CSM به برخی از قسمت‌های فناوری وب، مانند: برنامه رابط برنامه نویسی (API)، خدمات وب، وب ۲,۰ و غیره بستگی دارد.

همچنین، CSM به چهار دسته تقسیم می شود:

نرم‌افزار به عنوان یک سرویس (SaaS)، بسترهای نرم‌افزاری به‌عنوان یک سرویس (PaaS) ، فرآیند بانکداری به‌عنوان یک سرویس (BPaaS)[۱۹] و زیرساخت‌ها به‌عنوان یک سرویس (IaaS).

در بخش اول IaaS, PaaS , SaaS معرفی شدند و مورد ارزیابی قرار گرفتند، حال مفهموم BPaaS را بررسی می‌شود.

: BPaaS

ارائه منطق و جریان برای کنترل فرآیندهای کسب و کار که کاربران اجرا می‌کنند.

فرآیندهای کسب و کار به عنوان سرویس از طریق افزایش خودکارسازی، تعداد نیروی انسانی را کاهش می‌دهد که این امر موجب کاهش هزینه‌های فرآیند نیز می شود.

مزایا:

- این امکان را به وجود می‌آورد که به‌راحتی تغییرات درخواستی و یا نیازمندی‌های آینده کسب و کار با کمترین زمان و هزینه قابل توسعه باشند.
- قابلیت یکپارچه شدن با وب‌سایت کسب‌وکار را فراهم می‌کند. از این رو این امکان را به وجود می‌آورد که فرآیندهای انتها به انتها (End to End Process) را اجرا کند .
- امکان پرداخت الکترونیک را برای مشتریان کسب‌وکار شما فراهم می‌کند.
- امکان همکاری و تعامل بیشتر پرسنل داخلی و مشتریان بیرونی کسب‌وکار شما را فراهم می‌کند.

۳-۱) CDM را می‌توان به چهار نوع متفاوت تقسیم کرد:

- ابر عمومی:

برای عموم مردم یا گروه بزرگی از صنعت قابل دستیابی است و توسط شخص ثالثی که خدمات ابری را می‌فروشد ،ارائه می‌شود.

- ابرخصوصی:

تنها مختص یک سازمان یا شرکت خاص بوده که دسترسی کامل و ایمنی به ان دارد و تنها کاربران و مشتریان مشخص می‌توانند در ان فعالیت کرده و از سرویس‌های ان استفاده نمایند.

- ابر جامعه:

با توجه به مجموعه هدف مصرف کنندگان در میان ابرهای عمومی و خصوصی قرار می‌گیرد. این مدل توسط گروه خاصی از جامعه در درون سازمانی استفاده می‌شود که همان نگرانی، اهداف یا ضرورت‌های امنیتی را دارند.

- ابر ترکیبی :

ترکیبی از ابرخصوصی و ابرعمومی است که با استفاده از تکنولوژی این ابرها به یکدیگر متصل می‌شوند و امکان به اشتراک گذاشتن داده‌ها و اپلیکیشن‌ها بین آن‌ها فراهم می‌شود؛ این نوع ابر، موجب انعطاف‌پذیری بیشتر کسب‌وکارها می‌شود و امکانات گسترده‌تری را در اختیار آن‌ها قرار می‌دهد.

۴-۱) مدیریت ریسک ابر (CRM):

انواع مختلفی از خطرات وجود دارد که مدیریت بانک باید در برابر آن‌ها محافظت شود.

برای بسیاری از بانک‌ها ریسک اصلی، ریسک اعتباری است؛ اما چندین خطر دیگر نیز وجود دارد که مقامات نظارت باید به بانک‌ها اطلاع دهند.

هشت مرحله برای مدیریت مؤثر ریسک ابر وجود دارد:

- مرحله برنامه‌ریزی خطر ابر (CRPL)
- فاز تجزیه‌وتحلیل خطر ابر (CRA)
- مرحله شناسایی خطر ابر (CRI)
- مرحله اولویت‌بندی خطر ابر (CRP)
- مرحله ارزیابی خطر ابر (CRE)
- مرحله درمان ریسک ابر (CRT) شامل چهار استراتژی برای پاسخ به خطرات ابر است:
  - کاهش خطر ابر، اجتناب از خطر ابر، رفع خطر ابر، پذیرش خطر ابر.
- مرحله کنترل خطر ابر (CRC)
- فاز ارتباطات و مستندات Cloud Risk (CRCD).

۵-۱) مدل‌های Issue Security Cloud (CSIM):

امنیت ابر موضوعی بسیار متداول است و هرگروه‌بندی از سیاست-ها، فن‌آوری‌ها، کنترل‌ها برای محافظت از داده‌ها، زیرساخت‌ها و خدمات باید در برابر حملات احتمالی یا دستیابی به اهداف تجاری همه حوزه‌های امنیتی به‌روشی مؤثر کارکند.

۲)مسائل امنیتی ابر:

طبقه‌بندی موضوعات مهم امنیتی در بانکداری ابری :

۲-۱) ارائه‌دهندگان خدمات ابر و مسائل مربوط به امنیت سیاست‌ها:

عدم رعایت استاندارد، توافق‌نامه سطح خدمات (SLA)، حاکمیت، قانون و سیاست، وابستگی، عدم شفافیت، قابلیت اطمینان بودن ارائه‌دهنده خدمات ابر، خودی‌های مخرب، رعایت مقررات و اصلاحات، مسائل فناوری مشترک، مشخصات ریسک ناشناخته، قابل‌اعتماد بودن ابر، سوءاستفاده از محاسبات ابری.

۲-۲) مشکلات امنیتی برنامه (نرم افزار):

تأیید اعتبار، مجوز، رابط های ناامن (API)، دردسترس بودن و تحرک، قابلیت حمل و قابلیت همکاری.

۲-۳) مسائل مربوط به امنیت داده و اطلاعات:

حفظ حریم خصوصی، محرمانه بودن، محافظت از داده‌ها، محدودیت‌ها و تفکیک داده‌ها، یکپارچگی داده‌ها، مکان‌یابی داده‌ها ، از دست‌دادن اطلاعات، نشت، کشف و بازیابی، ربودن حساب یا سرویس و ترافیک.

۲-۳) کنترل امنیتی و مشکلات شبکه:

کنترل جریان اطلاعات، محدودیت‌های ذاتی شبکه بی‌سیم، طرح-های دسترسی به شبکه، پهنای باند، ناشناس ماندن و تجزیه و تحلیل ترافیک شبکه، امنیت شبکه، محافظت از شبکه مجازی، کنترل محدود، انکار توزیع خدمات (DDoS)، ناهمگونی در دستگاه‌های ابری موبایل، قابلیت اطمینان و تأخیر.

۲-۴) موضوعات امنیتی و مدیریت خدمات:

مدیریت جلسه، مدیریت هویت، دسترسی، کیفیت خدمات (QoS) ،تغییرات سازمانی IT.

۵-۲) مسائل امنیتی زیرساخت‌های فیزیکی:
انعطاف‌پذیری زیرساخت‌ها، اهداف حمله سایبری با ارزش بالا، چند اجاره، مقیاس پذیری و هزینه.

نتیجه گیری:
طبق گزارشات ۱۰ استارتاپ برتری که در مقیاس جهانی در زمینه رایانش ابری به فعالیت اشتغال دارند، موفق شده‌اند بیش از ۷۳۶ میلیون دلار بودجه از سرمایه‌گذاران خطرپذیر به‌دست اورند.
باتوجه به این‌که این فناوری یک فناوری جدید نوظهور است؛ اما رشد خوبی داشته است و در تمام این رشد، امنیت نقش اساسی دارد.
در این مقاله، چالش‌های امنیتی و راه‌حل‌های امنیتی برای غلبه بر این چالش‌ها و خطرهای درگیر در محاسبات ابری ارائه شده‌است.
برای فراهم کردن دسترسی ایمن به داده‌ها در ابر، می‌توان از روش‌های پیشرفته رمزگذاری برای ذخیره و بازیابی داده‌ها از ابر استفاده کرد.
رمزگذاری AES از سطح امنیتی بسیار بالایی برخوردار است.
AES، سریع‌ترین روشی است که قابلیت انعطاف‌پذیری و مقیاس پذیری را دارد و به‌راحتی اجرا می‌شود؛ در این رمزگذاری، حداقل فضا برای ذخیره‌سازی استفاده می‌شود و می‌توان گفت بدون هیچ‌گونه ضعف و محدودیت است. در حالیکه سایر الگوریتم‌های متقارن دارای نقاط ضعف و اختلاف در عملکرد و فضای ذخیره سازی هستند.

مقایسه:
در **بخش اول**، انواع مدل‌های رایانش ابری بررسی و مزایا و معایب ان‌ها بیان شد، به این صورت که:
مدل IaaS: اساسی‌ترین بخش سرویس‌های رایانش ابری است. زیرساخت‌های IT (سرورهای فیزیکی و مجازی)، ذخیره‌سازی، شبکه‌بندی و سیستم‌عامل‌ها را در ازای پرداخت اجاره‌بها، از یک ارائه دهنده خدمات ابری دریافت می‌کند. از موارد استفاده‌شده این مدل، می‌توان به استفاده در زیر ساخت‌های سازمانی و میزبانی وب‌سایت‌ها اشاره کرد.
مدل PaaS: شامل نرم‌افزار و سرویس‌هایی است که به کاربران اجازه می‌دهد، با استفاده از ابزارهای عرضه شده توسط ارایه‌دهنده، اپلیکیشن و نرم‌افزار ایجادکنند.این مدل برای استفاده برنامه-نویسان و توسعه‌دهندگان کسب‌وکار مناسب است.
مدل SaaS: به عنوان سرویس به مشتری، یک اپلیکیشن کامل ارایه میکند، که این سرویس، همان سرویسی است که مشتری تقاضا کرده است. مشتری دیگر نیازی به پرداخت هزینه برای تهیه سرور مناسب و یا خریداری لایسنس نرم‌افزار به صورت جداگانه ندارد و در نتیجه هزینه‌ها به شکل قابل توجهی کاهش می‌یابد. در حال حاضر این مدل در کسب‌وکارهای متفاوتی استفاده می‌شود.
در انتهای بخش، به یک مدل پیشنهادی که دانشمندان برای تامین امنیت داده‌ها در ابر ارائه داده‌اند، پرداخته شد.

در **بخش دوم**، برخی از چالش‌هایی که در تامین امنیت داده‌ها در ابر با ان مواجهه هستیم، بیان شد و مورد بررسی قرار گرفت؛ که از ان‌ها می‌توان به محرمانه بودن، دسترسی، حفظ یکپارچگی و تمامیت داده‌ها اشاره کرد.

در **بخش سوم**، به تامین امنیت داده با استفاده از رمزنگاری پرداخته شد، که شامل سه گروه است:
الگوریتم کلید متقارن: از یک کلید خصوصی برای رمزنگاری و رمزگشایی استفاده می‌کند. این الگوریتم‌ها سرعت پردازشی سریعی دارند و قادر به پردازش حجم وسیعی از داده‌ها هستند.
الگوریتم کلید نامتقارن: از یک کلید برای رمزنگاری و از کلید دیگر برای رمز گشایی استفاده می‌کند. این الگوریتم‌ها در مقایسه با الگوریتم کلید متقارن، سرعت پایین و هزینه محاسباتی بالایی دارند.
توابع هش: از یک انتقال ریاضی برای تبدیل داده‌ها به یک مقدار فشرده استفاده می‌کند، که غیرقابل برگشت است.
در ادامه به بررسی الگوریتم AES پرداخته شد؛ یک الگوریتم رمز-نگاری متقارن است که امروزه بسیار متداول است.این الگوریتم مبتنی‌بر چندین تعویض و جایگشت است؛ مراحل رمزنگاری توسط این الگوریتم نیز بیان شد.

در **بخش چهارم**، برخی از مسائلی که بانک‌ها در محاسبات ابری با ان مواجهه هستند، بیان شد و مورد بررسی قرار گرفت. در بانک-ها، تامین امنیت داده‌ها یک امر بسیار مهم است، زیرا از دست‌دادن امنیت باعث از بین رفتن برند و محبوبیت ان‌ها می‌شود.
در این بخش نیز به بررسی یک مدل رایانش ابری پراخته شد:
مدل BPaaS: فرآیندهای کسب و کار به عنوان سرویس هستند که هرگونه فرآیندهای کسب و کار را در بستر ابر ارائه می‌دهند. هدف اصلی این مدل کاهش هزینه‌های نیروی انسانی، از طریق افزایش خودکارسازی است.

مراجع:

[1] Abdelrafe Elzamly1, Burairah Hussin 2, Samy S. Abu Naser3, Tadahiro Shibutani4, and Mohamed Doheir5. "Predicting Critical Cloud Computing Security Issues using Artificial Neural Network (ANNs) Algorithms in Banking Organizations". International Journal of Information Technology and Electrical Engineering, April ,2017

[2] Nidal Hassan Hussein And Ahmed Khalid."A survey of Cloud Computing Security challenges and solutions". International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 1, January 2016

[3] R. Velumadhava Raoa,*, K. Selvamanib,* ." Data Security Challenges and Its Solutions in Cloud Computing". International Conference on Intelligent Computing, Communication & Convergence , India,2015

[4] Vishal R. Pancholi And Dr. Bhadresh P. Patel ."Enhancement of Cloud Computing Security with Secure Data Storage using AES". International Journal for Innovative Research in Science & Technology, Volume 2 ,ISSN: 2349-6010, 2016

پاورقی‌ها:

[۱] Software as a Service

[۲] Platform as a Service

[۳] Infrastructure as a Service

[۴] Virtual Machine

[۵] Denial of Service

[۶] Intrusion Detection System: وظیفه شناسایی و تشخیص هر گونه استفاده غیرمجاز به سیستم، سوءاستفاده یا آسیب‌رسانی توسط هر دو دسته کاربران داخلی و خارجی را بر عهده دارند.

[۷] Operating System

[۸] Cloud Service Provider

[۹] Policy Enforcement Point

[۱۰] Application Programming Interface

[۱۱] Extendable Markup Language

[۱۲] *Atomicity*, *Consistency*, *Isolation*, *Durability*

[۱۳] Breaches

[۱۴] Structured Query Language

[۱۵] Data Encryption Standard

[۱۶] Advanced Encryption Standard

[۱۷] Rivest Shamir Adleman

[۱۸] Personal Digital Assistant

[۱۹] Business Process as a Service