



دانشگاه آزاد اسلامی

واحد علوم تحقیقات

دانشکده تحصیلات تکمیلی گروه فنی و مهندسی

پایان نامه برای دریافت درجه کارشناسی ارشد در رشته کامپیوتر (M.Sc)

گرایش نرم افزار

عنوان

بررسی، مقایسه و شبیه سازی راهکارهای امنیتی در رایانش ابری

استاد راهنما

دکتر عبدالمجید موسوی

استاد مشاور

دکتر حسن نادری

نگارش

عرفان نیازی

شهریور ۱۳۹۳

فهرست مطالب

چکیده ۱

فصل اول: مقدمه

۱-۱- تعریف ۳

۱-۱-۱- رایانش ابری سیار ۳

۱-۱-۲- سیستم های تشخیص نفوذ در ابر رایانشی ۴

۱-۱-۳- امنیت در ابر رایانشی ۵

۱-۱-۴- امضای دیجیتال ۵

۱-۲- روش شناسی تحقیق ۵

۱-۳- اهداف مشخص تحقیق ۶

۱-۴- دستاورد پروژه ۶

۱-۵- اهمیت و ضرورت انجام تحقیق ۷

۱-۵-۱- حمله به بسته (SOAP (Wrapping Attack) - لایه پلتفرم به عنوان سرویس ۹

۱-۵-۲- حمله از طریق کدهای مخرب (Malware-Injection) - لایه نرم افزار کاربردی ۱۱

۱-۵-۳- حمله سیل آسا (Flooding Attack) - لایه پلتفرم به عنوان سرویس ۱۱

۱-۵-۴- سرقت اطلاعات (Data Stealing) - لایه پلتفرم به عنوان سرویس ۱۱

۱-۶- جنبه جدید بودن و نوآوری در تحقیق ۱۲

فصل دوم: سابقه پژوهش

۱-۲- شرح تحقیق ۱۵

۲-۲- سابقه پژوهش ۱۵

۱-۲-۲- سابقه پژوهش ابر رایانشی ۱۵

۱-۲-۲-۱- مزایا و نقاط قوت Cloud Computing ۱۵

۱-۲-۲-۱-۱- هزینه های کمتر ۱۵

۱-۲-۲-۱-۲- سرعت بیشتر ۱۶

۱-۲-۲-۱-۳- مقیاس پذیری ۱۶

۱۶	به روزرسانی نرم افزاری سریع و دائم	۲-۱-۱-۴
۱۶	ذخیره سازی اطلاعات	۲-۱-۱-۵
۱۶	دسترسی جهانی به اسناد	۲-۱-۱-۶
۱۷	مستقل از سخت افزار	۲-۱-۱-۷
۱۷	نقاط ضعف رایانش ابری	۲-۱-۲-۲
۱۷	نیاز به اتصال دائمی اینترنت	۲-۱-۲-۱
۱۷	با اتصال های اینترنتی کم سرعت کار نمی کند	۲-۱-۲-۲
۱۷	محدودیت ویژگی ها	۲-۱-۲-۳
۱۸	عدم امنیت داده ها	۲-۱-۲-۴
۱۸	انواع ابر	۲-۱-۳-۳
۱۸	ابر عمومی (Public cloud)	۲-۱-۳-۱
۱۸	ابر خصوصی (Private cloud)	۲-۱-۳-۲
۱۸	ابر گروهی (Community cloud)	۲-۱-۳-۳
۱۸	ابر آمیخته (Hybrid cloud)	۲-۱-۳-۴
۱۹	معرفی نمودارها و معماری های ابر	۲-۱-۴-۴
۱۹	Single "All-in-one" Server	۲-۱-۴-۱
۱۹	Non-Redundant 3-Tier Architecture	۲-۱-۴-۲
۲۰	Multi-Datcenter معماری	۲-۱-۴-۳
۲۱	Autoscaling معماری	۲-۱-۴-۴
۲۱	Membase مقیاس پذیر با	۲-۱-۴-۵
۲۲	Memcached مقیاس پذیر با	۲-۱-۴-۶
۲۲	Scalable Queue-based Setups مقیاس پذیر مبتنی بر صف	۲-۱-۴-۷
۲۳	Hybrid داخلی	۲-۱-۴-۸
۲۳	مقیاس پذیر مبتنی بر هشدار و مبتنی بر صف	۲-۱-۴-۹
۲۳	Hybrid Cloud Site Architectures ابر ترکیبی سایت	۲-۱-۴-۹
۲۳	معماری مقیاس پذیر چند ابری	۲-۱-۴-۱۰

۲۴	Failover	۱۱-۴-۱-۲-۲ معماری چند ابری
۲۴		۱۲-۴-۱-۲-۲ معماری بازیابی فاجعه چند ابری
۲۴		۱۲-۴-۱-۲-۲ معماری ابر و میزبانی اختصاصی
۲۵		۲-۲-۲ سابقه پژوهش بررسی سیستم های تشخیص و پیشگیری از نفوذ در محاسبات ابری
۲۶		۱-۲-۲-۲ نتیجه گیری از سابقه پژوهش سیستم های تشخیص و پیشگیری نفوذ
۲۶		۱-۲-۲-۲ طبقه بندی سیستم های تشخیص و پیشگیری نفوذ
۳۱		۲-۱-۲-۲-۲ چالش های توسعه سیستم های تشخیص و جلوگیری از نفوذ
۳۱		۳-۱-۲-۲-۲ سیستم های تشخیص پیشگیری نفوذ در محاسبات ابری
۳۲		۴-۱-۲-۲-۲ مسائل امنیتی در محاسبات ابری
۳۲		۵-۱-۲-۲-۲ چالش های استقرار سیستم های تشخیص و جلوگیری از نفوذها در محیط های پردازش ابری
۳۳		۶-۱-۲-۲-۲ سیستم های تشخیص و جلوگیری از نفوذ مبتنی بر محاسبات ابری
۳۴		۷-۱-۲-۲-۲ الزامات سیستم های تشخیص و جلوگیری از نفوذ
۳۵		۳-۲-۲ سابقه پژوهش ایجاد امنیت در ابر رایانشی
۳۶		۱-۳-۲-۲ مفهوم حریم خصوصی در محاسبات ابری
۳۷		۲-۳-۲-۲ انواع اطلاعات نیازمند به حفاظت
۳۷		۳-۳-۲-۲ چرخه زندگی داده
۳۸		۱-۳-۳-۲-۲ تولید (Generation)
۳۸		۲-۳-۳-۲-۲ استفاده (Use)
۳۸		۳-۳-۳-۲-۲ انتقال (Transfer)
۳۸		۴-۳-۳-۲-۲ تبدیل (Transformation)
۳۸		۵-۳-۳-۲-۲ ذخیره سازی (Storage)
۳۸		۶-۳-۳-۲-۲ بایگانی (Archive)
۳۹		۷-۳-۳-۲-۲ تخریب (Destruction)
۳۹		۴-۳-۲-۲ مسائل حریم خصوصی و چالش های آن
۳۹		۱-۴-۳-۲-۲ دسترسی (Access)
۳۹		۲-۴-۳-۲-۲ مقبولیت (Compliance)

۳۹	 ذخیره سازی (Storage) ۳-۴-۳-۲-۲
۴۰	 حفظ و نگهداری (Retention) ۴-۴-۳-۲-۲
۴۰	 تخریب (Destruction) ۵-۴-۳-۲-۲
۴۰	 نظارت و مانیتورینگ (Audit & Monitoring) ۵-۳-۲-۲
۴۰	 نقض حریم خصوصی (Breaches) امنیت و محرمانگی ۶-۳-۲-۲
۴۰	 تکنیک های متداول جهت حفظ حریم خصوصی ۷-۳-۲-۲
۴۰	 Encryption Model ۱-۷-۳-۲-۲
۴۱	 Access Control Mechanism ۲-۷-۳-۲-۲
۴۱	 سابقه پژوهش کلی در بررسی راهکارهای امنیتی در رایانش ابری ۳-۲-۲
۴۳	 علل شکست امنیت رایانش ابری ۱-۳-۲-۲
۴۳	 سابقه پژوهش امضای دیجیتالی ۴-۲-۲
۴۳	 ۱-۴-۲-۲ امضای دیجیتال و امنیت دیجیتالی چیست
۴۴	 ۲-۴-۲-۲ گواهینامه دیجیتالی چیست
۴۴	 ۳-۴-۲-۲ ثبت نام برای یک گواهینامه دیجیتالی
۴۴	 ۴-۴-۲-۲ پخش کردن گواهینامه دیجیتالی
۴۵	 ۵-۴-۲-۲ انواع مختلف گواهینامه دیجیتالی
۴۵	 ۶-۴-۲-۲ امضای دیجیتالی از دید برنامه نویسی
۴۶	 ۷-۴-۲-۲ چگونه یک امضای دیجیتالی درست کنیم
۴۷	 ۸-۴-۲-۲ نحوه عملکرد یک امضای دیجیتال
۴۸	 ۹-۴-۲-۲ نحوه ایجاد و استفاده از کلیدها
۴۸	 ۱۰-۴-۲-۲ حملات ممکن علیه امضاءهای دیجیتالی
۴۸	 ۱۱-۴-۲-۲ مرکز صدور گواهینامه چیست
۴۹	 ۱۲-۴-۲-۲ رمزنگاری چیست
۵۰	 ۱۳-۴-۲-۲ تشخیص هویت از طریق امضای دیجیتالی
۵۰	 ۱۴-۴-۲-۲ امضای دیجیتالی زیربنای امنیت تبادلات الکترونیکی
۵۱	 ۱۵-۴-۲-۲ منظور از امضای دیجیتالی چیست

۵۱	استفاد از امضای دیجیتال تا چه حد امنیت تبادل اسناد مالی و محرمانه را تضمین می‌کند
۵۳	چیست SSL-۱۷-۴-۲-۲
۵۴	چیست InstantSSL-۱-۱۷-۴-۲-۲
۵۴	تکنولوژی پیشرفته تأیید کردن (Authentication)-۲-۱۷-۴-۲-۲
۵۴	دسترسی آنلاین به پروفایل تان در ابر-۳-۱۷-۴-۲-۲
۵۵	مفاهیم رمز گذاری-۱۸-۴-۲-۲
۵۵	معرفی و اصطلاحات-۱-۱۸-۴-۲-۲
۵۶	الگوریتم‌ها-۲-۱۸-۴-۲-۲
۵۶	رمزنگاری کلید عمومی-۳-۱۸-۴-۲-۲
۵۷	مقدار Hash-۴-۱۸-۴-۲-۲
۵۸	آیا شما معتبر هستید-۵-۱۸-۴-۲-۲
۶۰	سیستم های کلید متقارن-۶-۱۸-۴-۲-۲
۶۱	سیستم های کلید نامتقارن-۷-۱۸-۴-۲-۲
۶۴	ساختار و روند آغازین پایه گذاری یک ارتباط امن-۱۹-۴-۲-۲
۶۵	پروتکل های مشابه-۲۰-۴-۲-۲
۶۵	مفهوم گواهینامه در پروتکل SSL-۲۱-۴-۲-۲
۶۶	مراکز صدور گواهینامه-۲۲-۴-۲-۲
۶۶	مراحل کلی برقراری و ایجاد ارتباط امن در وب-۲۳-۴-۲-۲
۶۷	نکاتی در مورد گواهینامه ها-۲۴-۴-۲-۲
۶۸	تشخیص هویت-۲۵-۴-۲-۲
۶۸	سرویس های امنیتی WEP – Authentication-۲۶-۴-۲-۲
۶۹	بدون رمزنگاری Authentication-۲۷-۴-۲-۲
۷۰	Authentication با رمزنگاری RC4-28-۴-۲-۲
۷۱	محرمانگی و امنیت-۲۹-۴-۲-۲
۷۲	Integrity-۳۰-۴-۲-۲
۷۳	ضعف های اولیه ای امنیتی WEP-۳۱-۴-۲-۲

۷۵	 ۲-۲-۴-۳۲-خطر ها، حملات و ملزومات امنیتی
۷۷	 ۲-۲-۴-۳۳-مشکلات و معایب SSL
۷۷	 ۲-۲-۴-۳۳-۱-مشکل امنیتی در SSL
۷۸	 ۲-۲-۴-۳۳-۲-مشکلات تجارت الکترونیکی در ایران

فصل سوم: روش تحقیق

۸۰	 ۳-۱-۱-بازار مورد استفاده در شبیه سازی
۸۰	 ۳-۲-۲-نصب NS-2 در لینوکس Fedora

فصل چهارم: نتیجه گیری

۸۴	 نتیجه گیری
۸۵	 ۴-۱-۱- راه حل های پیشنهادی ممکن جهت حملات راهکارهای امنیتی رایانش ابری
۸۷	 ۴-۲-۲- معیارهای مقایسه مورد استفاده در شبیه سازی و ارتباط هریک از آنها به امنیت ابری به تفکیک
۸۷	 ۴-۲-۱- معیار Delay Time
۸۷	 ۴-۲-۲- معیار Throughput Security
۸۸	 ۴-۲-۳- معیار Response Time
۸۸	 ۴-۲-۴- معیار Traffic Ratio
۸۸	 ۴-۳-۳- نتایج به دست آمده از شبیه سازی راهکارهای امنیتی با نرم افزار NS2
۸۸	 ۴-۳-۱- Delay Time (Sec)
۸۹	 ۴-۳-۱-۱- نتیجه گیری از شبیه سازی معیار Delay Time
۹۰	 ۴-۳-۲- Throughput Security (Kb)
۹۱	 ۴-۳-۱-۲- نتیجه گیری از شبیه سازی معیار Throughput Security
۹۱	 ۴-۳-۳- Response Time (Sec)
۹۲	 ۴-۳-۱-۳- نتیجه گیری از شبیه سازی معیار Time Response
۹۳	 ۴-۳-۴- Packet Traffic Ratio (%)
۹۴	 ۴-۳-۱-۴- نتیجه گیری از شبیه سازی معیار Traffic Ratio
۹۴	 ۴-۴- نتیجه گیری کلی از شبیه سازی و مقایسه راهکارهای امنیتی ابر

فصل پنجم: جمع بندی و پیشنهادات

جمع بندی	۹۶
۱-۵- حفاظت از داده‌ها	۹۶
۲-۵- مکان فیزیکی	۹۶
۳-۵- از بین رفتن داده‌ها	۹۶
۴-۵- کنترل دسترسی	۹۶
۵-۵- قوانین حفظ حریم خصوصی	۹۷
۶-۵- پیشنهاداتی برای بهبود حفظ حریم خصوصی	۹۷
۱-۶-۵- برای کاربران ابر	۹۷
۲-۶-۵- برای سرویس دهنده‌های ابر	۹۷
فهرست منابع	۹۹

فهرست اشکال

شکل ۱-۱	۱- بسته SOAP	۹
شکل ۱-۲	پیام SOAP قبل از حمله	۱۰
شکل ۱-۳	پیام SOAP بعد از حمله	۱۰
شکل ۲-۱	Single Cloud Site Architectures	۱۹
شکل ۲-۲	Redundant 3-Tier Architecture	۲۰
شکل ۲-۳	Multi-Datacenter معماری	۲۰
شکل ۲-۴	Autoscaling معماری	۲۱
شکل ۲-۵	Membase مقیاس پذیر با	۲۱
شکل ۲-۶	Memcached مقیاس پذیر با	۲۲
شکل ۲-۷	Scalable Queue-based Setups مقیاس پذیر مبتنی بر صف	۲۲
شکل ۲-۸	Scalable Alarm-based Setups مقیاس پذیر مبتنی بر هشدار	۲۳
شکل ۲-۹	طبقه بندی سیستم های تشخیص و پیشگیری از نفوذ	۲۸
شکل ۲-۱۰	چهارچوب عملکردی IDPS	۳۰
شکل ۲-۱۱	دید مفهومی از CIDS	۳۱
شکل ۲-۱۲	چرخه زندگی داده	۳۷
شکل ۲-۱۳	نتایج بررسی IDC از چالش های رایانش ابری در سال (۲۰۰۲)	۴۱
شکل ۲-۱۴	رمزنگاری خصوصی و عمومی	۴۹
شکل ۲-۱۵	اهداف CA	۵۰
شکل ۲-۱۶	SSL	۵۴
شکل ۲-۱۷	سیستم های کلید نامتقارن	۶۳
شکل ۲-۱۸	ساختار نهایی سیستم های کلید نامتقارن	۶۴
شکل ۲-۱۹	مراکز صدور گواهینامه	۶۶
شکل ۲-۲۰	تشخیص هویت	۶۹
شکل ۲-۲۱	Authentication با رمزنگاری RC4	۷۰

شکل ۲-۲۲- روش استفاده شده توسط WEP برای تضمین محرمانگی	۷۲
شکل ۲-۲۳- ضعف‌های اولیه‌ی امنیتی WEP	۷۵
شکل ۲-۲۴- خطرها، حملات و ملزومات امنیتی	۷۵
شکل ۳-۱- تصویر خط اعلان Terminal	۸۲
شکل ۴-۱- اجرای برنامه‌ها توسط Hypervisor	۸۶
شکل ۴-۲- پیام بین سرورها	۸۷
شکل ۴-۳- نمودار مقایسه چهار راهکار امنیتی Delay Time	۸۹
شکل ۴-۴- نمودار مقایسه چهار راهکار امنیتی Throughput Security	۹۰
شکل ۴-۵- نمودار مقایسه چهار راهکار امنیتی Response Time	۹۲
شکل ۴-۶- نمودار مقایسه چهار راهکار امنیتی Packet Traffic Ratio	۹۳

فهرست جداول

جدول ۱-۲	چهار عملکرد ضروری امنیتی سیستم های نفوذ	۲۷
جدول ۱-۴	مقایسه Delay Time چهار راهکار امنیتی با زمان های ۴۲ تا ۳۰۰	۸۸
جدول ۲-۴	نتیجه معیار مقایسه Delay Time چهار راهکار امنیتی با زمان های ۴۲ تا ۳۰۰	۸۹
جدول ۳-۴	مقایسه Throughput Security چهار راهکار امنیتی با زمان های ۴۲ تا ۳۰۰	۹۰
جدول ۴-۴	نتیجه معیار مقایسه Throughput Security چهار راهکار امنیتی با زمان های ۴۲ تا ۳۰۰	۹۱
جدول ۵-۴	مقایسه Response Time چهار راهکار امنیتی با زمان های ۴۲ تا ۳۰۰	۹۱
جدول ۶-۴	نتیجه معیار مقایسه Time Response چهار راهکار امنیتی با زمان های ۴۲ تا ۳۰۰	۹۲
جدول ۷-۴	مقایسه Packet Traffic Ratio چهار راهکار امنیتی با زمان های ۴۲ تا ۳۰۰	۹۳
جدول ۸-۴	نتیجه معیار مقایسه Traffic Ratio چهار راهکار امنیتی با زمان های ۴۲ تا ۳۰۰	۹۴
جدول ۹-۴	نتیجه کلی مقایسه معیارها	۹۴

چکیده

باتوجه به آینده محاسبات ابری و گسترش کاربردهای آن و مزایای موجود در این تکنولوژی، همواره چالش‌هایی نیز برای کاربران وجود دارد که یکی از مهمترین و بحث برانگیزترین این چالش‌ها حفظ حریم خصوصی می باشد. با توجه به ذخیره‌سازی داده‌های خصوصی کاربران و داده‌های تجاری شرکت‌ها در محاسبات ابری، حفظ حریم خصوصی مسئله‌ای بسیار مهم برای کاربران استفاده کننده از محاسبات ابر و خود ارائه‌دهندگان سرویس‌های ابری می باشد. از بین حملات ابری چهار حمله اصلی که شامل حمله سیل آسا، حمله به بسته، حمله کدهای مخرب و حمله سرقت اطلاعات می باشد که در ابتدا این حملات و روش‌های مقابله با آن‌ها بررسی و در نهایت در این گزارش ما با استفاده از شبیه سازی این چهار راهکار امنیتی پیشنهادی رایانش ابری در نرم افزار NS2 و مقایسه نتایج به دست آمده آن به بررسی مسائل مربوط به حفظ حریم خصوصی در ابر و چالش‌های پیش رو می پردازیم و پیشنهاداتی را برای کاربران و ارائه دهندگان مطرح می کنیم.

کلمات کلیدی

محاسبات ابری^۱، حریم خصوصی^۲، حفظ حریم خصوصی^۳، سیستم‌های تشخیص نفوذ، امضای دیجیتال

^۱Cloud computing

²Privacy

^۳Privacy preserving

فصل اول

مقدمه

۱-۱- تعریف

با توجه به گستردگی بحث امنیت در ابر رایانشی بررسی این مقوله ملزم به تفکیک قسمت‌های مختلف می‌باشد. در ابتدای امر باید تعریف کلی از ابر رایانشی داشته و سپس سیستم‌های تشخیص نفوذ توضیح داده خواهد شد.

۱-۱-۱- رایانش ابری سیار

رایانش ابری به گونه‌ای سیستم‌های توزیع شده و موازی اطلاق می‌گردد که مجموعه‌ای از کامپیوترهای را که به یکدیگر متصل هستند شامل می‌شود. این کامپیوترها بطور پویا عرضه شده و بعنوان یک یا چند منبع محاسباتی یکپارچه بر اساس توافقات سرویس دیده می‌شوند. این توافقات در طول رد و بدل شدن پیام میان سرویس‌دهندگان و کاربران برقرار می‌گردند. رایانش ابری سعی در ایجاد نسل جدیدی از مراکز داده‌ای، با ارائه سرویس‌ها و خدمات در ماشین‌های مجازی شبکه شده بصورت پویا دارد، و این عمل به گونه ای تحقق می‌یابد که کاربران بتوانند از هر جای دنیا به برنامه‌های کاربردی دسترسی داشته باشند. [1]

بر طبق تعریف ویکی‌پدیا موسسه ملی فناوری و استانداردها (NIST) رایانش ابری را اینگونه تعریف می‌کند: «رایانش ابری مدلی برای فراهم کردن دسترسی آسان به مجموعه‌ای از منابع رایانشی قابل تغییر و پیکربندی (مثل: شبکه‌ها، سرورها، فضای ذخیره‌سازی، برنامه‌های کاربردی و سرویس‌ها) بر اساس تقاضای کاربر از طریق شبکه می‌باشد بشکلی که این دسترسی بتواند با کمترین نیاز به مدیریت منابع یا دخالت مستقیم فراهم‌کننده سرویس به سرعت فراهم شود.» عموماً کاربران رایانش ابری مالک زیر ساخت فیزیکی ابر نیستند، بلکه برای اجتناب از هزینه آن را از عرضه کنندگان شخص ثالث اجاره می‌کنند. آنها منابع را در قالب سرویس مصرف می‌کنند و تنها بهای منابعی که به کار می‌برند را می‌پردازند. بسیاری از سرویس‌های رایانش ابری ارائه شده، با به کارگیری مدل رایانش همگانی امکان مصرف این سرویس‌ها را به گونه‌ای مشابه با صنایع همگانی (مانند برق) فراهم می‌سازند. این در حالی است که سایر گونه‌های عرضه کننده سرویس، بر مبنای اشتراک سرویس‌های خود را عرضه می‌کنند.

۱-۲- سیستم‌های تشخیص نفوذ در ابر رایانشی

ساختار باز و توزیع شده پردازش ابری و سرویس‌ها، هدفی مورد توجه برای حملات سایبری مهاجمان شده است. سیستم‌های تشخیص و پیشگیری نفوذ قدیمی به دلیل باز بودن و ماهیت خاصشان، تا حد زیادی برای مستقر شدن در محیط‌های پردازش ابری ناکارآمد هستند. معرفی سیستم‌های تشخیص و پیشگیری از نفوذ و نحوه عملکرد و طبقه‌بندی‌های متفاوت آن‌ها، می‌تواند آخرین دستاورد در زمینه شناسایی چالش‌های استقرار در محاسبات ابری باشد.

در طول سال‌های گذشته جوامع بشری بیش از پیش به تکنولوژی وابسته شده‌اند. کاربران برای دریافت اخبار، قیمت سهام، ایمیل و خرید آنلاین بر شبکه‌های کامپیوتری تکیه می‌کنند. یکپارچگی و در دسترس بودن همه این سیستم‌ها، نیازمند دفاع در مقابل شماری از تهدیدها می‌باشد. هکرها، آماتور، شرکت‌های رقیب، تروریست‌ها و حتی دولت‌های خارجی دارای انگیزه و توانایی بالقوه‌ای برای انجام حملات پیچیده علیه سیستم‌های کامپیوتری می‌باشند.

بنابراین امنیت اطلاعات برای ایمنی و رفاه اقتصادی جامعه با توجه به اینکه رشد سریع و استفاده گسترده از پردازش الکترونیکی داده‌ها و کسب و کار الکترونیکی، از طریق شبکه‌های ارتباطی سیمی و بی‌سیم، اینترنت و برنامه‌های کاربردی وب انجام می‌شود به عنوان یک اصل، مهم و حیاتی است. [1]

معماری سرویس پردازش ابری ترکیبی از 3 لایه زیرساخت، پلت‌فرم و برنامه کاربردی است که به هم وابسته می‌باشند. هر لایه ممکن است توسط برنامه‌نویسی‌های مختلف یا خطاهای پیکربندی کاربر و یا ارائه‌دهنده سرویس آسیب‌پذیر باشد. یک سیستم پردازش ابری می‌تواند در مقابل تهدیدات مختلف از جمله تهدیدات مربوط به جامعیت، محرمانگی و دسترس‌پذیری منابع و زیرساخت‌های مجازی آسیب‌پذیر باشد. این مشکل هنگامی که محیط یک ابر با پردازش و ظرفیت ذخیره‌سازی عظیم توسط یک نفوذ خودی مورد تهاجم قرار می‌گیرد، مهم‌تر می‌شود. اهمیت این موضوع بیشتر روشن می‌گردد وقتی بدانیم در سال 2011 یک هکر با استفاده از سرویس پردازش ابر Amazon Elastic به سیستم‌های سرگرمی آنلاین سونی با ثبت نام و بازکردن یک حساب حمله کرد.

سرویس‌های ابر برای هکرها هنگامی که خود را به عنوان مشتریان سرویس معرفی می‌کنند، قابل دسترس و راحت هستند. عدم کنترل کامل بر روی زیرساخت یک نگرانی بزرگ برای مشتریان سرویس ابر می‌باشد. این خود نشانگر نقش سیستم‌های تشخیص در حفاظت از دارایی‌های اطلاعاتی کاربر در پردازش ابری است. [1]

۱-۳- امنیت در ابر رایانشی

مفهوم امنیت و محرمانگی^۴ در میان کشورها و جوامع و حوزه‌های قضایی مختلف متفاوت می‌باشد و به کمک انتظارات عمومی و تفاسیر حقوقی شکل می‌گیرد، ارائه یک تعریف کامل از محرمانگی و امنیت گرچه غیرممکن نیست ولی دشوار است. تعهداتی که شامل حریم خصوصی می‌شود عبارتند از جمع‌آوری، استفاده، افشاء، ذخیره‌سازی و تخریب داده‌های شخصی افراد می‌باشد. بخاطر عدم وجود هیچگونه اجماع جهانی در مورد اینکه چه مواردی شامل حریم خصوصی می‌شود در اینجا از تعریفی که توسط موسسه آمریکایی AICPA^۵ و موسسه کانادایی CICA^۶ ارائه شده است استفاده می‌کنیم: حریم خصوصی شامل حقوق و تعهدات اشخاص و سازمانها در رابطه با جمع‌آوری، استفاده، حفظ و افشاء اطلاعات خصوصی افراد می‌باشد. [2]

۱-۴- امضای دیجیتال

یکی از مهمترین روش‌های کنونی ایجاد امنیت در شبکه، امضای دیجیتال می‌باشد. امضای دیجیتالی بر روش‌های رمزنگاری از طریق کلیدهای عمومی و خصوصی مبتنی است. در حال حاضر در کشورهای متعدد و برای کاربردهای گوناگون از صدور ایمیل گرفته تا نقل و انتقالات مالی و امضای اسناد تعهدآور همانند ابزاری که به اطلاعات روح می‌دهد مورد استفاده قرار می‌گیرد و کاربرد آن در شبکه‌های الکترونیکی به یک ضرورت تبدیل شده و در شرایطی که ایمیل‌های ارسال شده به صندوق الکترونیکی یک فرد از لحاظ امنیتی قابل تأیید نیست، امضای دیجیتال این امکان را فراهم می‌کند تا فرد مورد نظر با اطمینان از لحاظ امنیتی تبادلات خود را انجام دهد.

۱-۲- روش شناسی تحقیق

۱- مطالعه مباحث مربوط به امنیت در وب و رانش ابری

۲- طرح مسئله

۳- انتخاب یک مسئله خاص در بحث امنیت در ابر رایانشی و بررسی کامل و جامع آن

۴- تحلیل مسئله بررسی شده

۵- نتیجه گیری

برای تحقق اهداف فوق از کتب مرجع، بانک‌های اطلاعاتی آنلاین، اینترنت، مقالات و تجربیات اساتید محترم استفاده می‌شود.

⁴Privacy

^۵American Institute of Certified Public Accountants

^۶Canadian Institute of chartered Accountants

۱-۳- اهداف مشخص تحقیق

- ✓ بررسی انتقادی مسائل امنیتی ابر و مدل امنیتی جاری ابر رایانشی.
- ✓ شناسایی محدودیت های اصلی مدل امنیتی فعلی و شبیه سازی حملات امنیتی برای داده های ابر و امنیت اطلاعات.
- ✓ ایجاد یک سناریوی معمولی که در آن هیچ پیاده سازی برای مبارزه با حملات ابری وجود ندارد، و ایجاد یک سناریوی با اعمال راهکارهای امنیت ابری.
- ✓ اندازه گیری عملکرد ابر در این چهار سناریو با استفاده از برخی از معیارهای عملکرد.
- ✓ مقایسه نتایج سناریو و نمودار مربوطه و ارزیابی عملکرد ابر و درک سطح امنیت مورد نیاز.

۱-۴- دستاورد پروژه

هدف اصلی این پروژه بررسی امنیت رایانش ابری می باشد که تحت چهار سناریو مختلف در محیط شبیه ساز NS2 ایجاد شده است. سناریو اول بررسی راهکار امنیتی در حمله از طریق کدهای مخرب، سناریوی دوم راهکار امنیتی حمله به بسته SOAP در حالیکه سومین سناریو راهکار امنیتی حمله سیل آسا می باشد. هر چهار سناریو بعنوان معیارهای برای برنامه های کاربردی فردی و نیز تخمین زدن عملکرد درست ابر مقایسه شده است. بمنظور درک موضوع امنیت در رایانش ابری باید مشکلات امنیتی را به بخش های کوچک تر تجزیه کنیم. در سازمان هایی که از سرویس های پردازش ابری استفاده می کنند، تمام مشکلات امنیتی در سه گروه اصلی جای می گیرند که ما نیز اهداف خود را بر مبنای این سه گروه قرار خواهیم داد:

- امنیت پلتفرمی که در اقامتگاه سرویس دهنده ابری قرار دارد.
 - امنیت ایستگاه های کاری (نقاط انتهایی) که در اقامتگاه کلاینت ها قرار دارد.
 - امنیت داده هایی که از نقاط انتهایی به پلتفرم ارسال می شود.
- در این چارچوب پس از شناسایی کاربران مجاز داده ها رمزگذاری شده و در سمت فراهم آورنده رمزگشایی و سپس ذخیره خواهد شد. مراحل کار در چارچوب فوق عبارتند از:

۱- سیاست های امنیتی

امکان تنظیم تغییر رمز عبور کاربران به صورت اجباری در زمان های مشخص
تأمین کننده رمز عبور سرور

۲- پشتیبان گیری، بازیابی، ثبت وقایع

پشتیبان گیری از داده ها باید در فواصل زمانی منظم صورت گیرد.
تدابیر لازم جهت بازگردانی داده ها توسط فراهم آورندگان باید صورت بگیرد.
به روز رسانی ها به صورت منظم باید صورت بگیرد.

۳- تست نفوذ

برای اطمینان از سیستم ارائه دهنده باید در فواصل منظم زمانی تست سیستم صورت پذیرد. فایروال نصب شده و تنظیمات آن انجام شود. نرم افزار ضد ویروس نصب و به روزرسانی شود.

۴- زیرساخت های فیزیکی امن

محل فیزیکی سرور امری حیاتی است، ارائه دهندگان ابر باید از دستگاه های ذخیره سازی در مکان های امن با حفاظت فیزیکی مناسب نگهداری کنند. البته باید توجه داشت که چارچوب فوق شاید خیلی ساده به نظر برسد اما می تواند به عنوان کمکی در گسترش امنیت در ابر باشد.

۱-۵- اهمیت و ضرورت انجام تحقیق

اهمیت و ضرورت انجام تحقیق جاری شامل اختلاف نظرها و خلاءهای تحقیقاتی موجود، میزان نیاز به موضوع، فواید احتمالی نظری و عملی آن و همچنین مواد، روش و یا فرآیند تحقیقی احتمالاً جدیدی که در این تحقیق مورد استفاده قرار می گیرد.

با شبیه سازی و مقایسه راهکارهای امنیتی موجود در رایانش ابری می توان به نقاط ضعف و قدرت هر یک دست یافت که این می تواند در بکارگیری هر کدام از این راهکارها و بالا بردن امنیت محیط ابر، کمک شایانی به ما بکند. همچنین با بررسی نقاط قوت این راهکارها می توان در آینده راهکاری جدید مبتنی بر تلفیقی از این نقاط قوت ارائه داد که البته خارج از بحث این پایان نامه می باشد.

با توجه به تکامل در عرصه رایانش ابری، روش های بسیاری جهت توزیع منابع و پیشرفت استفاده از داده ها از قبیل خوشه بندی داده ها، رایانش توری و سیستم مدیریت پایگاه داده های توزیع شده معرفی شده اند. امروزه رایانش ابری مکانیزمی در حال ظهور برای محاسبات سطح بالا به عنوان یک سیستم ذخیره سازی تلقی می شود که در آن ابرها به کاربران خود بر مبنای میزان استفاده از منابع هزینه دریافت کرده و سرویس های خود را در اختیار آنها قرار می دهند. از این رو می توان سرویس های ابری را در ایجاد انگیزه برای شروع یک کسب و کار با هزینه های مالی پایین تر سهیم دانست. رایانش ابری بسته به نوع توزیع منابع از سه لایه زیرساخت به عنوان سرویس، پلتفرم به عنوان سرویس و نرم افزار کاربردی به عنوان سرویس تشکیل شده است.

در پایین ترین سطح که لایه زیرساخت به عنوان سرویس^۷ نامیده می شود. پردازنده، حافظه و اجزای سخت افزاری توسط فراهم کننده سرویس ابری ارائه می گردد. لایه میانی یا پلتفرم به عنوان سرویس^۸ میزبان محیط های مختلف برای ارائه خدمات

7 IaaS
8 PaaS

می‌باشد. در آخر بالاترین لایه نرم‌افزار کاربردی به عنوان سرویس^۹ است که دسترسی به این خدمات از طریق وب سرویس ها و مرورگرهای وب صورت می‌گیرد Amazon Ec2, Google App و Salesforce به ترتیب نمونه‌های لایه‌های ارائه شده رایانش ابری می‌باشند.

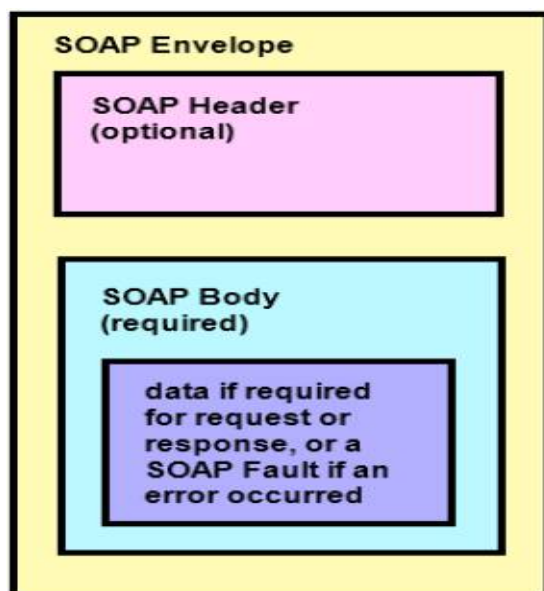
واضح است که رایانش ابری گام بعدی تکامل سرویس های فناوری اطلاعات بر حسب تقاضا می‌باشد. با این حال مسئله امنیت در رایانش ابری یکی از مسائل پیچیده به شمار رفته که تمامی سه لایه ابر، مسئولیت‌هایی که بین کاربران و ارائه دهندگان تقسیم می‌شود و حتی شخص ثالث کاربر را نیز درگیر می‌کند. مشکلات امنیتی به عنوان یک مانع بزرگ در مقابل استفاده کاربران از سیستم‌های رایانش ابری قلمداد می‌شود. هدف از ارائه این مقاله شناخت حملات امنیتی اولیه بر روی ابر می‌باشد. در ادامه به معرفی کوتاه امنیت ابر و مسائل مطرح در آن پرداخته شده و سه حمله امنیتی و راه کار مقابله با آن مورد بررسی قرار خواهد گرفت.

در ادامه مهم‌ترین مسائل مربوط به امنیت رایانش ابری از جمله پیام SOAP و حملات ابر که توسط دشمنان مزاحم آن صورت می‌گیرد، مطرح می‌شود.

وب سرویس تکنولوژی است که اخیراً در معماری سرویس‌گرا^{۱۰} مورد استفاده قرار گرفته است. یک وب سرویس به معنای ساده نوعی مولفه تحت وب است. این مولفه به برنامه‌های کاربردی که از آن استفاده می‌کنند این امکان را می‌دهد که بتوانند از متدهای این وب سرویس استفاده کنند. در سیستم ابر تبادل سرویس بین مرورگر وب کاربر و وب سرویس صورت می‌گیرد به طوری که درخواست‌های کاربر از طریق مرورگر خود به وب سرویس منتقل می‌شود. با این وجود سیستم امنیتی وب سرویس باید به اندازه کافی برای بهینه‌سازی امنیتی در برابر حملات دشمن مقاوم باشد. حملات امنیتی می‌تواند پیام‌های SOAP را مورد حمله قرار دهد.

SOAP (Simple Object Access Protocol) پیام‌های متنی مبتنی بر Xml است که برای تبادل اطلاعات کد گذاری شده بین وب سرویس و کاربر با استفاده از پروتکل‌های مختلف از جمله HTTP, SMTP و MIME به کار می‌رود. SOAP اجازه می‌دهد که یک برنامه در حال اجرا در یک سیستم با یک برنامه در حال اجرا در یک سیستم دیگر بدون در نظر گرفتن مدل برنامه‌نویسی آن‌ها تماس برقرار کند.

پیام SOAP به دو واحد سرپیام و بدنه همانند شکل زیر تقسیم‌بندی می‌شود که در آن سر پیام بسته SOAP از دو قسمت رمز امنیت دودویی و برچسب زمانی تشکیل شده است. که در آن قسمت رمز امنیت دودویی شامل مجوز برقراری ارتباط با وب سرویس و برچسب زمانی حاوی تاریخ ساخت و انقضای پیام SOAP می‌باشد.



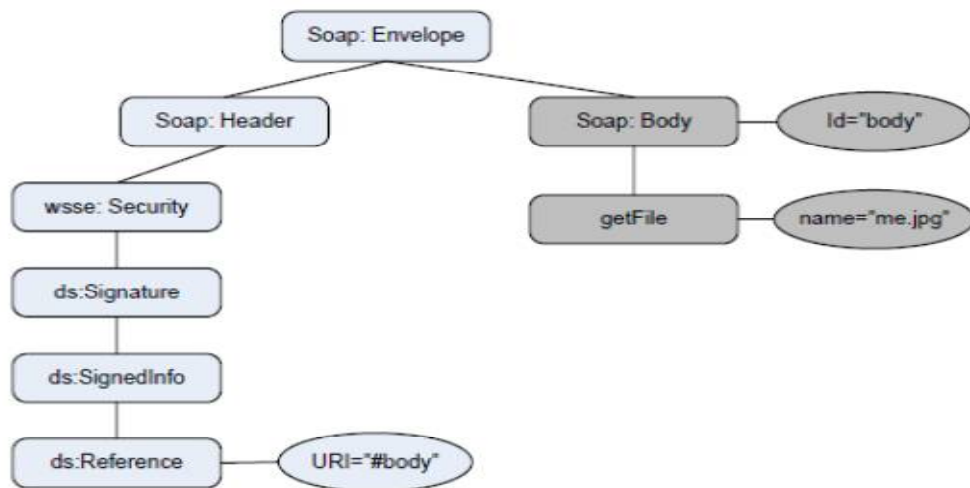
شکل ۱-۱- بسته SOAP [2]

در شروع ارتباط با وب سرویس کاربر می‌بایست جهت ارسال درخواست و دریافت پاسخ خود از وب سرویس مجوزی را دریافت نماید. پس از دریافت مجوز کاربر قادر به ادامه ارتباط با وب سرویس و دریافت پیام SOAP می‌باشد. همانگونه که قبلاً ذکر شد بسته SOAP می‌تواند مورد حمله Wrapping قرار بگیرد. حمله مذکور با حفظ شناسه بسته و تغییر در قسمت بدنه آن می‌تواند محتویات بسته در حال انتقال را دستخوش تغییر گرداند و با ایجاد یک بدنه ساختگی برای پیام به فعالیت بپردازد.

در ادامه حملات امنیتی ممکن به ابر از جمله حمله به بسته SOAP، تزریق کدهای مخرب، حملات سیل‌آسا، سرقت اطلاعات و پس از آن راه‌حل مقابله با هر کدام مورد بررسی قرار خواهد گرفت. لازم به ذکر است از میان چهار حمله فوق تنها دو حمله سیل‌آسا و سرقت اطلاعات در محیط‌های رایانش خوشه‌ای و توری نیز رخ می‌دهند.

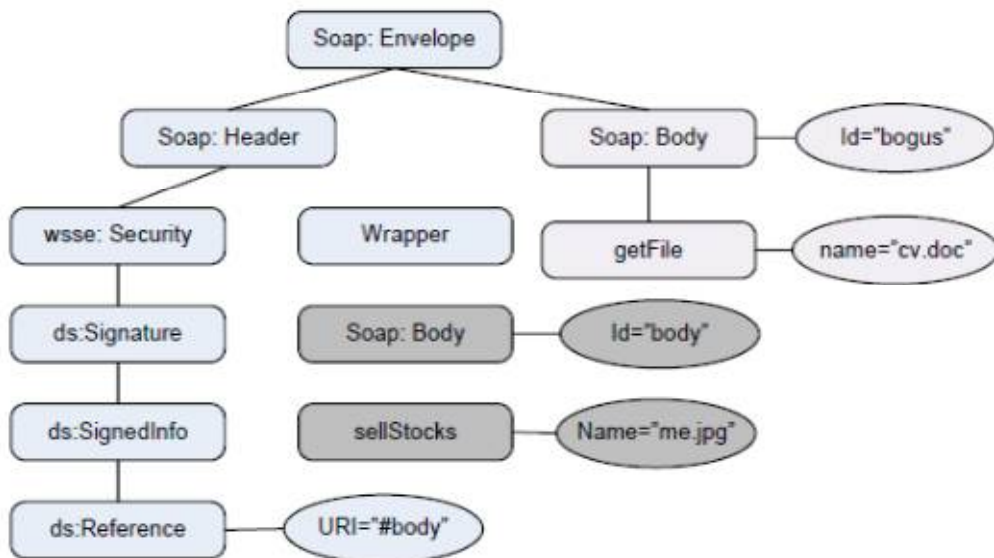
۱-۵-۱- حمله به بسته SOAP (Wrapping Attack) - لایه پلتفرم به عنوان سرویس

هنگامی که کاربر درخواست خود را از طریق مرورگر خود به سمت وب سرور می‌فرستد، در سمت سرور پیام SOAP که شامل اطلاعات ساختاری تبادل اطلاعات بین سرور و مرورگر می‌باشد، ساخته می‌شود. همانطور که گفته شد پیام SOAP دارای دو قسمت سر پیام حاوی امضا و بدنه جهت نگهداری اطلاعات می‌باشد. شکل ذیل یک پیام SOAP ایده‌آل قبل از حمله بسته را نشان می‌دهد که در آن کاربر فایل Me.jpg را از سرور درخواست نموده است.



شکل ۱-۲ پیام SOAP قبل از حمله [3]

مهاجم در پی حمله خود به پیام SOAP، با نگهداری سر پیام یک بسته قسمت بدنه آن را تغییر داده و بدنه ساختگی خود را در بسته جایگذاری می‌کند. در شکل ذیل پیام SOAP پس از حمله نشان داده شده است همانگونه که مشاهده می‌شود مهاجم با تغییر قسمت بدنه پیام و ارسال درخواست به سمت سرور اقدام به حمله نموده است. چنانچه تغییر در بدنه به صورتی باشد که منجر به تغییر تمام ساختار بدنه شود وب سرور این حمله را تشخیص داده و از قبول بسته خودداری خواهد کرد.



شکل ۱-۳ پیام SOAP بعد از حمله [3]

۱-۵-۲- حمله از طریق کدهای مخرب (Malware-Injection) - لایه نرم افزار کاربردی

نوع دیگری از حمله که حقه بازی ابر داده (Meta-Data Spoofing) نیز نامیده می شود در ادامه بررسی می شود. در سیستم های ابری درخواست های کاربر بر اساس تشخیص هویت شناسایی و اجرا می شوند. چنانچه محتوای درخواست های سمت سرور زیاد باشد سرور باید درخواست ها را زمان بندی کند. در برقراری ارتباط آوایه یک سری ابر داده بین کاربر و سرور جابجا می شود در این مرحله است که مهاجم از فرصت استفاده کرده و با رسوخ در سرویس در حال اجرا، سرویس ساختگی خود را به صورت یک سرویس در حال اجرای معتبر در آورده و با ایجاد کدها یا سرویس های مخرب به استراق سمع اقدام می نماید.

چنانچه مهاجم موفق به حمله به کاربری که درخواست خود را به سمت سرور فرستاده شود، باید برای زمان بندی درخواستی که خود منجر به تولید آن نشده است منتظر بماند.

۱-۵-۳- حمله سیل آسا (Flooding Attack) - لایه پلتفرم به عنوان سرویس

یکی از اقداماتی که مهاجم برای دسترسی به سرور انجام می دهد محرومیت کاربران مجاز از سرویس های درخواستی می باشد. حملات سیل آسا نه تنها در محیط ابری بلکه در رایانش های خوشه ای و توری نیز رخ می دهد. در سیستم های ابری سرور هایی که از طریق ارتباطات داخلی با هم در ارتباطند به انجام کار خاصی می پردازند و هنگامی که درخواست های سمت یک سرور زیاد می شود و سرور پربار می شود قسمتی از کارهای خود را به سرور خاص شبیه به خود از لحاظ کاری می دهد و اینگونه لود جانبی صورت می گیرد. هنگامی که مهاجم با مجوز و داده های ساختگی درخواست های خود را به سمت سرور گسیل می کند، مهاجم درخواست ساختگی خود را به سمت سرور می فرستد در سمت سرور درخواست های ارسالی کنترل شده، مجوز آن ها بررسی می شود و مشخص می گردد که درخواست فعلی نامعتبر بوده است. در طی این فرآیند کنترل کردن درخواست های فوق به مصرف پردازشگر و حافظه زیادی نیاز دارد که این امر باعث بالا رفتن بار روی سرور شده و سرور مجبور به بارگذاری جانبی به سرور دیگر می شود. در نتیجه مهاجم با ایجاد اختلال در فرآیندهای معمول و عادی سرور موفق به انجام حمله خود شده است.

۱-۵-۴- سرقت اطلاعات (Data Stealing) - لایه پلتفرم به عنوان سرویس

یکی از راه های سنتی و معمول حمله به ابر سرقت اطلاعات از طریق به دست آوردن حساب کاربری و رمز عبور می باشد. در طی این نوع حمله که در محیط های خوشه ای، توری و ابری رخ می دهد، مهاجم به سرقت اطلاعات محرمانه یا تخریب داده های کاربر اقدام می کند که این امر موجب برهم زدن یکپارچگی داده ها و امنیت موجود در ابر می شود.

۱-۶- جنبه جدید بودن و نوآوری در تحقیق

با بررسی این نکته‌ها به خوبی متوجه می‌شویم که رایانش ابری در آینده پیشرفت عظیمی خواهد داشت و رفته رفته جایگاه واقعی خود را در جهان پیدا خواهد کرد. در زمینه معماری و مدل‌های توسعه آن و... پژوهش‌های زیادی در سال‌های اخیر انجام شده است. طبیعتاً با پیشرفت در زمینه‌های متفاوت رایانش ابری مسئله امنیت اهمیت بیشتری پیدا خواهد کرد. در دو سال گذشته پژوهش‌هایی انجام گرفته است که مقالات معتبر مربوطه در قسمت مراجع آورده شده است. تهدیدهای امنیتی بر روی کاربران ابر به دو دسته داخلی و خارجی تقسیم‌بندی می‌شود. تهدیدهای خارجی شامل تهدید مراکز داده بزرگ می‌باشد که این نگرانی امنیتی در میان کاربران ابر و فراهم‌آوردندگان (که به عنوان شخص ثالث در نظر گرفته شده‌اند) در حصول اطمینان از نرم‌افزارهای امن وجود امکان‌پذیر است.

مجازی‌سازی یکی از مکانیزم‌های اصلی است که در مقابل تلاش‌های کاربران برای حمله به یکدیگر و متعاقباً حمله به زیرساخت رایانش ابری، دفاع قدرتمندی را از خود نشان می‌دهد. البته در پی گفته قبلی باید به این نکته توجه داشت که منابع مجازی و محیط‌های مجازی‌سازی عاری از ایراد نیستند و نرم‌افزارهای کاربردی مجازی‌سازی شامل اشکالاتی در زمینه کدها می‌باشند. مجازی‌سازی شبکه‌هایی که نادرست طراحی شده‌اند اجازه دسترسی یک کاربر به زیرساخت ارائه‌کننده و منابع دیگر کاربران را می‌دهند. همچنین ابر باید از ارائه‌دهندگان که پایین‌ترین لایه زیرساخت به عنوان سرویس را در دست دارند هم محافظت شود زیرا این مهم می‌تواند در از دست دادن داده‌های ناخواسته سهیم باشد.

نحوه پرداخت در سیستم ابری براساس میزان استفاده کاربر می‌باشد. هنگامی که کاربر سرویس مورد تقاضای خود را درخواست می‌کند در طی اجرا مواردی از قبیل مدت زمان سرویس‌گیری، میزان داده منتقل شده در شبکه و چرخه‌های کاری پردازشگر در ثانیه همگی ثبت خواهد شد و پس از اتمام اعتبار، کاربر می‌بایست به شارژ مجدد اقدام نماید. در این صورت هنگامی که مهاجم به حمله خود از طریق کدها یا سرویس مخرب اقدام نماید به صورت فزاینده‌ای از اعتبار کاربر کم کرده و در نتیجه این امر، در خوش نامی و سرویس دهی فراهم آورنده اختلال ایجاد می‌کند.

مفهوم و چارچوبی که در این تحقیق مورد بحث قرار خواهد گرفت به ایجاد یک ساختار امنیتی قوی در شاخه رایانش ابری کمک خواهد کرد. این امنیت ساختاربندی شده با دسترسی از طریق VPN تا حد بالایی قادر به بهبود رضایت مشتریان و جذب سرمایه‌گذاران بیشتری در زمینه این مفهوم از رایانش خواهد بود.

در این تحقیق حملاتی که می‌تواند از طریق مهاجم رخ دهد به همراه راه‌حل‌های آنها مطرح خواهد شد. ایجاد یک ساختار امنیتی قوی می‌تواند در بالابردن ضریب امنیت و همچنین کاهش خطر حملات احتمالی موثر واقع شود. چارچوب ذکر شده محیطی امن را جهت دسترسی کاربران مجاز به سرویس‌های مورد نیاز از طریق شبکه خصوصی مجازی (VPN) فراهم می‌آورد. و با توجه به تحقیقات بنده مقایسه راهکارهای امنیتی در ابر بوسیله شبیه‌سازی آنها و ارزیابی و مقایسه نتایج نهایی تاکنون صورت پذیرفته است و نتایج این تحقیق باعث تمرکز بیشتر بر روی روش امنیتی بهتر خواهد شد.

در مجموع هدف از این مقاله شناخت علت‌های اصلی حملات توسط مهاجمان و مقایسه راه‌حل‌های موجود برای حل مشکلات آنها می‌باشد. همچنین رایانش ابری اصطلاحی است که برای ارائه خدمات میزبانی تحت اینترنت به کار رفته و به عنوان نسل بعدی معماری فناوری اطلاعات پیش‌بینی شده که پتانسیل بسیار خوبی را برای بهبود بهره‌وری و کاهش هزینه‌ها ارائه می‌دهد. در مقایسه با راه‌حل‌های سنتی که در آن سرویس‌های فناوری اطلاعات بر پایه کنترل‌های فیزیکی و منطقی بودند، رایانش ابری نرم‌افزارهای کاربردی و پایگاه داده‌ها را به سمت مراکز داده‌های بزرگ سوق داده است. با این حال ویژگی‌های منحصر به فرد رایانش ابری همواره با شمار بسیاری از چالش‌های امنیتی جدید و شناخته نشده همراه بوده است. در این تحقیق به بررسی حملات به ابر از جمله: حملات بسته SOAP، تزریق نرم‌افزارهای مخرب، حملات سیل آسا، سرقت اطلاعات و راه‌حل‌های مورد نیاز با توجه به این حملات مورد ارزیابی قرار خواهد گرفت. هدف از این تحقیق شناخت علت‌های اصلی حملات توسط مهاجمان و ارائه راه‌حل‌های نظری برای مشکلات آنها و مقایسه راه‌حل‌های ممکن می‌باشد.

فصل دوم

سابقه پژوهش

۲-۱- شرح تحقیق

در ابتدای امر باید تعریف کلی از ابر رایانشی داشته و سپس سیستم‌های تشخیص نفوذ را توضیح داده و در نهایت به امر ایجاد امنیت در آن پرداخته و با توجه به اینکه تمرکز ما بر روی حمله‌هایی ست که منجر به اختلال در محاسبات ابری می‌شود و ایجاد امنیت در آن هدف نهایی تحقیق ما خواهد بود. ما بر اساس تحقیقات سعی خواهیم کرد تا شمای کلی از رایانش ابری و معماری آن ارائه دهیم و سپس سعی خواهیم کرد تا به صورت تخصصی وارد بحث امنیت رایانش ابری شویم و چالش‌هایی که در این زمینه وجود دارد را مورد بررسی و مقالات جدیدی که در این زمینه بررسی شده را مورد تحلیل قرار خواهیم داد و در انتها سعی خواهیم کرد تا با مقایسه مفاهیم بیان شده در مقالات نتیجه‌گیری خود را در این زمینه بیان کنیم.

۲-۲- سابقه پژوهش

۲-۲-۱- سابقه پژوهش ابر رایانشی

رایانش ابری مدتهاست که در محدوده فناوری اطلاعات خودنمایی می‌کند اما در سال‌های اخیر قصد دارد در حیطه تجاری حضور موفق‌تری داشته باشد. در این قسمت نقاط قوتی که طرفداران رایانش ابری به آن‌ها تکیه می‌کنند و نقاط ضعفی که منتقدان آن به آن اشاره می‌کنند را به صورت اجمالی مورد بررسی قرار می‌دهیم.

۲-۲-۱-۱- مزایا و نقاط قوت Cloud Computing [44]

۲-۲-۱-۱-۱- هزینه‌های کم‌تر

به دلیل اینکه زیرساخت‌های گران قیمت به وسیله شرکت‌های ارائه دهنده فراهم می‌گردند ما نیازی به خرید تجهیزات گران قیمت نداریم و برای اجرای برنامه کاربردی، رایانه خانگی ما می‌تواند ارزان‌تر، با یک دیسک سخت کوچک‌تر، با حافظه

کمتر و دارای پردازنده کارآمدتر باشد. در واقع، pc ما در این سناریو حتی نیازی به یک درایو CD یا DVD هم ندارد زیرا هیچ نوع برنامه نرم‌افزاری بار نمی‌شود و هیچ سندی نیاز به ذخیره شدن بر روی کامپیوتر ندارد. در مورد هزینه‌های نرم‌افزاری می‌توان Google Docs را مثال زد که کاملاً رایگان است و می‌تواند جایگزین مناسبی برای آفیس باشد.

۲-۲-۱-۱-۲-۲-سرعت بیشتر

مشابه مورد اول باید توجه داشت با توجه به اینکه سخت‌افزارهای گران قیمت با قدرت محاسباتی بالا توسط شرکت‌های ارائه دهنده خدمات به ما عرضه می‌گردد سرعت در مقایسه با خرید سخت‌افزارهای شخصی با قدرت پایین‌تر بهتر خواهد بود.

۲-۲-۱-۱-۲-۲-مقیاس پذیری

در رایانش ابری، مقیاس‌پذیری در ابعاد گوناگون تعریف شده است و با رشد کاربران و یا نیازهای دیگر سیستم به خوبی می‌توان با اضافه کردن منابع محاسباتی و موارد دیگر مشکل را مرتفع کرد.

۲-۲-۱-۱-۲-۲-به روزرسانی نرم‌افزاری سریع و دائم

با توجه به اینکه ارائه‌دهندگان نرم‌افزارهای اصلی را خریداری و نصب می‌کنند به روزرسانی به صورت مداوم و خودکار صورت می‌پذیرد و با اضافه شدن مشخصات جدید به نرم‌افزارها، پچ‌های جدید به سیستم اضافه می‌گردند. این خصوصیت به خصوص در ایران که قانون کپی رایت در آن به خوبی رعایت نمی‌شود و مهاجمان بهتر قادرند از باگ‌های نرم‌افزارهای غیر اصلی استفاده کنند، می‌تواند ویژگی منحصر به فرد باشد.

۲-۲-۱-۱-۲-۲-ذخیره سازی اطلاعات

برخلاف سیستم‌های خانگی که در صورت خرابی هارد می‌تواند مشکلات بزرگی به وجود آورد، با توجه به اینکه اطلاعات روی سیستم‌های متعددی ذخیره می‌گردد و عملیات پشتیبان‌گیری به صورت مداوم صورت می‌پذیرد امنیت در محافظت از داده‌ها به خوبی در رایانش ابری رعایت می‌شود.

۲-۲-۱-۱-۲-۲-دسترسی جهانی به اسناد

در رایانش ابری، شما در هر کجا که باشید به سرعت می‌توانید به اسناد خود دسترسی پیدا کنید و به همین دلیل، نیازی به همراه داشتن آن‌ها نخواهید داشت.

۲-۱-۱-۲-۲-۷-مستقل از سخت افزار

در نهایت، در این جا به آخرین و بهترین مزیت رایانش ابری اشاره می‌کنیم. ما در رایانش ابری دیگر مجبور نیستیم به یک شبکه یا یک کامپیوتر خاص محدود باشیم. کافی است کامپیوتر خود را تغییر دهیم تا ببینیم برنامه‌های کاربردی و اسناد ما کماکان و به همان شکل قبلی، بر روی ابر در اختیارمان هستند. حتی اگر از ابزار پرتابل نیز استفاده کنیم، باز هم اسناد به همان شکل در اختیارمان هستند. دیگر نیازی به خرید یک نسخه خاص از یک برنامه برای یک وسیله خاص، یا ذخیره کردن اسناد با یک فرمت مبتنی بر یک ابزار ویژه نداریم. فرقی نمی‌کند که از چه نوع سخت‌افزاری استفاده می‌کنیم زیرا اسناد و برنامه‌های کاربردی مورد استفاده ما در همه حال به یک شکل هستند.

۲-۱-۲-۲-۲-نقاط ضعف رایانش ابری

چند دلیل وجود دارد که منتقدان رایانش ابری به آن‌ها اشاره می‌کنند و استفاده از آن را مورد قبول نمی‌دانند:

۲-۱-۲-۲-۱-نیاز به اتصال دائمی اینترنت

در صورتیکه نتوانیم به اینترنت متصل شویم، رایانش ابری غیرممکن خواهد بود. از آن جایی که باید برای ارتباط با برنامه‌های کاربردی و اسناد خود به اینترنت متصل باشیم، اگر یک ارتباط اینترنتی نداشته باشیم نمی‌توانیم به هیچ چیزی، حتی اسنادمان دسترسی پیدا کنیم.

۲-۱-۲-۲-۲-با اتصال‌های اینترنتی کم سرعت کار نمی‌کند

به همان شکلی که در بالا اشاره شد، یک ارتباط اینترنتی کم سرعت نظیر نمونه‌ای که در سرویس‌های Dial-up دیده می‌شود، در بهترین حالت، استفاده از رایانش ابری را با دردسرهای فوق‌العاده‌ای همراه می‌کند و اغلب اوقات، استفاده از آن را غیرممکن می‌سازد. برنامه‌های کاربردی تحت وب و همچنین اسنادی که بر روی ابر ذخیره شده‌اند برای دانلود شدن به پهنای باند بسیار زیادی نیاز دارند. اگر از یک اینترنت Dial-up استفاده کنیم، اعمال تغییر در یک سند یا رفتن از یک صفحه به صفحه دیگر همان سند ممکن است برای همیشه به طول بینجامد.

۲-۱-۲-۲-۳-محدودیت ویژگی‌ها

ویژگی‌های آن ممکن است محدود باشند. این وضعیت در حال تغییر است اما بسیاری از برنامه‌های کاربردی مبتنی بر وب به اندازه همتای دسک تاپ خود دارای ویژگی‌ها و امکانات غنی نیستند. به عنوان مثال، می‌توانیم کارهای بسیار زیاد با برنامه PowerPoint انجام دهیم که امکان انجام همه آن‌ها توسط برنامه ارائه GoogleDocs وجود ندارد. اصول این برنامه‌ها یکسان هستند، اما برنامه کاربردی که بر روی ابر قرار دارد فاقد بسیاری از امکانات پیشرفته PowerPoint است.

۲-۲-۱-۲-۴-عدم امنیت داده‌ها

داده‌های ذخیره شده ممکن است از امنیت کافی برخوردار نباشند. با استفاده از رایانش ابری، تمام داده‌های ما بر روی ابر ذخیره می‌شوند. از نظر تئوری، داده‌های ذخیره شده بر روی ابر ایمن هستند و بین چندین ماشین توزیع شده‌اند. اما در صورتی که داده‌های ما مفقود شوند، هیچ نسخه پشتیبان فیزیکی یا محلی در اختیار نخواهیم داشت (مگر این تمام اسناد ذخیره شده بر روی ابر را بر روی دسکتاپ خود دانلود کنیم که معمولاً کاربران کمی چنین کاری می‌کنند).

۲-۲-۱-۳-انواع ابر [45]

۴ نوع مختلف از ابر وجود دارد که بر اساس نیازمان می‌توانیم انتخاب کنیم:

۲-۲-۱-۳-۱-ابر عمومی^{۱۱}: که سرویس‌ها در آن به صورت پویا و از طریق یک ارتباط اینترنتی ارائه داده می‌شوند و ارائه دهنده سرویس منابع را به صورت اشتراکی به کاربران عرضه می‌کند.

۲-۲-۱-۳-۲-ابر خصوصی^{۱۲}: که برای شرکت‌ها و سازمان‌های خاصی ارائه خدمت می‌دهد و دسترسی به آن محدود به همان سازمان‌های می‌شود.

۲-۲-۱-۳-۳-ابر گروهی^{۱۳}: که برای دو یا چند سازمان که نیازهای مشابهی دارند ارائه خدمت می‌دهد.

۲-۲-۱-۳-۴-ابر آمیخته^{۱۴}: لزوماً ترکیبی از حداقل دو سرویس ابری است و شامل ترکیب انواع عمومی، خصوصی و یا گروهی است.

حال بعد از معرفی این چهار دسته کلی به معرفی چند معماری که از این چهار دسته معماری مشتق شده‌اند می‌پردازیم. بیشتر این معماری‌ها می‌توانند با استفاده از الگوهای سرور موجود که در دسترس هستند ایجاد شوند. هر برنامه کاربردی منحصر به فرد است و یک مجموعه سفارشی از الزامات خودش را دارد. هدف از معماری‌هایی که در زیر نشان داده می‌شود ارائه نمونه‌های جهان واقعی است که می‌توانیم به عنوان مرجعی پایه برای معماری سیستم ابری خود استفاده کنیم. زمانیکه در میان معماری‌های زیر یک معماری سیستم شبیه به آنچه که در حال تلاش برای طراحی آن هستیم پیدا کردیم، می‌توانیم آن را مطابق با نیازهای پروژه خود تغییر دهیم.

11 Public cloud

12 Private cloud

13 Community cloud

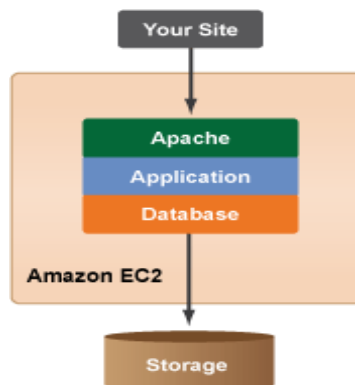
14 Hybrid cloud

نمودارهایی که در کنار مفاهیم معماری‌ها وجود دارد برای نشان دادن یک مفهوم خاص از قبیل بازیابی فاجعه (disaster recovery) یا استقرار چند ابری طراحی شده‌اند. هنگامی که در حال طراحی معماری خود هستیم باید مفاهیمی مانند هزینه، پیچیدگی طراحی، سرعت، امنیت و... را در نظر بگیریم. حال به معرفی نمودارها و معماری‌ها به ترتیب صعودی پیچیدگی می‌پردازیم.

۲-۱-۲-۲- معرفی نمودارها و معماری‌های ابر [35]

۲-۱-۲-۲- Single "All-in-one" Server

این الگو در LAMP (لینوکس، آپاچی، MySQL، PHP) که یک سرور واحد شامل یک وب سرور (آپاچی) و برنامه (PHP) و پایگاه داده MySQL است، استفاده شده است.

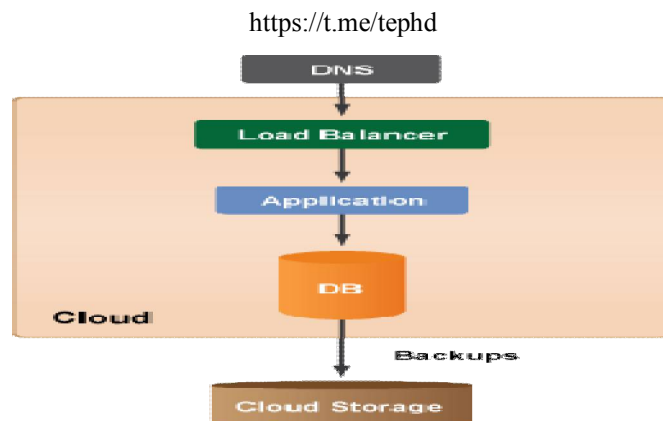


شکل ۲-۱- Single Cloud Site Architectures

این معماری سه لایه استاندارد دارد و حداقل یک سرور اختصاصی در هر ردیف از معماری سیستم وجود دارد (سرور حفظ تعادل بار، سرور برنامه کاربردی، سرور پایگاه داده)

۲-۱-۲-۲- Non-Redundant 3-Tier Architecture

اگر بخواهیم تعامل بین هر ردیف از معماری خود را تست کنیم می‌توانیم برای صرفه‌جویی در هزینه‌ها و منابع از یک معماری سیستم non-redundant استفاده می‌کنیم. درواقع معماری سیستم non-redundant در درجه اول برای تست پایه و اهداف توسعه استفاده می‌شود به عنوان مثال در نمودار زیر، سرورهای اختصاصی برای هر ردیف از نرم افزار / سایت وجود دارد. معماری non-redundant برای محیط‌های تولید توصیه نمی‌شود.

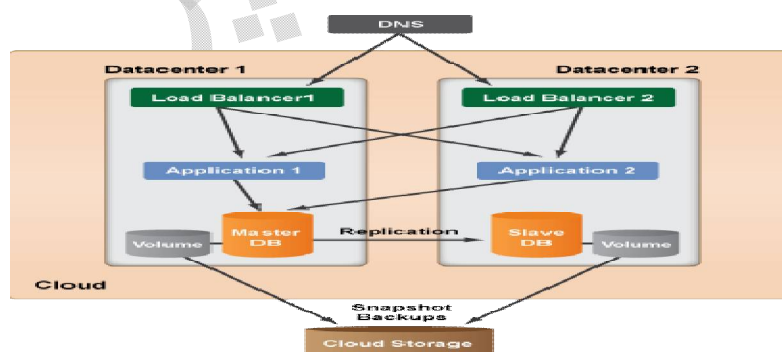


Redundant 3-Tier Architecture-۲-۲ شکل

هر محیط تولیدی که در ابر راه اندازی شود باید یک معماری redundant برای خطاها و اهداف بازیابی داشته باشد. به طور معمول، از یک آرایه سرور برای هر ردیف از برنامه کاربردی به منظور استفاده از مزایای autoscaling در ابر استفاده می شود. با این حال ممکن است بعضی از برنامه های کاربردی با مقیاس پذیری خودکار سازگار نباشند. در چنین مواردی، می توان از یک معماری چند لایه redundant استفاده کرد که در آن باید افزونگی در هر ردیف از معماری مرجع ایجاد شود.

۲-۲-۱-۳-۴-۳ معماری Multi-Datacenter

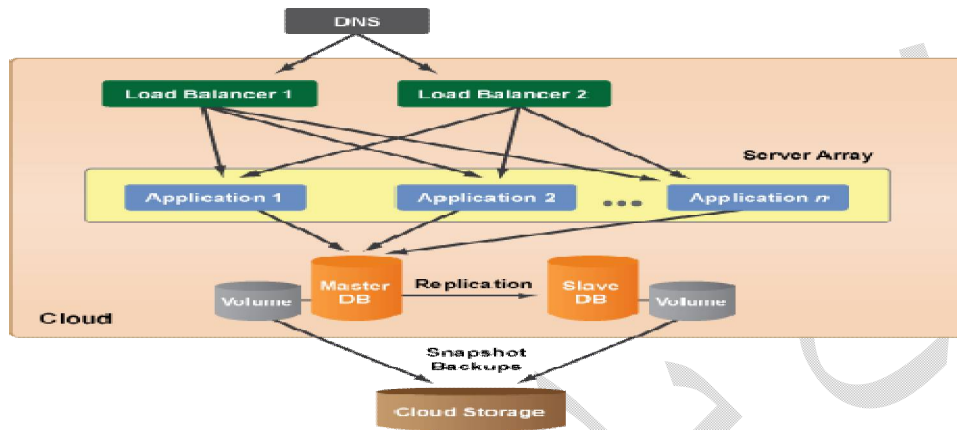
اگر زیرساخت های ابر ما از مراکز داده چندگانه پشتیبانی کند پیشنهاد می شود برای اضافه کردن لایه ای دیگر از افزونگی و حفاظت معماری سیستم خود را در مراکز داده ای متعدد گسترش دهیم. مزیت استفاده از معماری مراکز داده چندگانه حفاظت سایت یا برنامه کاربردی اجرا شده روی ابر در مقابل اثرات منفی رخ داده با انواع خرابی های شبکه، کمبود منابع موجود یا خارج شدن سرویس از دسترس در یک مرکز داده است.



Multi-Datacenter ۳-۲ شکل

۲-۱-۴-۴-معماری Autoscaling

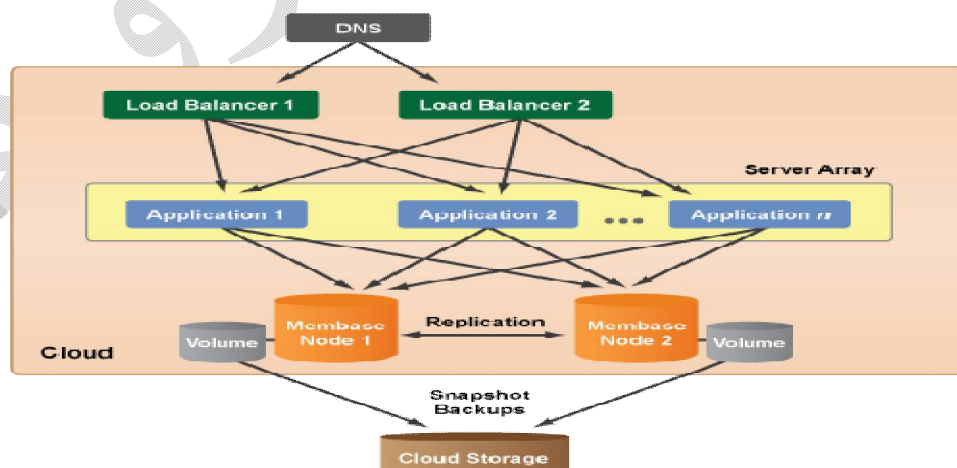
یکی از مزایای کلیدی ابر توانایی مقیاس‌پذیری افقی (رشد منابع در حال اجرای سرور) آن است. با این معماری، می‌توانیم از آرایه سرور برای راه‌اندازی یک لایه خاص از معماری استفاده کنیم. مقیاس‌پذیری خودکار اغلب برای لایه برنامه کاربردی از معماری ابر مرجع مورد استفاده قرار می‌گیرد.



شکل ۲-۴-معماری Autoscaling

۲-۱-۴-۵-معماری مقیاس‌پذیر با Membase

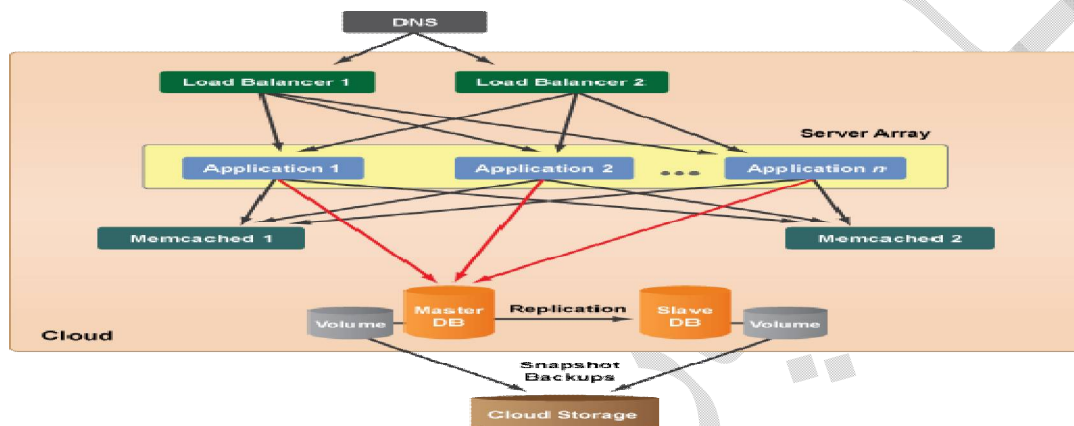
اگر در معماری مقیاس‌پذیر نخواهیم از پایگاه داده MySQL master/slave استفاده کنیم باید از گره‌های mambase که نوعی پایگاه داده توزیع شده NoSQL است برای ردیف پایگاه داده استفاده کنیم. اگر از نسخه سازمانی آن استفاده کنیم می‌توانیم volume‌ها را به هر گره attach کنیم (مشابه شکل)، اما نسخه community استفاده از volume‌ها را پشتیبانی نمی‌کند.



شکل ۲-۵-معماری مقیاس‌پذیر با Membase

۲-۱-۴-۶- معماری چند لایه مقیاس پذیر با Memcached

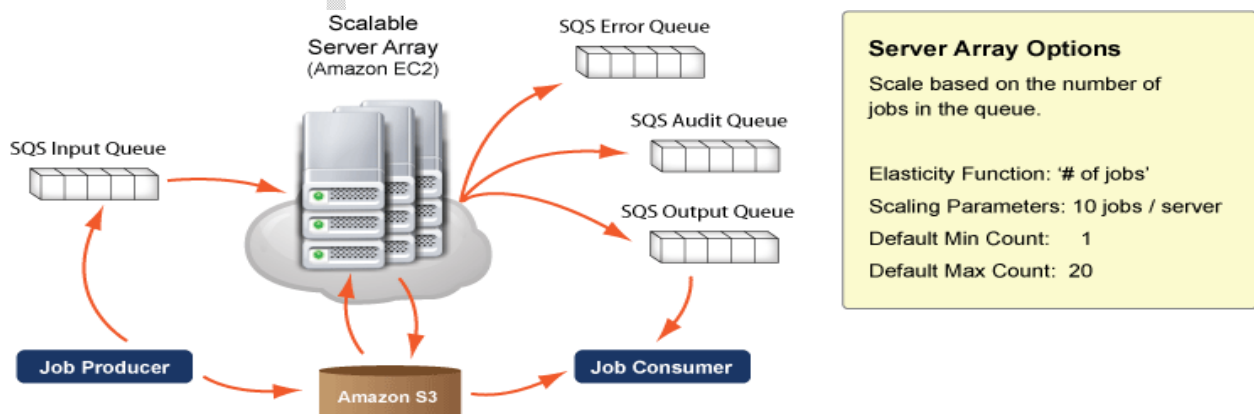
برای برنامه‌های کاربردی / سایت‌هایی که نیاز به خواندن زیاد از پایگاه داده را دارند می‌توانیم یک لایه Memcached به معماری سیستم ابر خود به منظور جلوگیری از بارگذاری اعمال تکراری اضافه کنیم. Memcached یک سیستم کش حافظه منبع باز توزیع شده است که برای بالا بردن سرعت برنامه‌های کاربردی تحت وب با کاهش بار پایگاه داده ایده‌آل است. به عنوان مثال در شکل زیر، سرور برنامه کاربردی می‌تواند عملیات نوشتن را در پایگاه داده انجام دهد، اما بسیاری از object های استفاده شده معمول از سرورهای Memcached به جای استفاده از سرور اصلی DB بازیابی می‌شوند.



شکل ۲-۶- معماری چند لایه مقیاس پذیر با Memcached

۲-۱-۴-۷- معماری مقیاس پذیر مبتنی بر صف Scalable Queue-based Setups

این معماری یک framework برای پردازش دسته‌ای فراهم می‌کند که یک راه حل کارآمد را برای پردازش گروهی Job ها با بهره‌گیری از ظرفیت محاسبه زیرساخت‌های رایانش ابری مانند آمازون EC2 فراهم می‌کند. رایج‌ترین روش اندازه‌گیری یک برنامه کاربردی برای پردازش دسته‌ای شمارش job های در صف است.



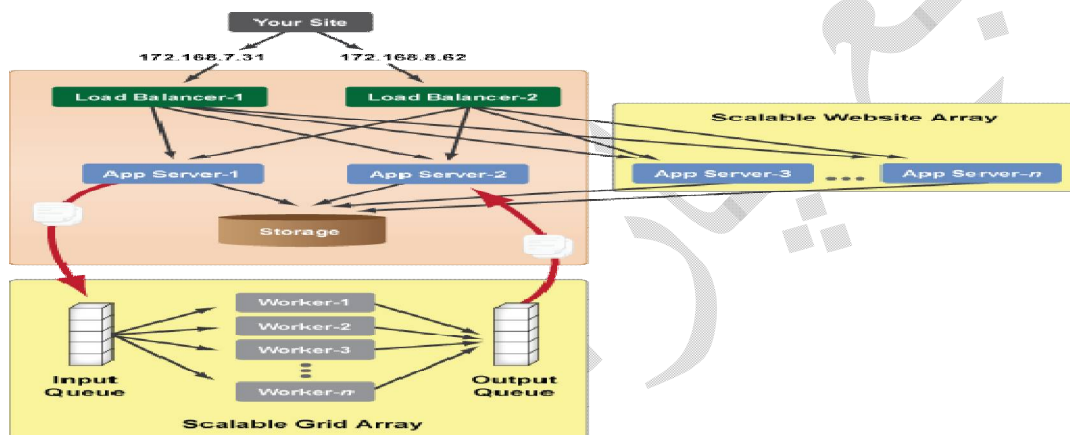
شکل ۲-۷- معماری مقیاس پذیر مبتنی بر صف Scalable Queue-based Setups

۲-۲-۱-۴-۸ معماری Hybrid داخلی

اگر در حال حاضر یک معماری grid داشته باشیم یا بخواهیم از منابع داخلی محاسباتی استفاده کنیم می‌توانیم از مدل hybrid داخلی استفاده کنیم. این مدل با استفاده از منابع داخلی، قابلیت انعطاف پذیری استفاده از منابع محاسباتی ابر را به ما می‌دهد.

۲-۲-۱-۴-۹ معماری مقیاس پذیر مبتنی بر هشدار و مبتنی بر صف

از آنجا که می‌توان آرایه سرورهای چندگانه را برای توسعه معماری مورد استفاده قرار داد، می‌توانیم یک معماری مقیاس پذیر دوگانه را با آرایه front-end و back-end مقیاس پذیر ایجاد کنیم.



شکل ۲-۸-۲ معماری مقیاس پذیر مبتنی بر هشدار Scalable Alarm-based Setups

۲-۲-۱-۴-۹ معماری ابر ترکیبی سایت Hybrid Cloud Site Architectures

راه دیگر که می‌توان برای حفاظت از برنامه‌های کاربردی در ابر استفاده کرد، طراحی معماری ابر ترکیبی سایت است. یکی از مزایای کلیدی این معماری این است که در آن می‌توانیم از منابع مشابه برای راه اندازی سرویس‌دهنده چندگانه ابر عمومی یا خصوصی استفاده کنیم. به طور مشابه می‌توانیم از معماری hybrid استفاده کنیم که در آن سرورها در ابر می‌توانند با سرورهای اختصاصی که در مراکز داخلی داده میزبان قرار دارند ارتباط داشته باشند.

۲-۲-۱-۴-۱۰ معماری مقیاس پذیر چند ابری

می‌توانیم از یک زیرساخت ابر برای طراحی معماری برنامه کاربردی یا سایت استفاده کنیم و از آرایه سرورها برای مقیاس پذیری خودکار (autoscaling) لایه برنامه کاربردی در زیرساخت‌های ابر مختلف استفاده کنیم. برای مثال می‌توانیم از سرورهای ابر خصوصی قبل از قبول هزینه‌های مربوط به زیرساخت ابر عمومی استفاده کنیم. شکل زیر انعطاف پذیری

برنامه کاربردی را در زیرساخت ابر خصوصی نشان می‌دهد. البته باید به این نکته توجه داشت که در صورت لزوم می‌توان مقیاس پذیری خودکار را در زیرساخت‌های ابر عمومی تعریف کرد.

۲-۲-۱-۴-۱۱-معماری چند ابری Failover

یک مزیت این معماری این است که اگر مشکلی پیش بیاید که نیاز به تغییر ابرها داشته باشیم معماری چند ابری به ما اجازه می‌دهد که به راحتی برنامه خود را در میان ابرها منتقل کنیم. توجه داشته باشید که اگر بخواهیم از ابر X به Y مهاجرت کنیم ردیف‌های دیگر معماری، پیکربندی شده‌اند و آماده راه‌اندازی هستند و نیازی به پیکربندی مجدد ندارند. اگر بخواهیم داده‌ها را به شیوه‌ای امن بین سرورها در میان دو ابر منتقل کنیم می‌توانیم از رمزگذاری داده‌ها (encryption) یا VPN در کنار آدرس IP عمومی استفاده کنیم.

۲-۲-۱-۴-۱۲-معماری بازیابی فاجعه چند ابری

واقعیتی که وجود دارد این است که سرورها و سرویس‌های ابری در معرض مشکلاتی قرار دارند که می‌توانند منجر به فاجعه (disaster) شوند. بنابراین مهم است که معماری سیستم طوری طراحی شود که سناریوهای مختلفی برای بازیابی و بهبود خرابی‌ها داشته باشد. برای مثال چه اتفاقی خواهد افتاد اگر مشکلی ناگهانی در ابری که محیط تولید اطلاعات در آن است پیش بیاید؟ در مدل بازیابی سنتی اختصاصی تنها انتخاب ما این است که منتظر بمانیم تا شرکت ارائه دهنده میزبانی مشکل را رفع کند و سرورهای ما به شرایط عادی و محیط عملیاتی برگردند. اما در ابر اگر ما از معماری مناسبی استفاده کنیم خودمان این توانایی را خواهیم داشت که به سرعت و فوراً پاسخ مناسبی به رخداد دهیم و به بازیابی بپردازیم.

۲-۲-۱-۴-۱۲-معماری ابر و میزبانی اختصاصی

شاید یک شرکت به دلیل این که سرور پایگاه داده آن حاوی اطلاعات حساس کاربران و یا داده‌های اختصاصی باشد الزامات سختگیرانه‌ای در اطراف محل فیزیکی سرور پایگاه داده داشته باشد. در چنین مواردی، می‌توان از یک معماری سیستم Hybrid با استفاده از یک شبکه خصوصی مجازی (VPN) برای ایجاد یک تونل ارتباطی امن بین سرورهای ابری و سرورهای اختصاصی استفاده کرد.

نتیجه گیری:

رایانش ابری متناسب با نیاز کاربران و اهداف آنها می‌تواند روش مناسبی برای صرفه جویی و کاهش هزینه‌ها باشد.

۲-۲-۲- سابقه پژوهش بررسی سیستم‌های تشخیص

پژوهش‌های بسیاری در زمینه سیستم‌های تشخیص و پیشگیری از نفوذ در محاسبات ابری انجام شده است که بیشتر بر روی یک ویژگی خاص و یا نوع خاص از حمله یا نفوذ تمرکز می‌کنند در حالی که یکی از راه‌حل‌های موجود، معرفی سیستم‌های همه منظوره‌ای است که جنبه‌های بیشتری از راه‌حل‌ها و اجزای سیستم را در نظر بگیرد. برای مثال Carl و همکاران روش‌های مختلف تشخیص انکار سرویس DOS^{۱۵} را بررسی کرده‌اند و smith و johnson برای بهبود کیفیت حسگرها جهت تشخیص بیشتر نفوذ در محیط پردازش ابری تلاش کرده‌اند. [1]

Kleber و schulter در لایه میان‌افزار یک سرویس IDS ارائه کرده‌اند که حملاتی که HIDS و NIDS قادر به تشخیص آنها نیستند را پوشش می‌دهد. [5]

Roschke و همکاران یک راه‌حل مجتمع برای مدیریت IDS مرکزی ارائه داده‌اند که می‌تواند گزارش‌های خروجی حسگرهای IDS گوناگون را با هم ترکیب کند. حسگرها برای برقراری ارتباط از استاندارد فرمت مبادله پیام^{۱۶} (IDMEF) استفاده می‌کنند. حسگرهای IDS روی لایه‌های مجزای ابر مانند لایه برنامه‌کاربردی، سیستم و پلت‌فرم مستقر می‌شوند. رویداد پیام هشدار را دریافت و طبق استاندارد تبدیل کرده و در پایگاه‌داده ذخیره می‌نماید. [5]

Bakshi راه‌حل دیگری در مورد تشخیص نفوذ در ابر ارائه داده است که بر روی دفاع محیط ابر در برابر حملات DDOS^{۱۷} متمرکز می‌باشد. این مدل از یک سیستم تشخیص نصب شده بر روی روتر مجازی استفاده می‌کند و هنگامی که یک حمله DDOS تشخیص داده می‌شود، اتصالات بعدی از حمله کننده مسدود می‌شود. [29]

Lo و همکارانش چارچوبی ارائه کرده‌اند در آن با اشتراک هشدارهای مربوط به حملات DOS و DDOS میان نواحی مختلف محاسبه ابری، تأثیر این حملات را کاهش می‌یابد. DMEF هشدارهای میان IDSها در قالب اسناد xml مبادله می‌نماید. [28]

Dastjerdi و همکارانش IDS مبتنی بر عامل را به عنوان یک راه‌حل امنیتی برای محیط ابر پیاده‌سازی کرده‌اند. مدل آنها یک عامل موبایل با وظیفه خاصی را به هر میزبان مجازی که هشدارهای مشابه را ایجاد کرده است می‌فرستد. عامل‌های موبایل می‌توانند به شناسایی حملات کمک کنند. [29]

Bosin و همکاران مدلی برای مدیریت امنیت ارائه کرده‌اند که دسترسی به سرویس‌های تشخیص نفوذ را هنگامی که نیاز باشد، فراهم می‌کند. [29]

Gul و همکاران یک سیستم تشخیص نفوذ توزیع شده چندمنحی را ارائه کرده‌اند که در واقع یک نمونه بهبود یافته NIDS می‌باشد. مدل آنها با استفاده از حسگرها ترافیک شبکه را برای شناسایی بسته‌های مشکوک کنترل و نظارت می‌کند. یکی از ویژگی‌های آن پردازش حجم بیشتری از داده‌ها و کاهش سربار شبکه می‌باشد. [5]

15 Denial of service

16 Intrusion detection message exchange format

17 Distributed denial of service

Alhoby مدلی ارائه کرده است که در آن سیستم تشخیص نفوذ به عنوان سرویس بر روی ابر در اختیار کاربران قرار می‌گیرد و کاربران با توجه به نیازمندی‌های امنیتی خود، میزان سطح امنیتی را درخواست می‌کنند. [29]

Turki نیز چهارچوب IDSaaS (سیستم تشخیص نفوذ به عنوان سرویس) را مطرح کرده است که در آن تشخیص نفوذ بعنوان سرویس در اختیار کاربران ابر در V-Lan ها قرار می‌گیرد. یکی از ویژگی‌های چهارچوب ارائه شده این است که کاربر کنترل آن را در اختیار خواهد داشت و می‌تواند قوانین و قواعد امنیتی آن را سفارشی‌سازی نماید. ویژگی دیگر آن نوشتن سناریوهای حمله تطبیق شده با نیازهای امنیتی برنامه‌های کاربردی توسط کاربر می‌باشد. [28]

۲-۲-۱-۲- نتیجه‌گیری از سابقه پژوهش سیستم‌های تشخیص و پیشگیری نفوذ

۲-۲-۱-۲-۲- طبقه‌بندی سیستم‌های تشخیص و پیشگیری نفوذ

تشخیص نفوذ روند نظارت بر کامپیوترهای شبکه برای ورود، فعالیت یا تغییر فایل‌های غیرمجاز می‌باشد. حملات بیشتر در گروه‌های مشخصی به نام حوادث رخ می‌دهد. اگر چه بسیاری حوادث در طبیعت مخرب و بسیاری دیگر غیرمخرب هستند. برای مثال یک شخص ممکن است اشتباهاً آدرس یک کامپیوتر را تایپ کند و تصادفاً تلاش کند بدون اجازه به یک سیستم دیگر متصل شود. [1]

یک IDS نرم‌افزاری است که بطور خودکار روند تشخیص نفوذ و رسوخ ممکن را اجرا می‌کند. یک سیستم تشخیص و پیشگیری از نفوذ وسیله سخت‌افزار یا نرم‌افزاری است که تمام قابلیت‌های سیستم تشخیص نفوذ را دارد و همچنین می‌تواند برای جلوگیری از حوادث احتمالی تلاش کند.

برای استفاده از سیستم‌های به روز و پیشرفته، پیشگیری از نفوذ یک ویژگی جدید برای سیستم‌های تشخیص نفوذ می‌باشد. در تمام کارهای اخیر روی سیستم‌های پیشگیری نفوذ^{۱۸} و یا سیستم‌های تشخیص نفوذ^{۱۹} یک ماژول پیشگیری جهت ارتقاء به آنها اضافه شده است. پیشگیری نفوذ بوسیله یک ویژگی از تشخیص نفوذها متمایزند. یک سیستم پیشگیری نفوذ می‌تواند به یک تهدید شناسایی شده با تلاش برای جلوگیری از رخ دادن آن پاسخ دهد. [1]

معمولاً یک سیستم پیشگیری نفوذ درون شبکه قرار گرفته و بر شبکه نظارت می‌کند و هنگامی یک حادثه رخ می‌دهد براساس قوانین از تعیین شده واکنش نشان می‌دهد. برخلاف آن سیستم تشخیص نفوذ در شبکه مستقر نمی‌شود و انفعالی عمل می‌کند. به این دلیل که سیستم پیشگیری نفوذها گاهی قابلیت‌های تشخیص بیشتری دارند، بعضی آنها را به عنوان نسل بعدی سیستم‌های تشخیص می‌شناسند. سیستم‌های پیشگیری و سیستم‌های تشخیص نفوذ هر دو امنیت نسبتاً متفاوتی به وجود می‌آورند و قابلیت‌های متفاوتی دارند. [13]

سیستم‌های پیشگیری از نفوذ	سیستم‌های تشخیص نفوذ
نصب روی قسمت شبکه و میزبان	نصب شده روی قسمت های شبکه و میزبان
استقرار روی شبکه بطور فعال	استقرار روی شبکه بصورت غیرفعال
عملکرد بهتر در کاربرد های پیشگیری	نمی تواند ترافیک رمزنگاری شده را تشریح کند
کنترل مدیریتی عمومی	کنترل مدیریتی عمومی
ایده ال برای بلوکه کردن خرابی وب	تشخیص بهتر حملات هک
ایجاد بلوکه سازی	ایجاد هشدار (واکنش)

جدول 1-2- چهار عملکرد ضروری امنیتی سیستم های نفوذ [13]

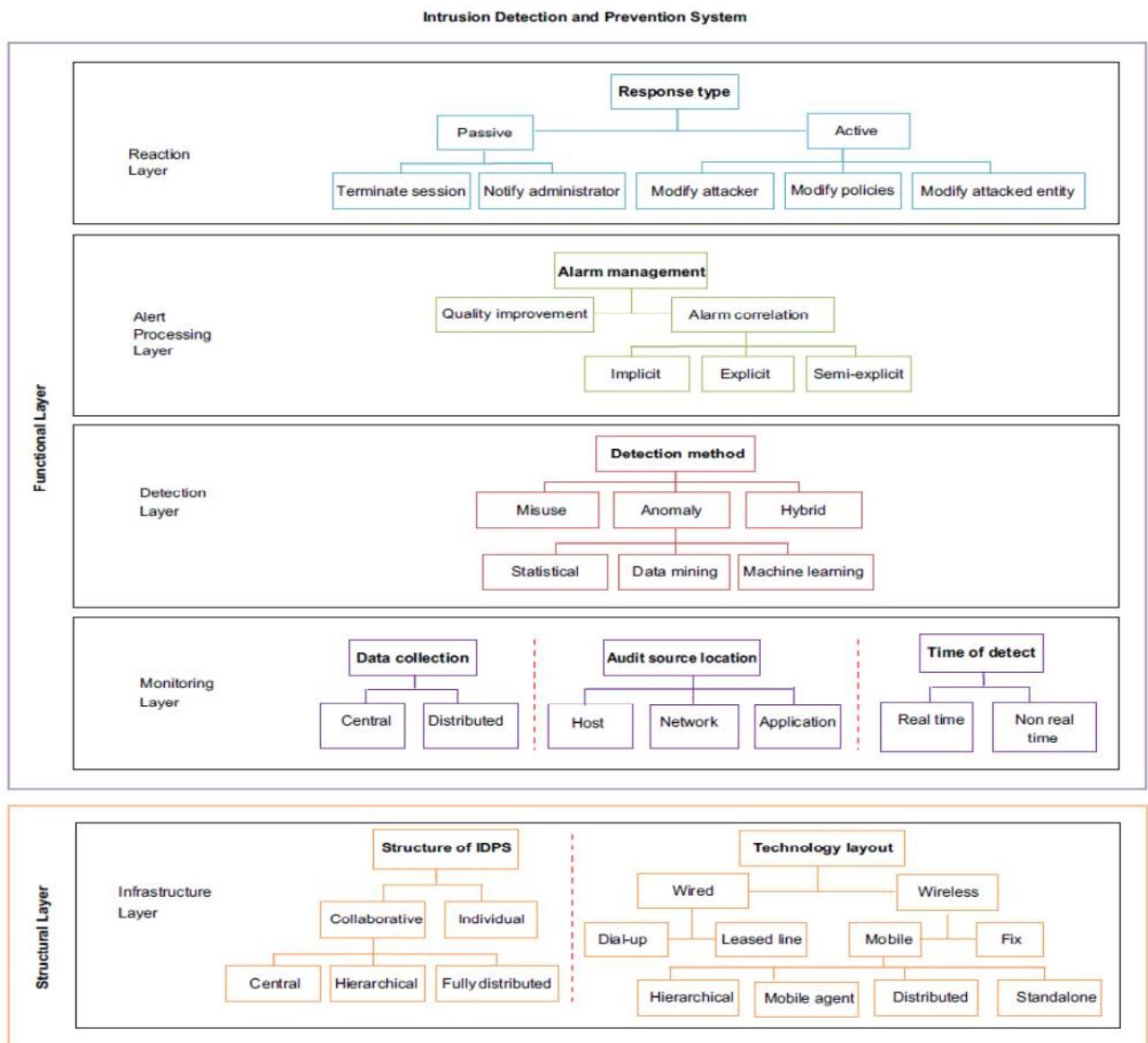
Patel و همکاران یک طبقه‌بندی جامع در مورد سیستم‌های تشخیص نفوذ ارائه داده‌اند که در بخش زیر به آن می‌پردازیم. سیستم‌های تشخیص نفوذ چهار عملکرد ضروری امنیتی را سرویس می‌دهد. آنها فعالیت‌های غیرمجاز را نظارت، شناسایی، آنالیز کرده و نسبت به آنها واکنش نشان می‌دهند که در لایه عملیاتی به تصویر کشیده شده است. سیستم‌های تشخیص نفوذ، حمله را به وسیله آنالیز کردن داده‌های جمع‌آوری شده تشخیص می‌دهند. محیط‌های نظارتی می‌تواند مبتنی بر شبکه، مبتنی بر میزبان یا مبتنی بر برنامه‌های کاربردی باشند:

- ۱- **مبتنی بر شبکه (NIDPS^۹):** بر ترافیک شبکه، بخش‌ها یا ابزار ویژه شبکه نظارت می‌کند و شبکه و فعالیت پروتکل برنامه کاربردی را برای شناسایی فعالیت‌های مشکوک آنالیز می‌کند.
- ۲- **مبتنی بر میزبان (HIDPS^{۱۰}):** بر تمام یا بخشی از رفتار حالت پویای سیستم‌های کامپیوتر نظارت می‌کند. از آنجا که یک سیستم‌های تشخیص نفوذ مبتنی بر شبکه بصورت پویا بسته‌های شبکه را بررسی می‌کند یک سیستم تشخیص نفوذ مبتنی بر میزبان ممکن است تشخیص دهد کدام برنامه به چه منابعی دسترسی دارد. همچنین یک روش مکمل که ترکیبی از هر دو مولفه مبتنی بر شبکه و مبتنی بر میزبان است انعطاف‌پذیری بیشتری فراهم کنند.
- ۳- **مبتنی بر برنامه کاربردی (AIDPS^{۱۱}):** روی وقایعی که در بعضی از برنامه‌های کاربردی خاص رخ می‌دهند، از طریق تجزیه و تحلیل فایل‌های ورودی، برنامه کاربردی یا اندازه‌گیری عملکرد آنها تمرکز می‌کند. غالباً ورودی آنها منابع داده‌ای برنامه‌های کاربردی در حال اجرا است.

^۹ Network-based intrusion detection and prevention systems

^{۱۰} Host-based intrusion detection and prevention systems

^{۱۱} Application-based intrusion detection and prevention systems



شکل ۲-۹- طبقه بندی سیستم های تشخیص و پیشگیری از نفوذ [1]

روش های معرفی شده تشخیص در سه گروه سوءاستفاده، آنومالی و مدل هیبریدی که ترکیبی از دو کلاس اول است طبقه بندی شده اند.

تشخیص سوءاستفاده (تشخیص امضاء): این روش بطور خاص از الگوهای شناخته شده، رفتارهای غیرمجاز و امضاهای معرفی شده برای پیش بینی و تشخیص تلاش های مشابه برای دسترسی استفاده می کند. تشخیص امضاء شامل تطبیق رفتار نفوذی کاربران با کدهای مخرب می باشد.

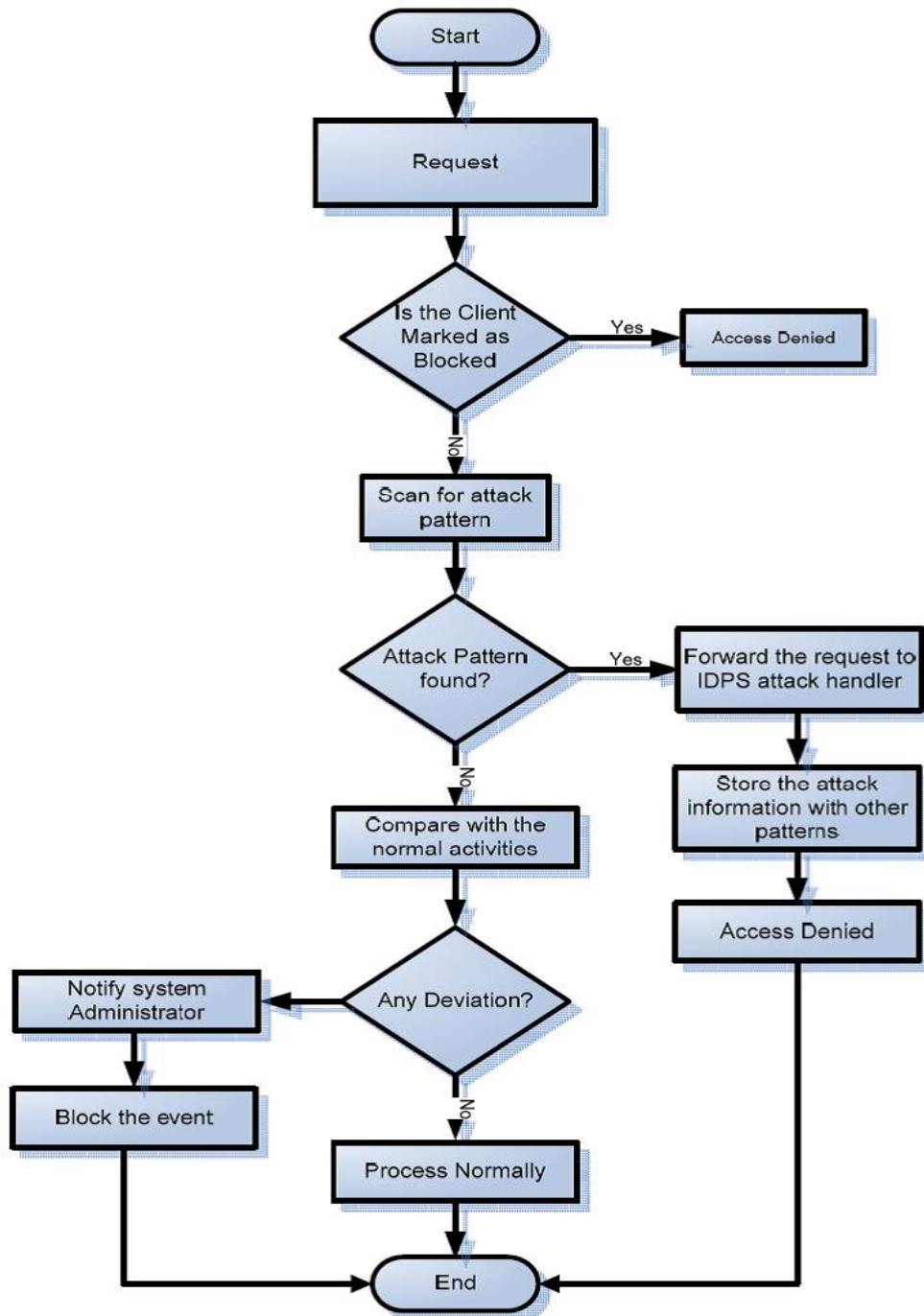
موتورهای بستر امضاء دیجیتال نیز معایب خود را دارند. در حالی که اعمال روش امضاء به خوبی در برابر حمله با یک الگوی رفتاری ثابت کار می‌کند، ولی ممکن است علیه بسیاری از الگوهای حمله ایجاد شده توسط یک انسان یا یک کرم با ویژگی‌های رفتاری پویا به خوبی کار نکنند. از آنجا که آنها فقط حملات از قبل شناخته شده را شناسایی می‌کنند، باید برای هر حمله یک امضاء ساخته شود که در این صورت حملات نوظهور نمی‌تواند شناسایی شود.

تشخیص ناهنجاری: تشخیص ناهنجاری بوسیله ایجاد رفتار نرمال سیستم اعمال می‌شود. رفتار نرمال یک سیستم با مشاهده عمل استاندارد سیستم یا شبکه تعیین می‌شود. سپس سیستم تشخیص ناهنجاری یک مدل معمولی را می‌گیرد و با استفاده از روش‌های واریانس آماری یا داده کاوی با هوش مصنوعی تعیین می‌کند که آیا رفتار شبکه یا سیستم موردنظر به طور طبیعی در حال اجرا است یا غیرطبیعی. فرض در تشخیص آنومالی این است که نفوذ می‌تواند بوسیله مشاهده یک انحراف از رفتاری عادی و مورد انتظار سیستم یا شبکه، شناسایی شود.

اشکال تشخیص ناهنجاری این است که فعالیت‌های مخرب ممکن است در الگوهای مورد استفاده عادی تشخیص داده نشوند. [13][1]

هیبرید: این روش به منظور ارتقاء قابلیت‌های سیستم‌های تشخیص نفوذ جاری بوسیله ترکیب دو روش سوءاستفاده و ناهنجاری مطرح شده است. ایده اصلی این است که تشخیص سوءاستفاده حملات را می‌شناسد در حالی که آنومالی حملات را نمی‌شناسد. از جمله عملیات سیستم‌های تشخیص نفوذ می‌توان به نظارت و آنالیز فعالیت‌های کاربر و سیستم، آنالیز پیکربندی سیستم و آسیب‌پذیری، ارزیابی سیستم و جامعیت فایل، تشخیص انواع الگوهای حملات، آنالیز الگوهای فعالیت غیر معمول و ردیابی تخلفات کاربر اشاره کرد. [22]

شکل زیر چهارچوب عملکردی سیستم‌های تشخیص نفوذ را نشان می‌دهد:



شکل ۲-۱۰-چهارچوب عملکردی IDPS [22]

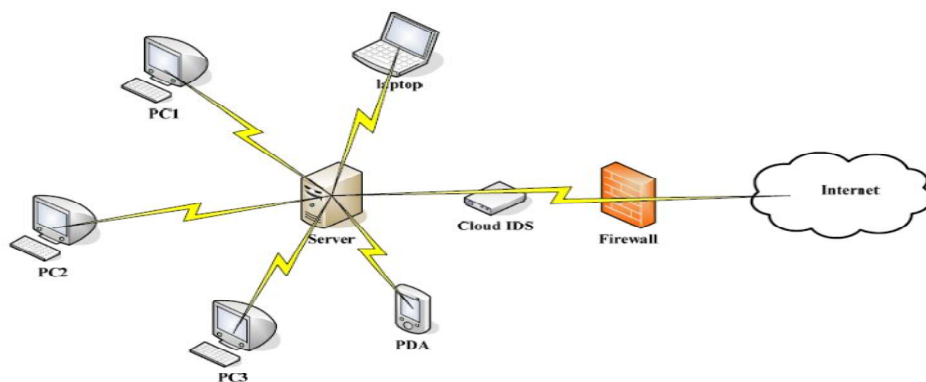
۲-۲-۱-۲-۲- چالش‌های توسعه سیستم‌های تشخیص و جلوگیری از نفوذ

سیستم‌های تشخیص و جلوگیری از نفوذهای قدیمی برای نمونه‌های جدید شبکه‌سازی مشابه شبکه‌های بی‌سیم و موبایل بکار برده نمی‌شوند. آنها همچنین برای اینکه نیازمندی‌های شبکه‌هایی با سرعت بالا را برطرف نمایند با مشکل مواجه شده‌اند. یکی از فاکتورهای مهم در عدم استفاده گسترده سیستم‌های تشخیص و جلوگیری از نفوذ، نرخ بالای اعلان خطای اشتباه است. همچنین با وجود روش‌ها و راه‌حل‌های گوناگون، استاندارد عمومی و یا معیار جامعی برای ارزیابی یک سیستم تشخیص و جلوگیری از نفوذ وجود ندارد.

تشخیص حملات داخلی نیز خیلی مشکل است. ضمناً تهدیدات داخلی در حال افزایش هستند. تنظیمات مناسب سیستم و ارائه سیاست‌های مناسب برای اجرای مجموعه‌ای از قوانین برای نفوذگران داخلی کاری بسیار سخت می‌باشد. [13] از جمله ویژگی‌های سیستم‌های تشخیص و جلوگیری از نفوذ ایده آل برای داشتن عملکرد بهینه، با حداکثر محافظت و حداقل خطا می‌توان به طراحی ساده، انطباق با تغییرات در رفتار کاربر و سیستم در طول زمان، عملکرد بلادرنگ، نظارت و محافظت از خود در مواردی که بوسیله مهاجم تغییر می‌کند و تنظیم خودکار با توجه به تغییر سیاست‌های امنیت سیستم نظارت شده، کار با حداقل سربار، اجرای پیوسته با کمترین مداخله انسان و کار با حداقل سربار اشاره کرد.

۲-۲-۱-۳- سیستم‌های تشخیص پیشگیری نفوذ در محاسبات ابری

امروزه خیلی از سازمان‌ها سرویس‌های پردازش خود را روی محیط ابر قرارداده‌اند که مسائل و چالش‌های امنیتی جدیدی را در مورد ایمنی و فعالیت مطمئن بوجود آورده است [13]. بیشتر سیستم‌های تشخیص نفوذ برای کنترل انواع خاصی از حملات طراحی شده‌اند. این نشان می‌دهد که یک تکنولوژی نمی‌تواند حفاظت در برابر حملات آینده را ضمانت کند از این رو نیاز به شمای مجتمع که می‌تواند حفاظت قوی در برابر یک طیف کامل تهدیدات را ارائه کند، وجود دارد.



شکل ۲-۱۱- دید مفهومی از CIDS [13]

اگرچه سیستم‌های تشخیص و جلوگیری از نفوذهای توزیع شده برای توانایی حفاظت از ایمنی در شبکه‌های با مقیاس بالا طراحی شده‌اند اما بهره برداری و استقرار آنها در محاسبات ابری با مشکلات بسیاری مواجه شده است و هنوز یک کار چالش برانگیز است. تنوع کاربران سرویس ابر و پیچیدگی معماری منحصربفرد آن کار را پیچیده‌تر کرده است. محاسبات ابری همه مسائل ایمنی شبکه و سیستم‌های موجود را به ارث می‌برد. [13]

۲-۲-۱-۴- مسائل امنیتی در محاسبات ابری

هنگامی که مشتریان ابر از تکنولوژی ماشین مجازی استفاده می‌کنند، حملات مبتنی بر شبکه و میزبان روی سرور راه دور مهمترین مسئله امنیتی در محیط‌های ابر می‌باشد. همچنین بررسی مشتری توسط ابر برای کنترل انسجام همه سیاست‌های امنیتی کار دشواری است. بنابراین وجود یک مکانیزم خودکار برای کنترل جامعیت داده و آنالیز آنها ضروری است. کاربر ابر یک قرارداد یا موافقت نامه برای ارائه سرویس، با ارائه دهنده سرویس ابر منعقد می‌نماید. این قرارداد مسائل امنیتی مانند عدم انکار مسئولیت پذیری کاربر در قبال رخداد اشتباه در داده‌ها و برنامه‌های کاربردی با ارزش را شامل می‌شود. هنگامی که محیط ابر مورد تهاجم قرار می‌گیرد، عدم دسترسی به سرویس منجر به خروج (از دست رفتن) محیط ابر می‌شود که این خود می‌تواند باعث خسارت مالی برای سازمان‌ها و کاربران ابر شود. محرمانگی داده روی ابر یکی از مسائل امنیتی مهم است. داده رمزنگاری شده می‌تواند از دسترسی یک کاربر خطرناک ایمن باشد اما محرمانگی داده حتی از مدیر داده در ارائه دهنده سرویس نیز پنهان نخواهد بود.

۲-۲-۱-۵- چالش‌های استقرار سیستم‌های تشخیص و جلوگیری از نفوذها در محیط‌های پردازش ابری

شناسایی چالش‌هایی که قبل از استقرار یک سیستم‌های تشخیص و جلوگیری از نفوذ آغاز می‌شوند، بسیار مهم است. چالش‌های خاصی وجود دارد که توسعه‌دهندگان در حین توسعه سیستم‌های تشخیص و جلوگیری از نفوذ در محیط‌های پردازش ابری با آنها مواجه‌اند. سیستم‌های قدیمی تشخیص و جلوگیری از نفوذ به دلیل ماهیت سیستم‌های نظارت شده، تمایل دارند به اینکه ثابت باشند.

سیاست‌های امنیتی معمولاً بوسیله مدیر سیستم برای امنیت کل سیستم محقق و مدیریت می‌شوند. ابر چندین مدیر امنیتی سیستم دارد که این مساله روی زمان پاسخ به نفوذ اثر منفی می‌گذارد زیرا مداخله انسان سرعت زمان پاسخ را کم خواهد کرد. [1]

فعالیت مخرب به راحتی بوسیله پیوستن یک مخرب به یک ارائه دهنده سرویس ابر انجام‌پذیر است. در همین حال، تحقیقات اخیر شواهدی ارائه می‌دهد که بسیاری از مهاجمان خودی هستند. پیشنهادات موجود برای حل این مشکل بطور عمده در نظارت بر فعالیت‌های کارکنان و تدوین سیاست‌های ارائه دهنده ابر اعمال می‌گردد. زیرساخت مشترک و تکنولوژی مجازی‌سازی آسیب‌پذیری بیشتری روی پردازش ابری اعمال کرده است. هر گونه نقصی در hypervisor که

اجازه ایجاد ماشین مجازی و اجرای چندین سیستم عامل را می‌دهد، پلت فرم را در معرض دسترسی و کنترل نامناسب قرار می‌دهد. یک مسئله بسیار مهم در محاسبات ابری، هزینه انتقال داده است. برای مثال در ابر آمازون هزینه انتقال داده در حدود 100 تا 150 دلار برای ترابایت است. بنابراین می‌بایست برای ارائه راه حل موثر کم هزینه برای سیستم‌های تشخیص و جلوگیری از نفوذ در محیط ابر با کاهش پهنای باند شبکه تلاش کرد.

مساله دیگر، نظارت درون ترافیک ماشین مجازی روی یک پلت فرم میزبان مجازی است. از آنجایی که سوئیچ هم مجازی است بنابراین، راه حل‌های قدیمی برای نظارت فیزیکی قادر به بازرسی ترافیک شبکه نیست، علاوه بر این پلت فرم جدید مجازی سازی آسیب پذیری خودشان را دارند بنابراین آنها باید نظارت و ارزیابی شوند.

عدم شفافیت در مورد شیوه‌های مدیریت امنیت مانند سیاست‌های امنیتی، حسابرسی، ورود به سیستم، آسیب پذیری و به پاسخ به حادثه منجر به عدم کارآمدی تکنیک‌های مدیریت تهدید قدیمی شده است.

۲-۲-۱-۶- سیستم‌های تشخیص و جلوگیری از نفوذ مبتنی بر محاسبات ابری

بیشتر سیستم‌های تشخیص و جلوگیری از نفوذهای پیشنهادی فعلی که روی محیط ابر کار می‌کنند در هر یک از لایه‌های زیرساخت، پلت فرم و برنامه‌های کاربردی بطور جداگانه عمل می‌کند و بطور عمده از تشخیص و پیشگیری مستقل از دیگر لایه‌ها حمایت می‌کند. در اینجا به برخی از پژوهش‌های انجام شده جهت برطرف نمودن چالش‌های استقرار سیستم‌های تشخیص و جلوگیری از نفوذ می‌پردازیم.

برای اجرای سیستم‌های تشخیص و جلوگیری از نفوذها در لایه زیرساخت، Tupakula یک مدل مبتنی بر مانیتور ماشین مجازی به اسم Hypervisor پیشنهاد داده که برای جلوگیری از انواع مختلف حمله در لایه زیرساخت می‌باشد. مدل آنها قابلیت اطمینان و دسترسی را برای سیستم بهبود می‌بخشد چون زیرساخت می‌تواند در بیشتر اوقات ایمن باشد و اجرای سرویس‌ها می‌تواند تکیه بر زیرساخت ایمن داشته باشد.

مانیتورهای ماشین مجازی قادر به بهبود کارایی تشخیص و جلوگیری از نفوذ در سیستم‌های تشخیص و جلوگیری از نفوذ می‌باشد به این دلیل که کنترل کامل منابع سیستم را در اختیار دارد و دید خوبی از وضعیت داخلی ماشین مجازی دارا است. بنابراین این راه حل می‌تواند بر مشکل پویایی سیستم‌های نظارتی ماشین مجازی فائق آید. [1]

یادگیری ماشین روش دیگری است که جهت آموزش سیستم برای تشخیص انومالی مورد استفاده است. Vieira و همکارانش یک سیستم تشخیص نفوذ پردازش ابری گرید پیشنهاد داده‌اند (GCCIDS) که حملات را بوسیله یک سیستم حسابرسی از طریق ادغام روش‌های سوءاستفاده و انومالی پوشش می‌دهد. [1]

برای تشخیص نفوذ خاص پژوهشگران از شبکه عصبی مصنوعی (ANN) برای آموزش سیستم و توسعه یک نمونه با استفاده از یک میان افزار به اسم Grid-M استفاده کرده‌اند. آنها ثابت کرده‌اند که سیستم شان هزینه پردازشی کمی دارد در حالیکه

کارایی رضایت بخشی برای پیاده سازی بلادرنگ دارد. زیرا در اینجا آنالیز جداگانه‌ای روی هر گره نود انجام می‌شود و این پیچیدگی سیستم را کاهش می‌دهد. [1]

با ارائه راه‌حل پردازش خودمختار به تازگی پژوهشگران برای طراحی، ساخت و مدیریت سیستم‌های تشخیص و جلوگیری از نفوذ با حداقل مداخله انسانی تلاش کرده‌اند. هر سیستم خودمختار می‌بایست قابلیت تطبیق با رفتار خودش را بطور مناسب با زمینه استفاده از طریق روش‌های خودمدیریت، خود تنظیم، خود پیکربندی و خود تشخیص داشته باشد. [1]

Azmandian و همکاران با استفاده از روش‌های داده‌کاوی، روشی جدید در طراحی سیستم‌های تشخیص برای محیط‌های سرور مجازی که با بهره‌برداری از اطلاعات موجود از مانیتورهای ماشین مجازی ارائه داده‌اند. تکنیک پیشنهادی آنها از دقت تشخیص بالا با حداقل هشدار خطا حمایت کرده است اما برطرف کردن عدم معناشناسی برنامه برای مقاومت نرم‌افزار مخرب و سهولت استقرار با استفاده از هستی شناسایی می‌تواند این شکاف معنایی را پر کند. بعضی از این پژوهشگران با بهره‌گیری از منابع موجود و بهینه‌سازی پاسخ از طریق ارزیابی و آنالیز ریسک با روش آنالیز فازی تلاش کرده‌اند. [1]

Lee و همکارانش سیستم‌های تشخیص چند لایه پیشنهاد کرده‌اند و مدیریت log بوسیله بکارگیری سطوح مختلف نقاط قوت امنیت برای کاهش حقوق دسترسی بر اساس سطح آنومالی و تعداد کاربران شبکه ابر یا مهاجمان بالقوه صورت گرفته است. این بدان معنی است که log‌های ایجاد شده بوسیله مهاجمانی که بالاترین سطح آنومالی یا ریسک امنیت دارند، با بالاترین اولویت حسابرسی شده‌اند. اشکال عمده این است که IDS آنها به اندازه کافی برای تشخیص حملات توزیع شده با مقیاس بالا، قدرتمند نیست. [1]

Takahashi و همکاران روش‌های ارزیابی خطر را معرفی کرده و یک سیستم‌های تشخیص هستی شناسانه روی محاسبات ابر تعریف کرده‌اند که بر اساس موجودیت کار می‌کند و به یک سیستم حسابرسی برای آسیب‌پذیری‌ها و ضعف‌ها مجهز شده است. [1]

سیستم‌های تشخیص و جلوگیری از نفوذ مبتنی بر مجازی‌سازی برای محیط‌های پردازش ابری بوسیله Jin پیشنهاد شده که مورد استفاده نظارت جریان داده شبکه و جامعیت فایل بلادرنگ است. سیستم‌های تشخیص و جلوگیری از نفوذ پیشنهادی آنها کنترلی بر روی میزبان ندارد که آسیب‌پذیری حملات داخلی را کاهش داده است. [1]

۲-۲-۱-۷- الزامات سیستم‌های تشخیص و جلوگیری از نفوذ

محاسبات ابری که شامل شبکه‌ها و سیستم‌هایی در مقیاس بزرگ می‌باشند نگهداری تغییرات در منابع بصورت خودکار و بدون دخالت انسان بسیار مهم است، برای غلبه بر پیچیدگی بشکل پویا، سیستم‌های تشخیص و جلوگیری از نفوذ می‌بایست قادر به مدیریت خودش با حداقل دخالت انسان باشد که نظارت و کنترل عناصر شبکه را بصورت بلادرنگ تسهیل می‌کند. با توجه به رشد حملات پیچیده غیرقابل پیش‌بینی برای سیستم ضروری است که حملات جدید و مقاصد آسیب‌پذیری را برای انتخاب بهترین پاسخ مطابق با شدت خطر و استراتژی‌های پیشگیری مناسب تشخیص داده شود. سیستم می‌بایست

قابلیت یادگیری داشته باشد و قابلیت تشخیص خود را در طول زمان برای پشتیبانی از درک تمام یا بیشتر تشخیص با حداقل تعداد هشدار اشتباه را بهبود بخشد که این نیز نیازمند یک طراحی کارآمد برای حفظ یک سطح عملکرد و امنیت مطلوب در زمان مشابه با کمترین منابع پردازشی است.

جلوگیری و تشخیص سریع یک فاکتور خیلی مهم برای سیستم‌های تشخیص و جلوگیری از نفوذ است از آنجا که این روی عملکرد کل سیستم برای تحویل QoS از پیش توافق شده تاثیر می‌گذارد. یک سیستم مبتنی بر محاسبه ابر با مدیران متعهد می‌بایست برای جلوگیری از اتلاف وقت برای پاسخ اجرایی، دخالت انسان را به حداقل یا صفر برساند. این می‌بایست بصورت بلادرنگ کار کند و بصورت خودکار به فعالیت‌های مشکوک پاسخ ارائه کند که این خود باعث افزایش این تحمل خطا و کاهش سربار شود. [1]

سیستم‌های تشخیص و جلوگیری از نفوذ می‌بایست این قابلیت را داشته باشد که با تغییرات پیکربندی گره‌های پردازشی که بصورت پویا اضافه و حذف می‌شوند منطبق باشد. طراحی یک معماری مناسب برای سیستم‌های تشخیص و جلوگیری از نفوذ همکار تعیین خواهد کرد که هشدارها چگونه می‌بایست پردازش شوند. سیستم‌های تشخیص و جلوگیری از نفوذ به منظور کنترل کارآمد تعداد زیادی از گره‌های موجود شبکه در ابر و ارتباط بار پردازش و ارتباط میان آنها می‌بایست مقیاس پذیر باشد. قرار دادن کنترل کننده تشخیص و ارتباط می‌تواند روی مقیاس‌پذیری و عملکرد سیستم‌های تشخیص و جلوگیری از نفوذها تاثیر می‌گذارد.

محاسبات ابری سرویس‌های عملیاتی حیاتی ارائه می‌کند که الزامات عملکردی خاصی را از جمله قابلیت اطمینان، دسترس‌پذیری و کیفیت سرویس و طراحی ساده و حداقل سربار حمایت می‌کند. یک سیستم تشخیص و جلوگیری از نفوذ می‌بایست قادر به ارائه و نگهداری یک سطح قابل قبول از سرویس در صورت شکست باشد.

یک سیستم تشخیص و جلوگیری از نفوذ مشترک عظیم شامل تعداد زیادی از سیستم‌های تشخیص و جلوگیری از نفوذهای مستقل است در حالی که هر سیستم بطور مستقل عمل می‌کند و نفوذ و ناهنجاری‌ها را تشخیص می‌دهد. اطلاعاتشان و فعالیت‌هایشان می‌بایست به منظور تشخیص حملات همزمان و اتخاذ استراتژی پیشگیری مناسب هماهنگ باشد.

با اشاره به نظارت و محافظت از خود در مواردی که ممکن است بوسیله مهاجم تغییر کند یک سیستم تشخیص و جلوگیری از نفوذ می‌بایست از خودش از دسترسی یا حملات ناشناس حفاظت کند. یک سیستم تشخیص و جلوگیری از نفوذ می‌بایست قادر به اعتبارسنجی وسایل شبکه باشد.

۲-۲-۳- سابقه پژوهش ایجاد امنیت در ابر رایانشی

در حال حاضر کاربران بطور فزاینده‌ای به سرویس‌های ذخیره‌سازی داده برای نگهداری اطلاعات و داده‌های خود، بصورت آنلاین متکی هستند که این سرویس‌ها قابلیت دسترسی، در هر زمان و هر مکانی را دارند. به همراه این سرویس‌ها مسائلی

همانند امنیت و حفظ حریم خصوصی مطرح می‌شود چرا که داده‌های کاربران در محلی خارج از کنترل کاربر ذخیره و نگهداری می‌شوند. [30]

بعنوان مثال در جدیدترین اقدام شرکت گوگل، جهت حفظ حریم خصوصی افراد در گوگل پلاس، برای رفع نگرانی‌های کاربر از افشاء اطلاعات محرمانه و شخصی خود بعد از مرگ، با ارائه سرویسی که در آن کاربر تعیین می‌کند در صورت غیبت‌های مکرر با فواصل زمانی مشخص به شرکت این اجازه داده می‌شود که اطلاعات را حذف و یا به شخصی که خود کاربر مشخص می‌کند ارسال گردد. (ارائه این گونه سرویس‌ها دلیلی بر اهمیت حفظ حریم خصوصی در محیط‌های به اشتراک‌گذاری داده همانند ابر می‌باشد).^{۲۳}

محاسبات ابری بعنوان یک مدل جدید برای ارائه سرویس‌های که دارای مزایای همچون حذف هزینه‌های اضافی از طریق به اشتراک‌گذاری منابع محاسباتی و فراهم کردن یک مدل هزینه‌ای براساس میزان استفاده (On-Demand) توجه کاربران زیادی را متوجه خود ساخته است [32]. بدون ارائه راه‌حلی جامع و شفاف درحوزه امنیت و حفظ حریم خصوصی، ارائه خدمات در ابر ممکن است به شکست بینجامد، لذا ارائه‌دهندگان سرویس‌های ابر ناچارند به یکی از مهمترین مسائل مربوط به محاسبات ابری که همان حفظ حریم خصوصی و امنیت می‌باشد بطور جدی توجه نموده و در این راستا اعتماد و رضایت کاربران را جلب نموده تا نگران داده‌های شخصی خود نباشند [35].

۲-۲-۳-۱- مفهوم حریم خصوصی در محاسبات ابری

مفهوم محرمانگی و امنیت در میان کشورها و جوامع و حوزه‌های قضایی مختلف متفاوت می‌باشد و به کمک انتظارات عمومی و تفاسیر حقوقی شکل می‌گیرد، ارائه یک تعریف کامل از محرمانگی و امنیت گرچه غیرممکن نیست ولی دشوار است، تعهداتی که شامل حریم خصوصی می‌شود عبارتند از جمع‌آوری، استفاده، افشاء، ذخیره‌سازی و تخریب داده‌های شخصی افراد می‌باشد. بخاطر عدم وجود هیچگونه اجماع جهانی در مورد اینکه چه مواردی شامل حریم خصوصی می‌شود در اینجا از تعریفی که توسط موسسه آمریکایی AICPA^{۲۴} و موسسه کانادایی CICA^{۲۵} ارائه شده است استفاده می‌کنیم:

حریم خصوصی شامل حقوق و تعهدات اشخاص و سازمانها در رابطه با جمع‌آوری، استفاده، حفظ و افشاء اطلاعات خصوصی افراد می‌باشد [30]

باتوجه به اهمیت داده و اطلاعات، بهتر است که ابتدا انواع اطلاعاتی را که شامل حریم خصوصی می‌باشد را بیان نموده و در ادامه آن چرخه زندگی داده را مطرح کنیم.

۲-۳-۲-۲- انواع اطلاعات نیازمند به حفاظت

اطلاعات شخصی کلمه ایست که به طریق مختلف توسط کاربران استفاده میشود اما در این گزارش آن را به اطلاعات حساس خصوصی که شامل موارد ذیل می باشد تفسیر می کنیم. [31]

- **اطلاعات شناسایی افراد**^{۲۶}: شامل هرنوع اطلاعاتی که بتوان از آن برای شناسایی افراد و مکان آنها (نام و آدرس) و یا اطلاعاتی که بتوان آن را با اطلاعات دیگری برای شناسایی یک نفر مرتبط کرد، می باشد که شامل شماره کارت اعتباری، کد پستی می باشد.

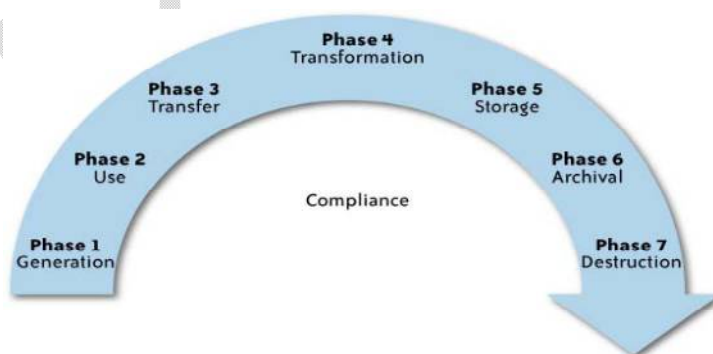
- **اطلاعات حساس**^{۲۷}: شامل اطلاعاتی درباره مذهب، بهداشت، گرایش های جنسیتی، عضویت در گروه ها، تخصص افراد و یا هر گونه اطلاعات خصوصی دیگر است.

- **داده های استفاده شده**^{۲۸}: شامل هر نوع اطلاعات مربوط به استفاده از دستگاه ها، محتوای دیده شده، وب سایت های که توسط کاربر استفاده شده اند و هر گونه اطلاعات مربوط به چرخه استفاده کاربر از تکنولوژی ها.

- **اطلاعات شناسایی یکتا دستگاه**^{۲۹}: شامل هرنوع اطلاعاتی که بتوان برای ردیابی دستگاه کاربر استفاده کرد مانند فرکانس رادیویی، تگ RFID و IP Address.

۲-۳-۳- چرخه زندگی داده

برای داشتن یک نگاهی بنیادین به حفظ حریم خصوصی بهتر است توجه خود را به داده و مراحل داده می کند که به آن اصطلاحاً چرخه عمر داده می گویند معطوف کنیم. همانطور که می دانیم اطلاعات شخصی افراد باید همانند قسمتی از داده های مورد استفاده در سازمان از همان مراحل ابتدایی ورود به سازمان تا آخرین مراحل مدیریت شوند. در ادامه مسائلی را که در هر مرحله از چرخه عمر داده، وجود دارد را با شکل مطرح می کنیم. [33]



شکل ۲-۱۲- چرخه زندگی داده [33]

26 Personally Identifiable Information

27 Sensitive Information

28 Usage Data

29 Unique Device Identities

۲-۲-۳-۱-تولید^{۳۰}

در این فاز سازمان باید در مورد مالکیت اطلاعات خصوصی، آگاهی کامل داشته به این معنی که اطلاعات خصوصی چگونه بوجود می‌آیند و مالکیت اطلاعات خصوصی در سازمان چگونه نگهداری می‌شود.

۲-۲-۳-۲-استفاده^{۳۱}

در این فاز به بررسی مسائل استفاده از داده‌های خصوصی افراد و سازمان‌ها پرداخته می‌شود و مشخص می‌شود آیا تنها استفاده کننده از داده‌ها فقط مالک داده می‌باشد یا توسط شخص سومی نیز مورد استفاده قرار می‌گیرد.

۲-۲-۳-۳-انتقال^{۳۲}

زمانی که اطلاعات یک سازمان از طریق یک شبکه عمومی به ابر ارسال می‌شود شانس سرقت اطلاعات وجود دارد و باید تمهیداتی جهت اینگونه مسائل در نظر گرفته شود.

۲-۲-۳-۴-تبدیل^{۳۳}

به هنگام تبدیل اطلاعات، هر کاربری باید از جامعیت داده‌های خصوصی خود اطمینان حاصل پیدا کند.

۲-۲-۳-۵-ذخیره سازی^{۳۴}

مکانیزم‌های کنترل دسترسی مناسبی برای محدود کردن دسترسی کاربران به داده‌ها باید در نظر گرفته شود.

۲-۲-۳-۶-بایگانی^{۳۵}

در این فاز مدت زمان نگهداری داده‌ها مشخص می‌شود به این معنی که فراهم کننده سرویس ابر برای چه مدت زمانی داده‌ها را باید نگهداری کند.

30 Generation

31 Use

32 Transfer

33 Transformation

34 Storage

35 Archive

۲-۲-۳-۷-تخریب^{۳۶}

فراهم کننده سرویس ابر باید پس از اینکه کاربر درخواست حذف داده‌های خود را کرد، باید بگونه‌ای اطلاعات را حذف نماید که توسط دیگران قابل بازیابی نباشد.

۲-۲-۳-۴-مسائل حریم خصوصی و چالش‌های آن

موضوع حریم خصوصی مدت زمانی است که وارد صنعت IT شده و قوانین بسیاری جهت حفاظت از اسرار تجاری شرکت‌ها و اطلاعات خصوصی افراد بوجود آمده است. متأسفانه با وجود این قوانین منقضی و ناکارآمد، دیگر جوابگویی مسائل مربوط به حفظ حریم خصوصی نیستند و نیاز به سناریوهای جدیدی می‌باشد که بتواند اعتماد کاربران را بخوبی جلب نماید بخصوص زمانی که یک رابطه جدیدی بین کاربران و فراهم کننده سرویس ابر بوجود می‌آید. در ادامه به مسائل مربوط به حفظ حریم خصوصی در محاسبات ابری می‌پردازیم. [31]

۲-۲-۳-۴-۱-دسترسی^{۳۷}

فراهم کنندگان سرویس ابر، دارای توانایی دسترسی به اطلاعات خصوصی افراد می‌باشند، بنابراین باید به کاربران این اطمینان داده شود که پس از صدور دستور حذف تمامی داده‌هایشان غیر قابل بازگشت هستند هر چند بسیاری از کاربران این اطمینان را پیدا نمی‌کنند.

۲-۲-۳-۴-۲-مقبولیت^{۳۸}

لیستی از قوانین بین المللی و استانداردها و تفاهم نامه‌ها وجود دارد که بر عملکرد سرویس دهندگان ابر در حوزه حریم خصوصی نظارت دارند مانند قطعنامه مادرید که در سال ۲۰۰۹ به تصویب پنجاه کشور رسید.

۲-۲-۳-۴-۳-ذخیره سازی^{۳۹}

در این فاز به مسائل مربوط به محل فیزیکی ذخیره‌سازی داده‌های کاربران در محاسبات ابری پرداخته می‌شود. مکان‌های فیزیکی زیادی در دنیا برای ذخیره‌سازی داده‌ها وجود دارد خیلی از سازمان‌ها مایل به ذخیره سازی داده‌هایشان در خارج از سازمان نیستند. ذخیره‌سازی داده‌ها در دیتا سترهای مختلف در مکان‌های گوناگون منجر به دسترسی‌های غیرمجاز در استفاده از داده‌ها ممکن است بشود.

-
- 36 Destruction
 - 37 Access
 - 38 Compliance
 - 39 Storage

۲-۲-۳-۴-حفظ و نگهداری^{۴۰}

که بر حفظ و نگهداری داده‌ها دلالت دارد، داده‌های ذخیره شده باید بطور اتوماتیک پس از کامل شدن مدت زمان نگهداری که از قبل مشخص شده مشخص شده توسط کاربر، توسط ارائه دهنده سرویس بطور کامل حذف شوند.

۲-۲-۳-۵-تخریب^{۴۱}

فراهم کننده سرویس ابر بدون کسب مجوز از کاربر، حق حذف داده‌ها را ندارد.

۲-۲-۳-۵-نظارت و مانیتورینگ^{۴۲}

که بر عملکرد فراهم کنندگان سرویس ابر از نگاه کاربران می پردازد چراکه فراهم کنندگان سرویس ابر بطور مناسبی مورد بازرسی قرار نمی گیرند که این امر موجب استفاده غیرمجاز از داده‌های کاربر می شود.

۲-۲-۳-۶-نقض حریم خصوصی^{۴۳}

اگر هر گونه عمل غیر انسانی با داده‌های کاربران انجام شود خود کاربران ابر باید متوجه این موضوع شوند، در صورت عدم تشخیص این موضوع توسط کاربر، ممکن است موجب خسارت‌های زیادی در تجارت بشود.

۲-۲-۳-۷-تکنیک های متداول جهت حفظ حریم خصوصی

در اینجا به دو مورد از تکنیک‌های متداول حفظ حریم خصوصی اشاره می‌کنیم. [34]

۲-۲-۳-۷-۱-Encryption Model

بخاطر حفظ حریم خصوصی افراد، رمزگذاری داده‌های خصوصی آنها قبل از ارسال به ابر، امری ضروری می باشد ولی این کار دارای نقاط ضعفی نیز می‌باشد زمانی که صاحب فایل رمزگذاری شده می خواهد درون فایل رمزگذاری شده به جستجوی داده خاصی پردازد، ناچار است همه فایل رمزگذاری شده را دانلود و سپس از حالت رمزگذاری خارج و به جستجوی اطلاعات پردازد، اگر حجم داده بالا باشد و کاربر بخواهد از طریق موبایل این کار را انجام دهد این روش بسیار ناکارآمد و نشدنی می‌باشد در غیر اینصورت کاربر باید کلید رمزگذاری را به خود ابر ارسال نموده و فراهم کننده سرویس

40 Retention

41 Destruction

42 Audit & Monitoring

43 Breaches

فایل را از حالت فشرده خارج نموده و به جستجو در فایل اقدام نموده که این اقدام خود موجب افشای کلید رمزنگاری می‌گردد، به همین خاطر مدل‌های جهت اطمینان از حفظ جامعیت فایل‌های داده‌ای بوجود آمدند.

۲-۲-۳-۷-۲-Access Control Mechanism

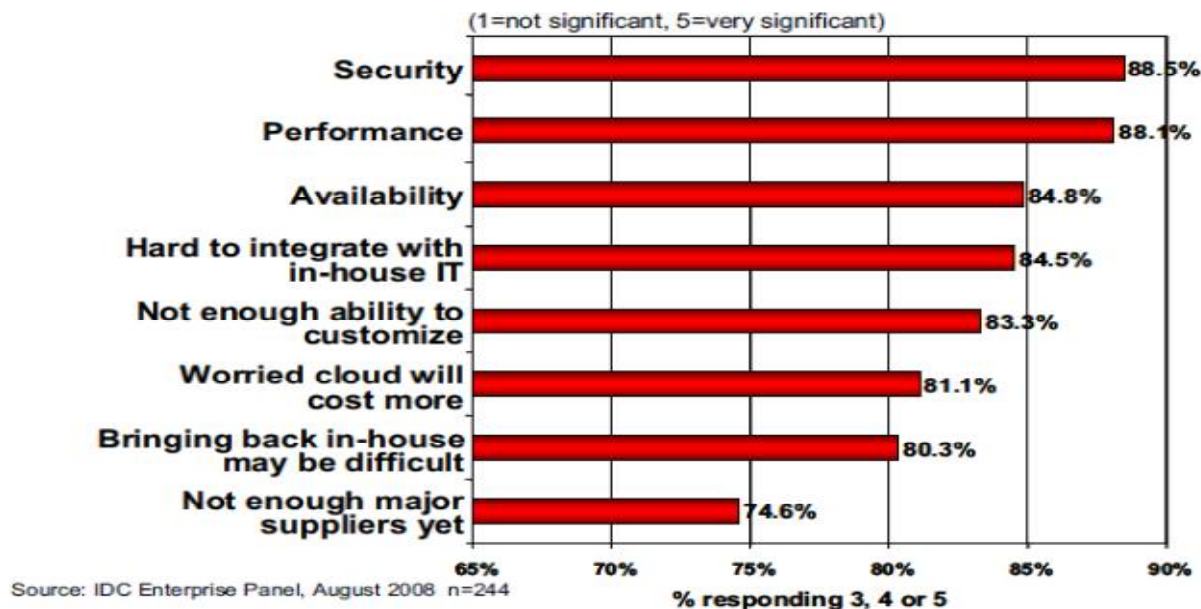
در این تکنیک هویت کاربران قبل از ورود به ابر جهت دسترسی به داده‌ها بدون اینکه خود کاربران متوجه شوند مورد بررسی قرار می‌گیرد و تنها کاربران مجاز قادر به دسترسی به داده‌ها می‌باشند.

هدف اصلی این پروژه بررسی امنیت ابر تحت چهار سناریو مختلف NS2 به عنوان ابزار شبیه‌سازی در این پروژه استفاده می‌شود و چهار سناریو در این زمینه ایجاد شده است. سناریو اول بررسی راهکار امنیتی در حمله از طریق کدهای مخرب، سناریو دوم راهکار امنیتی حمله به بسته در حالیکه سومین سناریو راهکار امنیتی حمله سیل آسا می‌باشد. هر چهار سناریو بعنوان معیارهای SOAP برای برنامه‌های کاربردی فردی و نیز تخمین زدن عملکرد درست ابر مقایسه شده است. بطور کلی رایانش ابری فن‌آوری کلیدی است که به شکل گسترده‌ای در بسیاری از سازمان‌ها مورد استفاده قرار گرفته است. مزیت اصلی محاسبات ابری این است که، خطر وابستگی به نگهداری زیرساخت‌های زیاد را کاهش می‌دهد. بسیاری از ارائه دهندگان خدمات طیف گسترده‌ای از خدمات را برای مشتریان خود به شکل خدمات ابری ارائه می‌دهند و مشتری می‌تواند از یک مکان از راه دور از آنها استفاده کند. به غیر از لیستی از مزایای محاسبات ابری برخی از محدودیت وجود دارد و امنیتی نقش مهمی را در میان آنها بازی می‌کند. تامین امنیت اطلاعات مشتری و داده‌ها با چالش‌های اصلی برای ارائه دهندگان خدمات ابر روبروست و تحقیقات بسیاری در این زمینه به ارائه امنیت مورد نیاز برای اطلاعات و داده‌ها انجام شده است. به طور کلی خدمات ارائه شده توسط ارائه‌دهندگان خدمات ابری از طریق وب قابل دسترسی هستند و مسدود کردن ترافیک وب در دسترسی همگانی به ابر باید اولویت داده شود.

۲-۲-۳-سابقه پژوهش کلی در بررسی راهکارهای امنیتی در رایانش ابری

براساس بررسی‌های انجام شده در سال 2002 میلادی همان گونه که در شکل زیر نشان داده شده است، امنیت به عنوان مهم‌ترین چالش رایانش ابری از میان 9 چالش موجود شناخته شده است. [39]

با این وجود نگرانی‌هایی در مورد عملکرد و قابلیت در دسترس بودن و رایانش ابری جزء دیگر چالش‌ها پس از امنیت مطرح شده است. جدیدترین بررسی‌ها در سال 2012 حاکی از کاهش 33 درصدی چالش امنیت و رسیدن این درصد به عدد 33 می‌باشد. [7,8]



شکل ۲-۱۳- نتایج بررسی IDC از چالش های رایانش ابری در سال (۲۰۰۲) [39]

تهدیدهای امنیتی بر روی کاربران ابر به دو دسته داخلی و خارجی تقسیم بندی می شود. [39] تهدیدهای خارجی شامل تهدید مراکز داده بزرگ می باشد که این نگرانی امنیتی در میان کاربران ابر و فراهم آورندگان (که به عنوان شخص ثالث در نظر گرفته شده اند) در حصول اطمینان از نرم افزارهای امن امکان پذیر است.

مسئولان امنیت رایانش ابری در سه لایه بیان شده متفاوت هستند به گونه ای که در لایه نرم افزار کاربردی به عنوان سرویس ارائه دهنده سرویس مسئول امنیت فیزیکی است و وظیفه اجرای سیاست های خارجی دیوار آتش را به عهده دارد. در برقراری امنیت لایه پلتفرم به عنوان سرویس کاربر و ارائه دهنده سرویس هر دو سهیم می باشند. در پایین ترین سطح یعنی لایه زیرساخت به عنوان سرویس بیشترین مسئولیت بر عهده کاربر می باشد. علاوه بر مسائل مربوط به امنیت خارجی ابر دارای برخی از مسائل مربوط به امنیت داخلی نیز می باشد که در آن کاربران باید در مقابل حملات از یکدیگر محافظت شوند.

مجازی سازی یکی از مکانیزم های اصلی است که در مقابل تلاش های کاربران برای حمله به یکدیگر و متعاقباً حمله به زیرساخت رایانش ابری، دفاع قدرتمندی را از خود نشان می دهد. البته در پی گفته قبلی باید به این نکته توجه داشت که منابع مجازی و محیط های مجازی سازی عاری از ایراد نیستند و نرم افزارهای کاربردی مجازی سازی شامل اشکالاتی در زمینه کدها می باشند. مجازی سازی شبکه هایی که نادرست طراحی شده اند اجازه دسترسی یک کاربر به زیرساخت ارائه کننده و منابع دیگر کاربران را می دهند. همچنین ابر باید از ارائه دهندگان که پایین ترین لایه زیرساخت به عنوان سرویس را در دست دارند هم محافظت شود زیرا این مهم می تواند در از دست دادن داده های ناخواسته سهیم باشد.

۲-۳-۱-علل شکست امنیت رایانش ابری

شکست در به دلایل زیر رخ می دهد:

الف) به علت سخت افزاری که در لایه زیرساخت به عنوان سرویس ابر رخ می دهد.

ب) به علت نفوذ کدهای مخرب در نرم افزار که در لایه نرم افزار کاربردی به عنوان سرویس رخ می دهد.

ج) به علت نفوذ کدهای مخرب در حال اجرا که توسط برنامه کاربردی کاربر یا تزریق اطلاعات ساختگی به برنامه توسط شخص ثالث صورت می گیرد. این رخداد در لایه پلتفرم به عنوان سرویس می تواند منجر به ایجاد نزاع و اختلا بین ارائه دهنده و مشتری شود.

با توجه به دلایل ذکر شده شکست در امنیت ابر می تواند نزاع میان ارائه دهنده سرویس و کاربران آن را به همراه داشته باشد. از طرفی از دیدگاه کاربر از دست رفتن اطلاعات یا قطعی در ارائه سرویس ها می تواند هزینه های مالی هنگفتی را در پی داشته باشد و از طرفی از دیدگاه ارائه دهنده سرویس ارائه خدمات با کیفیت مختلف شده و بدین ترتیب توافقات سطح سرویس (SLA) محقق نمی شود. [40]

۲-۲-۴-سابقه پژوهش امضای دیجیتالی [44,45,46]

۲-۲-۴-۱-امضای دیجیتال و امنیت دیجیتالی چیست

امضای [[دیجیتال]] برای فایل های اطلاعاتی همان کار را انجام می دهد که امضای شما بر روی سند کاغذی انجام می دهد. امضای دیجیتال و امضای دست نویس هر دو متکی بر این واقعیت هستند که پیدا کردن دو نفر با یک امضا تقریباً غیرممکن است. با امضای دیجیتال اصل بودن و صداقت یک پیغام یا سند و یا فایل اطلاعاتی تضمین می شود. به منظور ایجاد امضای دیجیتال از یک [[الگوریتم ریاضی]] به منظور ترکیب اطلاعات در یک کلید با [[اطلاعات]] پیام، استفاده می شود. ماحصل عملیات، تولید رشته ای مشتمل بر مجموعه ای از حروف و اعداد است. یک امضای دیجیتال صرفاً "به شما نخواهد گفت که" این شخص یک پیام را نوشته است، بلکه در پردازنده این مفهوم مهم است که: "این شخص این پیام را نوشته است".

از نگاهی دیگر یک گواهینامه دیجیتالی یک فایل دیجیتالی است که به صورت رمزگذاری شده ای حاوی اطلاعاتی از قبیل کلید عمومی و سایر اطلاعات دارنده خود است. دارنده می تواند یک شخص، یک شرکت، یک سایت و یا یک نرم افزار باشد. مانند یک گواهینامه رانندگی که عکس صاحب خود را به همراه سایر اطلاعات در مورد دارنده آن، شامل می شود، یک گواهینامه دیجیتالی نیز یک کلید عمومی را به اطلاعاتی در مورد دارنده آن متصل می کند. در کلام دیگر، گواهینامه دیجیتالی آلیس، تصدیق می کند که کلید عمومی به او و تنها او تعلق دارد. به همراه کلید عمومی، یک گواهینامه دیجیتالی حاوی اطلاعاتی در مورد شخص حقیقی یا حقوقی دارنده آن می باشد، که برای شناسایی دارنده (بر این اساس که گواهینامه ها محدود می باشند) و تاریخ ابطال آن را نمایش می دهد.

دفتر ثانویه مطمئن صادر کننده گواهینامه، هویت شخص دارنده گواهینامه را قبل از آنکه تصدیق کنند، چک می کنند. بخاطر اینکه گواهینامه دیجیتالی اکنون یک فایل اطلاعاتی کوچک است، اصل بودن آن توسط امضای دیجیتالی خودش قابل بررسی است لذا به همان صورتی که یک امضای دیجیتالی را تایید می کنیم به همان صورت از صحت امضای دیجیتالی به اصل بودن گواهینامه پی خواهیم برد.

۲-۲-۴-۲- گواهینامه دیجیتالی چیست [49]

یک گواهینامه دیجیتالی یک فایل دیجیتالی است که به صورت رمزگذاری شده ای حاوی اطلاعاتی از قبیل کلید عمومی و سایر اطلاعات دارنده خود است. دارنده می تواند یک شخص، یک شرکت، یک سایت و یا یک نرم افزار باشد. مانند یک گواهینامه رانندگی که عکس صاحب خود را به همراه سایر اطلاعات در مورد دارنده آن، شامل می شود، یک گواهینامه دیجیتالی نیز یک کلید عمومی را به اطلاعاتی در مورد دارنده آن متصل می کند.

۲-۲-۴-۳- ثبت نام برای یک گواهینامه دیجیتالی

کاربران می توانند از طریق وب برای یک گواهینامه دیجیتالی ثبت نام کنند. پس از کامل شدن فرم های مورد نیاز، مرورگر اینترنت کاربر یک جفت کلید عمومی درست می کند. نیمی از کلید عمومی به دفتر صدور گواهینامه برای درج در مشخصات دارنده آن ارسال می شود. درحالی که کلید خصوصی کاربر بر روی کامپیوتر او در جایی امن (هارد دیسک، فلاپی درایو و ...) نگهداری خواهد شد.

دفتر صدور گواهینامه در ابتدا ملزم به تایید اطلاعات ارسال شده توسط کلید عمومی کاربر می باشند. اینکار از جا زدن کسی به جای کس دیگر و احتمال وقوع تبادلات نامشروع و غیر قانونی جلوگیری می کند. اگر اطلاعات ارسال شده درست باشد، دفتر صادر کننده گواهینامه، یک گواهینامه دیجیتالی برای متقاضی خود صادر می کند. به محض صدور، دفتر صادر کننده گواهینامه امضای دیجیتالی را در یک بایگانی عمومی نگهداری می کند.

۲-۲-۴-۴- پخش کردن گواهینامه دیجیتالی

در حالیکه گواهینامه دیجیتالی در یک بایگانی عمومی ذخیره شده است نیز، می تواند با استفاده از امضای دیجیتالی پخش گردد. به طور مثال زمانیکه آلیس نامه ای را برای باب به صورت دیجیتالی امضا می کند، او همچنین گواهینامه خود را به آن نامه پیوست می کند. لذا همزمان با دریافت نامه دیجیتالی باب می تواند معتبر بودن گواهینامه آلیس را نیز بررسی کند. اگر با موفقیت تایید شد، هم اکنون باب کلید عمومی آلیس را دارد و نیز می تواند اعتبار نامه ارسالی از طرف آلیس را بررسی کند.

۲-۲-۴-۵- انواع مختلف گواهینامه دیجیتالی

بر حسب نوع استفاده از گواهینامه دیجیتالی، چند نمونه مختلف از آن موجود می‌باشد.

شخصی: قابل استفاده توسط اشخاص حقیقی برای امضای ایمیل و تبادلات مالی.

سازمان‌ها: قابل استفاده توسط اشخاص حقوقی برای شناساندن کارمندان برای ایمیل‌های محفوظ و تبادلات تحت اینترنت.

سرور: برای اثبات مالکیت یکی Domain اینترنتی.

تولید کنندگان: برای اثبات حق تالیف و حفظ حقوق آن برای نشر برنامه نرم‌افزاری.

سطوح مختلف گواهینامه‌های الکترونیکی: گواهینامه‌های دیجیتالی در سطوح مختلفی بسته به میزان و سطح اطمینان خواسته شده از طرف متقاضی، توسط دفاتر صدور گواهینامه موجود می‌باشند. در زبان ساده هر چه سطح گواهینامه بالاتر باشد، به میزان بیشتری دارنده آن را تایید می‌کند. یک گواهینامه سطح بالا می‌تواند به این معنی باشد که گواهینامه می‌تواند برای کارهای حساس‌تری مانند بانکداری آنلاین و معرفی هویت یک نفر برای تبادلات مالی و تجارت الکترونیکی، مورد استفاده قرار بگیرد.

سطح گواهینامه ارتباط نزدیکی با نوع گواهینامه دارد. سطوح پایین شامل اطلاعات شخصی کمتری و یا بدون اطلاعات شخصی می‌باشند (به طور مثال فقط یک آدرس ایمیل). گواهینامه‌های متعلق به چنین سطحی می‌توانند برای ارسال ایمیل حفاظت شده بکار بروند، در حالیکه برای اثبات گواهینامه یک موسسه و یا یک سازمان نیاز به اطلاعات بیشتری و در نتیجه سطح بالاتری از گواهینامه است.

۲-۲-۴-۶- امضای دیجیتالی از دید برنامه نویسی

در یک امضای دیجیتالی سه دسته اطلاعات وجود دارد: هویت تولید کننده نرم افزار، هویت منبع تایید کننده (سازمانی که امضاء را صادر کرده) و یک عدد رمز برای تایید این مطلب که محتویات نرم افزار دستکاری نشده است.

اگر می‌خواهید برای وب محتویات فعال بنویسید باید یک گواهینامه کد تعیین اعتبار برای خود دست و پا کنید تا بتوانید برای نرم افزارهای خود امضای دیجیتالی بگیرید. اگر فقط برای اینترنت برنامه می‌نویسید نیازی به این مراحل ندارید چون سطح امنیتی در آنها معمولاً پایین است و نیازی به امضای دیجیتالی وجود ندارد.

اگر صرفاً برای شرکت خود نرم افزار می‌نویسید می‌توانید از گواهینامه آن استفاده کنید. اما توصیه می‌شود خودتان هم این گواهینامه را بگیرید.

با آن که شرکت‌های متعددی برای صدور گواهینامه کد تعیین اعتبار وجود دارند، میکروسافت شرکت Verisign را توصیه می‌کند. برای کسب اطلاعات بیشتر می‌توانید به سایت وب این شرکت که در زیر آمده است مراجعه کنید:

<http://www.verisign.com/developers/index.html>

هزینه دریافت این گواهینامه ۲۰ دلار در سال و مراحل انجام آن بسیار ساده است:

۱- در سایت مزبور، یک فرم پر کنید و در آن اطلاعات خواسته شده (از جمله اطلاعات مربوط به کارت اعتباری) را وارد کنید.

۲- شرکت Verisign کد شناسایی شما را با پست الکترونیک برایتان ارسال خواهد کرد.

۳- به صفحه نصب گواهینامه رفته و کد شناسایی خود را وارد کنید. این کار باید در همان کامپیوتری که توسط آن کد شناسایی را گرفته‌اید، انجام شود.

۴- گواهینامه به کامپیوتر شما فرستاده خواهد شد.

هنگام ثبت گواهینامه دو گزینه در اختیار دارید: ذخیره کردن آن در یک فایل یا در رجیستری ویندوز. توصیه می‌شود گواهینامه خود را در یک فایل و روی دیسک ذخیره کنید تا بتوانید آن را از گزند نامحرمات حفظ کنید. در حقیقت، دو فایل به کامپیوتر شما فرستاده می‌شود: یکی حاوی خود گواهینامه (با پسوند SPC) و دیگری حاوی کلید رمزبندی (با پسوند PVK).

امضای دیجیتالی: امضای دیجیتالی برای ایمیل و فایل‌های اطلاعاتی همان کاری را انجام می‌دهد که امضای شما بر روی یک سند کاغذی انجام می‌دهد. امضای دیجیتالی اصل بودن و صداقت یک پیغام یا سند و یا فایل اطلاعاتی را تضمین می‌کند.

۲-۲-۴-۷- چگونه یک امضای دیجیتالی درست کنیم [47]

کنگره امریکا استفاده از امضاهای دیجیتال را تصویب کرد. این طرح هم اکنون باید در مجلس سنای امریکا تصویب شود. با تصویب این طرح، امضای دیجیتال رسمی می‌شود و می‌توان از آن برای امضای قراردادهای و اسناد مالی درست مانند امضای معمولی استفاده کرد. استفاده از امضای دیجیتال به چه تجهیزاتی نیاز دارد؟

۱- یک دستگاه کامپیوتر

۲- اتصال به اینترنت

۳- نرم افزار مخصوص امضای دیجیتالی

بوجود آوردن یک امضای دیجیتالی مراحل محاسباتی پیچیده‌ای دارد. در حالیکه این مراحل توسط کامپیوتر انجام می‌شود، درست کردن امضای دیجیتالی دیگر حتی از یک امضای دستی هم آسان‌تر است. مراحل زیر نشان دهنده اعمالی است که در حین ساخته شدن یک امضای دیجیتالی صورت می‌گیرد:

(a) آلیس دکمه sing را در نرم افزار ایمیل خود کلیک می‌کند و یا فایلی را که نیاز به امضا دارد انتخاب می‌کند.

(b) کامپیوتر آلیس رمزگذاری را محاسبه می‌کند (پیغام به یک تابع عمومی جهت رمزگذاری برده می‌شود). این تابع توسط کلید خصوصی آلیس رمزگذاری شده است (در این حالت آنرا کلید امضا می‌خوانیم).

(c) پیغام آلیس و امضای دیجیتالی آن برای باب ارسال می‌شود.

(d) باب پیغام امضا شده را دریافت می‌کند. در آنجا مشخص شده است که پیغام امضا شده است و نرم‌افزار ایمیل باب می‌داند که چگونه آن امضا را تایید کند.

(d) کامپیوتر باب امضای دیجیتالی آلیس را توسط کلید عمومی آلیس رمزگشایی می‌کند.

(e) کامپیوتر باب کد رمزگذاری را از امضای دیجیتالی استخراج می‌کند. سپس کامپیوتر باب کد رمزگذاری را که استخراج کرده است با کدی که با پیغام آلیس ارسال شده است مطابقت می‌کند.

(f) اگر پیغام آلیس صحیح انتقال یافته باشد و در طول راه مورد دستبرد واقع نشده باشد هر دو کلید استخراج شده یکسان می‌باشند. اگر دو کد رمزگذاری که استخراج شده‌اند با یکدیگر مطابقت نداشته باشد صلاحیت نامه متفی است.

(g) اگر پیغام اصلی مورد سرقت قرار گرفته باشد کد رمزگذاری که در کامپیوتر باب استخراج می‌شود متفاوت خواهد بود و در این صورت کامپیوتر باب به او اطلاع خواهد داد.

۲-۲-۴-۸- نحوه عملکرد یک امضای دیجیتال [48]

قبل از آشنائی با نحوه عملکرد یک امضای دیجیتال، لازم است در ابتدا با برخی اصطلاحات مرتبط با این موضوع بیشتر آشنا شویم:

• **کلیدها (Keys):** از کلیدها به منظور ایجاد امضاهای دیجیتال استفاده می‌گردد. برای هر امضای دیجیتال، یک کلید عمومی و یک کلید خصوصی وجود دارد: کلید خصوصی، بخشی از کلید است که شما از آن به منظور امضای یک پیام استفاده می‌نمائید. کلید خصوصی یک رمز عبور حفاظت شده بوده و نمی‌بایست آن را در اختیار دیگران قرار داد. کلید عمومی، بخشی از کلید است که امکان استفاده از آن برای سایر افراد وجود دارد. زمانی که کلید فوق برای یک حلقه کلید عمومی (Public key ring) و یا یک شخص خاص ارسال می‌گردد، آنان با استفاده از آن قادر به بررسی امضای شما خواهند بود.

• **حلقه کلید (Key Ring):** شامل کلیدهای عمومی است. یک حلقه کلید از کلیدهای عمومی افرادی که برای شما کلید مربوط به خود را ارسال نموده و یا کلیدهایی که از طریق یک سرویس دهنده کلید عمومی دریافت نموده اید، تشکیل می‌گردد. یک سرویس دهنده کلید عمومی شامل کلید افرادی است که امکان ارسال کلید عمومی در اختیار آنان گذاشته شده است.

• **اثرانگشت:** زمانی که یک کلید تائید می‌گردد، در حقیقت منحصر بفرد بودن مجموعه‌ای از حروف و اعداد که اثر انگشت یک کلید را شامل می‌شوند تائید می‌گردد.

• **گواهینامه‌های کلید:** در زمان انتخاب یک کلید از روی یک حلقه کلید، امکان مشاهده گواهینامه (مجوز) کلید وجود خواهد داشت. در این رابطه می‌توان به اطلاعات متفاوتی نظیر صاحب کلید، تاریخ ایجاد و اعتبار کلید دست یافت.

۲-۲-۴-۹- نحوه ایجاد و استفاده از کلیدها

- تولید یک کلید با استفاده از نرم‌افزارهایی نظیر PGP اقتباس شده از کلمات Pretty Good محرمانگی و امنیت و یا GnuPG اقتباس شده از کلمات GNU محرمانگی و امنیت Guard.
- معرفی کلید تولید شده به سایر همکاران و افرادی که دارای کلید می‌باشند.
- ارسال کلید تولید شده به یک حلقه کلید عمومی تا سایر افراد قادر به بررسی و تأیید امضای شما گردند.
- استفاده از امضای دیجیتال در زمان ارسال نامه‌های الکترونیکی. اکثر برنامه‌های سرویس دهنده پست الکترونیکی دارای پتانسیلی به منظور امضاء یک پیام می‌باشند.

۲-۲-۴-۱۰- حملات ممکن علیه امضاءهای دیجیتالی

- **حمله Key-only:** در این حمله، دشمن تنها کلید عمومی امضاءکننده را می‌داند و بنابراین فقط توانایی بررسی صحت امضاءهای پیام‌هایی را که به وی داده شده‌اند، دارد.
- **حمله Known Signature:** دشمن، کلید عمومی امضاءکننده را می‌داند و جفت‌های پیام / امضاء که به وسیله صاحب امضاء انتخاب و تولید شده است را دیده است. این حمله در عمل امکان‌پذیر است و بنابراین هر روش امضایی باید در مقابل آن امن باشد.
- **حمله Chosen Message:** به دشمن اجازه داده می‌شود که از امضاءکننده بخواهد که تعدادی از پیام‌های به انتخاب او را امضاء کند. انتخاب این پیام‌ها ممکن است به امضاءهای از قبل گرفته شده بستگی داشته باشد. این حمله در غالب حالات، ممکن است غیرعملی به نظر برسد، اما با پیروی از قانون احتیاط، روش امضایی که در برابر آن ایمن است، ترجیح داده می‌شود.
- **حمله Man-in-the-middle:** در این حمله، شخص از موقعیت استفاده کرده در هنگام مبادله کلید عمومی، کلید عمومی خود را جایگزین کرده و برای گیرنده می‌فرستد و بدین گونه می‌تواند به پیام‌ها دسترسی داشته باشد بدون اینکه فرستنده و گیرنده، مطلع باشند. در سیستم‌های کلید عمومی (نامتقارن) اغلب مدیریت کلید مورد حمله قرار می‌گیرد تا الگوریتم رمزنگاری.

۲-۲-۴-۱۱- مرکز صدور گواهینامه چیست [50]

مرکزی برای صدور گواهینامه و تایید هویت سرویس گیرنده و سرویس دهنده می باشد و بدین صورت عمل می کند که پس از درخواست گواهینامه از طرف کاربر، CA به آن دو کلید خصوصی و عمومی می دهد که کلید خصوصی در اختیار

کاربر قرار می گیرد و باید در جای امنی ذخیره شود. CA با استفاده از کلید عمومی و مشخصات کاربر برای آن گواهینامه ای صادر می کند، که این گواهینامه شامل مشخصات کاربر و تاریخ اعتبار آن و امضای صادر کننده گواهینامه می باشد.

مرکز صدور گواهینامه دارای بخش های مختلفی است که به توضیح هر کدام از آن ها می پردازیم.

۱- مرجع صدور گواهینامه ریشه (Root CA): این مرکز باید امنیت بالایی داشته باشد و کسی به کلیدهای خصوصی آن دسترسی پیدا نکند و به این علت وظیفه اعطا گواهینامه را به CA محول می کند.

۲- مرجع صدور گواهینامه (CA): این مرجع وظیفه اعطا گواهینامه را به کاربران بعهدہ دارد و دارای گواهینامه ای از سوی مرجع صدور گواهینامه ریشه برای اطمینان کاربران می باشد.

۳- مرجع ثبت نام (RA): این مرجع وظیفه ثبت درخواست گواهینامه کاربر و اعلام آن به CA و اعطا گواهینامه را از CA به کاربر بعهدہ دارد.

پس از گرفتن کلید خصوصی و عمومی، کاربر امکان رمزنگاری و امضا کردن متن ارسالی را پیدا می کند.

CA ها دارای یک لیستی به نام CRL می باشند که در آن لیست گواهینامه هایی که کلید خصوصی آن ها لو رفته وجود دارد و آن را به صورت پی در پی به اطلاع کاربران می رسانند.

۲-۲-۴-۱۲- رمزنگاری چیست

رمزنگاری عبارت است از به هم ریختگی اطلاعات به طوری که برای کسی قابل فهم نباشد. در رمزنگاری کاربر با استفاده از کلید عمومی گیرنده، اطلاعات را رمز می کند و برای گیرنده اطلاعات ارسال می کند. گیرنده اطلاعات، اطلاعات رمز شده را توسط کلید خصوصی رمزگشایی می کند و چون کلید خصوصی هر شخص فقط در اختیار خودش است تنها همان فرد امکان رمزگشایی اطلاعات را دارد.

رمزنگاری کلید خصوص-عمومی



شکل ۲-۱۴- رمزنگاری خصوصی و عمومی [50]

اهداف CA :

۱- تامین امنیت لازم در انجام معاملات و محیط های الکترونیکی و ترویج فرهنگ استفاده از هویت الکترونیکی است.

۲- تولید و ارائه گواهینامه دیجیتال برای تبادلات تجارت الکترونیکی C2B, B2B (در حوزه کالا و خدمات)

۳- تدوین آیین نامه‌ها و مقررات مربوط به مدیریت بر گواهی دیجیتال تولید و عرضه شده.

۴- ارائه خدمت به دفاتر ثبت گواهی دیجیتال (RA) و دفاتر خدمات گواهی دیجیتال در سراسر کشور.

۵- ارائه خدمات آموزشی برای استفاده از این فناوری در سراسر کشور.

با توجه به توضیحات داده شده و لزوم ایجاد CA در کشور به بررسی یکی از بزرگترین CAهای جهان پرداخته می‌شود.



۲-۲-۴-۱۳-تشخیص هویت از طریق امضای دیجیتالی

یکی از مباحث مهم و اصول در ارتباطات ایمن، تشخیص هویت متقابل از هر دو طرف Client و Server می‌باشد. در یک ارتباط، می‌باشد هویت اصلی سرور برای کاربران و برعکس مشخص شود زیرا در غیر این صورت هر سروری قادر به ایجاد اعتماد در کاربران خواهد بود. هر سرور باید دارای گواهینامه و امضای دیجیتالی باشد که این گواهینامه، نشان دهنده هویت اصلی آن است و توسط شرکت‌هایی مانند Verisign و Thawte ارائه می‌گردد. در این گواهینامه الکترونیکی اطلاعاتی از قبیل: کلید عمومی (برای مخفی سازی اطلاعات)، شماره سریال، نام دامنه، امضای دیجیتالی و تاریخ شروع و انقضای اعتبار گواهینامه درج می‌شود.

۲-۲-۴-۱۴-امضای دیجیتالی زیربنای امنیت تبادلات الکترونیکی

با توجه به توسعه روزافزون فناوری اطلاعات و در پی آن تجارت الکترونیکی و تغییر نمادهای فیزیکی به نمادهای الکترونیکی، ارسال و تبادل اطلاعات محرمانه الکترونیکی به ضرورتی اجتناب‌ناپذیر تبدیل شده است. بنابراین مسائل حقوقی ناشی از تبادل الکترونیکی اطلاعات بایستی با قراردادهای مشخصی تنظیم شود. حوزه این مسائل، استانداردهای تبادل و ایمنی اطلاعات، نحوه اعتبارسنجی و رسمیت بخشیدن به پیام‌ها، نحوه دریافت و ارسال پیام، قوانین حاکم و سرانجام مسئله دلایل اثبات پیام را در بر می‌گیرند. به هر حال در روش ارسال پیام الکترونیکی دریافت‌کننده بایستی

مطمئن شود که فرستنده همان فرد مورد نظر او بوده و از طرفی اطلاعات دریافتی پس از ارسال در بین راه تغییر نکرده باشد. برای حل این مشکل از امضای دیجیتالی در شبکه‌های الکترونیکی استفاده می‌شود. امروزه در اکثر کشورها امضای دیجیتالی به یک ضرورت تبدیل شده و حتی در کارت هوشمند شهروندان خود این رمز را درج می‌کنند از سوی دیگر جامعه بین‌المللی و همچنین انجمن قانونی بلژیک مجموعه قوانینی را ارائه کرده‌اند که باعث می‌شود امضاهای دیجیتالی به صورت قانونی صورت پذیرد و عموماً به صورت امضاهای مکتوب پذیرفته شود.

۲-۲-۴-۱۵- منظور از امضای دیجیتالی چیست

امضای الکترونیکی یا دیجیتالی مانند امضای سنتی نیست بلکه عددی بزرگ است که به صورت رمز و کد در آمده است. این عدد در حقیقت یک عدد انحصاری است و به فرد متقاضی، کد خاصی به عنوان امضای الکترونیک داده می‌شود. بخشی از آن مربوط به پرداخت و دریافت پول از طریق اینترنت می‌شود و در بخش دیگر به قراردادها، مرسولات الکترونیکی محرمانه و یا حتی شناخت طرف مقابل در شبکه مربوط می‌شود. یعنی تشخیص هویت فرد که برای شما چیزی ارسال کرده و یا شما خواهان دادن اطلاعاتی از سوی وی در شبکه اینترنت بوده‌اید. شناسایی هویت چیزی فراتر از تجارت است.

به طور کلی می‌توان گفت: امضای دیجیتالی شماره یا عدد انحصاری محرمانه‌ای است که توسط مرکزی به هر فرد متقاضی تعلق می‌گیرد و آن عدد یا رمز مبنای تعاملات آن فرد در شبکه یا محیط سایبر می‌شود.

۲-۲-۴-۱۶- استفاده از امضای دیجیتالی تا چه حد امنیت تبادل اسناد مالی و محرمانه را تضمین می‌کند

امنیت هیچ وقت صددرصد نمی‌شود، این مقوله هم یک مسئله نسبی است و بستگی دارد چقدر برای آن می‌خواهید هزینه کنید و سندی را که می‌خواهید حفاظت کنید چه ارزشی دارد، با توجه به ارزشی که یک سند دارد برای مصونیت آن سرمایه‌گذاری می‌کنند. به هر حال امضای الکترونیکی بر خلاف امضای دست‌نویس از امنیت بیشتری برای مصون ماندن از جعل، دستکاری و تقلید توسط دیگران برخوردار است چون آگاهی یافتن از یک امضای الکترونیکی محرمانه کار بسیار دشواری است. باید توجه داشت که گسترش تجارت الکترونیکی مستلزم ایجاد اطمینان و اعتماد عمومی نسبت به این نوع از تجارت است و این اطمینان باید از طریق تضمین امنیت تبادل داده‌های الکترونیکی صورت گیرد. هر چند با توسعه فناوری‌های نوین امنیت افزایش می‌یابد ولی همانطور که گفته شد هیچ‌گاه صددرصد نمی‌شود.

آیا در کشور امکانات و فناوری‌های لازم برای صدور امضای دیجیتالی وجود دارد؟ آیا از لحاظ حقوقی در این زمینه با مشکلی مواجه نیستیم؟

- از لحاظ امکانات نرم‌افزاری و سخت‌افزاری برای عملی کردن استفاده از امضای دیجیتالی در کشور سرمایه‌گذاری شده و سازمان‌هایی مشغول پیاده‌سازی این سیستم‌ها هستند. در قانون تجارت الکترونیکی امضای دیجیتالی برای کاربردهای

مشخصی به رسمیت شناخته شده است. البته نیاز به آیین‌نامه‌هایی دارد که به تصویب نرسیده ولی در دست تهیه و تدوین برای تصویب است.

معنی و مفهوم کلید عمومی و خصوصی در امضای الکترونیکی: منظور از کلید بخشی از سیستم یا الگوریتمی است که یک متن را رمزگذاری یا رمزگشایی می‌کند. کلید عمومی پیام را به صورت رمز در می‌آورد که شما می‌تواند کلید عمومی را در اختیار همگان و در معرض استفاده و دید عمومی قرار دهید.

مرکز گواهی برای آنها گواهی‌نامه‌ای صادر می‌کند که صحت انتساب کلید عمومی را به هر شخص دارنده گواهی تایید می‌کند. کلید خصوصی هم کلید شخصی و منحصر به فردی است که محرمانه و در اختیار شخص است و فرد دیگری نمی‌تواند به آن دسترسی یابد.

امضای دیجیتال مبتنی بر روش‌های رمزنگاری از طریق کلیدهای عمومی و خصوصی است. یک متن یا پیام رمزنگاری شده بی‌مفهوم است و فقط کسی می‌تواند به معنی و مفهوم آن پی ببرد که دارای کلید خصوصی باشد.

در حال حاضر در دنیا در کشورهای متعددی از امضای دیجیتال در کاربردهای گوناگون استفاده می‌شود از صدور یک ایمیل گرفته تا نقل و انتقالات مالی و امضای اسناد تعهدآور. بنابراین حوزه کاربرد آن گسترده است. تاکنون مقتضیات قانونی آن در بیشتر نظام‌های حقوقی فراهم آمده است. این موضوع تا حدی است که در برخی از کشورها مثل آلمان قانون مستقلی تحت عنوان قانون امضای الکترونیکی به تصویب رسیده است.

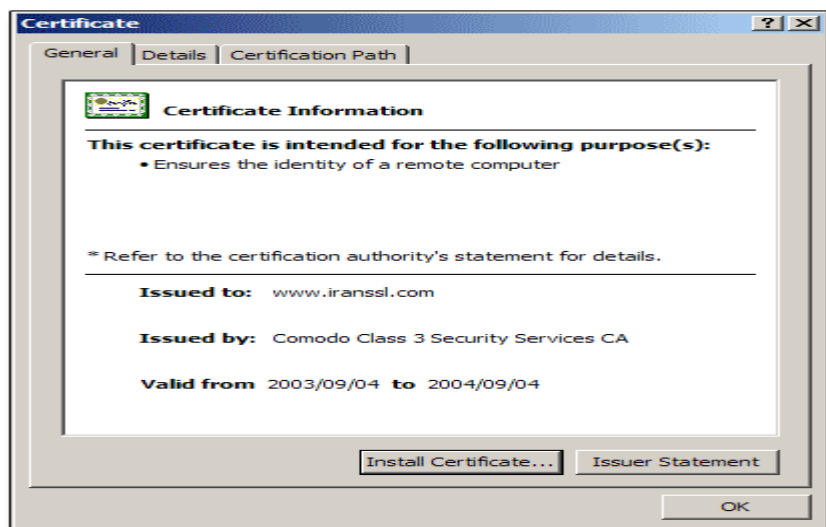
SSL پروتکلی است که توسط شرکت Netscape و برای رد و بدل کردن سند های خصوصی از طریق اینترنت توسعه یافته است. یک کلید خصوصی برای به رمز در آوردن اطلاعاتی که بر روی یک ارتباط منتقل می‌شوند استفاده می‌نماید. هر دو مرورگر Internet Explorer و Netscape Navigator {امروزه تمام مرورگر های مدرن} این پروتکل پشتیبانی می‌نمایند. همچنین بسیاری از وب سایت‌ها برای فراهم کردن بستری مناسب جهت حفظ کردن اطلاعات محرمانه کاربران (مانند شماره کارت اعتباری) از این پروتکل استفاده می‌نمایند. طبق آنچه در استاندارد آمده است، URLهایی که نیاز به یک ارتباط از نوع SSL دارند با https: به جای http: شروع می‌شوند.

پروتکل دیگری که برای انتقال اطلاعات به صورت امن بر روی شبکه جهانی وب وجود دارد، پروتکلی است به نام Secure HTTP یا S-HTTP، در حالیکه SSL یک ارتباط امن میان Client و Server ایجاد می‌کند تا هر اطلاعاتی که بر روی آن منتقل می‌شود امن باشد، S-HTTP برای این طراحی شده است تا طبق آن پیام‌های منفرد به طور امن منتقل شوند. بنابراین این دو تکنولوژی قبل از آنکه دو تکنولوژی رقیب باشند، دو تکنولوژی مکمل هستند. هر دو این پروتکل ها به عنوان استاندارد از سوی IETF پذیرفته شده‌اند.

توجه داشته باشید که SSL یک پروتکل مستقل از لایه برنامه است (Application Independent)، بنابراین پروتکل‌هایی مانند HTTP، FTP و Telnet قابلیت استفاده از آن را دارند. با این وجود SSL بروی پروتکل‌های HTTP، FTP و IPsec بهینه شده است.

پروتکل (SSL (Socket Secure Layer)، یک استاندارد وب برای کد کردن اطلاعات بین کاربر و وب سایت است. اطلاعاتی که توسط یک اتصال SSL مبادله می‌شوند بصورت کد شده ارسال می‌شوند و بدین ترتیب اطلاعات مبادله شده از دزدیده شدن یا استراق سمع محافظت می‌شوند. SSL برای شرکتها و مشتریان این امکان را فراهم می‌کند که بتوانند با اطمینان اطلاعات خصوصی شان را مانند شماره کارت اعتباری، به یک وب سایت بطور محرمانه ارسال کنند. برای برقراری یک اتصال SSL به Web Server Certificate ها نیاز می‌باشد. در تعریفی دیگر SSL اینگونه بیان شده، Secure Socket Layer یا همان SSL یک تکنولوژی استاندارد و به ثبت رسیده برای تامین ارتباطی امن مابین یک وب سرور و یک مرورگر اینترنت است. این ارتباط امن از تمامی اطلاعاتی که ما بین وب سرور و مرورگر اینترنت (کاربر) انتقال می‌یابد، محافظت می‌کند تا در این انتقال به صورت محرمانه و دست نخورده باقی بماند SSL. یک استاندارد صنعتی است و توسط میلیون‌ها وب سایت در سراسر جهان برای برقراری امنیت انتقال اطلاعات استفاده می‌شود. برای اینکه یک وب سایت بتواند ارتباطی امن از نوع SSL را داشته باشد نیاز به یک گواهینامه SSL دارد. زمانی که شما می‌خواهید SSL را بر روی سرور خود فعال کنید سؤالات متعددی در مورد هویت سایت شما (مانند آدرس سایت) و همین طور هویت شرکت شما (مانند نام شرکت و محل آن) از شما پرسیده می‌شود. آنگاه سرور دو کلید رمز را برای شما تولید می‌کند، یک کلید خصوصی (Private Key) و یک کلید عمومی.

(Public Key) کلید خصوصی به این خاطر، این نام را گرفته است چون بایستی کاملاً محرمانه و دور از دسترس دیگران قرارگیرد. اما در مقابل نیازی به حفاظت از کلید عمومی نیست و این کلید در قالب یک فایل درخواست گواهینامه یا Certificate Signing Request که به اختصار آنرا CSR می‌نامیم قرار داده می‌شود که حاوی مشخصات سرور و شرکت شما بصورت رمز است. آنگاه شما بایستی که این کد CSR را برای صادرکننده گواهینامه ارسال کنید. در طول مراحل سفارش یک SSL مرکز صدور گواهینامه درستی اطلاعات وارد شده توسط شما را بررسی و تایید می‌کند و سپس یک گواهینامه SSL برای شما تولید کرده و ارسال می‌کند. وب سرور شما گواهینامه SSL صادر شده را با کلید خصوصیتان در سرور و به دور از دسترس سایرین مطابقت می‌دهد. سرور شما آنگاه امکان برقراری ارتباط امن را با کاربران خود در هر نقطه دارد. نمایش قفل امنیت SSL پیچیدگیهای یک پروتکل SSL برای کاربران شما پوشیده است لیکن مرورگر اینترنت آنها در صورت برقراری ارتباط امن، وجود این ارتباط را توسط نمایش یک قفل کوچک در پایین صفحه متذکر می‌شود و در هنگامی که شما روی قفل کوچک زرد رنگی که در پایین صفحه IE نمایش داده می‌شود دوبار کلیک می‌کنید باعث نمایش گواهینامه شما به همراه سایر جزئیات می‌شود. گواهینامه‌های SSL تنها برای شرکتها و اشخاص حقیقی معتبر صادر می‌شوند. به طور مثال یک گواهینامه SSL شامل اطلاعاتی در مورد دامین، شرکت، آدرس، شهر، استان، کشور و تاریخ ابطال گواهینامه و همینطور اطلاعاتی در مورد مرکز صدور گواهینامه که مسؤول صدور گواهینامه می‌باشد.



شکل ۲-۱۶ SSL [50]

۲-۲-۴-۱-۱۷-InstantSSL چیست

InstantSSL یک Web Server Certificate است که اجازه می‌دهد مشتریان و وب سایت‌ها بتوانند یک تجارت الکترونیک (e-commerce) ایمن با اتصال کدگذاری شده SSL برقرار کنند. InstantSSL Web Server Certificate ها با ۹۸٪ مرورگرها سازگار هستند.

۲-۲-۴-۱۷-۲-تکنولوژی پیشرفته تائید کردن (Authentication)

با فعال کردن آیکون "LOCK" مرورگرتان، QuickSSL به کاربران آنلاین اطمینان می‌دهد که شماره کارت اعتباری و بقیه اطلاعات محرمانه نمی‌توانند دیده شوند، دزدیده شوند یا تغییر یابند. به علت اینکه سیستم authentication خودکار ما از پیشرفته‌ترین‌ها در صنعت می‌باشد، مشتریان و شرکای تجاری شما می‌توانند مطمئن باشند که QuickSSL Web Server Certificate ها فقط برای گیرندگانی که کاملاً تائید شده هستند، صادر می‌گردد.

۲-۲-۴-۱۷-۳-دسترسی آنلاین به پروفایل تان در ابر

بعنوان بخشی از مرحله تدارکاتی با QuickSSL، تجارت شما با ChoicePoint ثبت خواهد شد و یک (ChoicePoint Unique Identifier (CUI اختصاص داده خواهد شد که معادل عدد DUNS می‌باشد. CUI یک پروفایل شرکتی برای کاربر اینترنتی شما از طریق اطلاعات موجود در certificate تان، فراهم می‌کند. اطلاعات پروفایل تان در ابر، شامل اطلاعات اولیه گزارش شده از CSR تان از قبیل نام دومین، نام شرکت، بخش، کشور، استان و شهر می‌باشد. ChoicePoint اجازه می‌دهد اشخاص

معتمد بتوانند اطلاعات بیشتری در مورد شرکت شما را مشاهده کنند و خریداری نمایند. با دسترسی به اطلاعات شرکتی شما، مشتریان تان به برقراری یک تجارت آنلاین اطمینان پیدا خواهند کرد.

۲-۲-۴-۱۸- مفاهیم رمز گذاری

۲-۲-۴-۱۸-۱- معرفی و اصطلاحات

رمزنگاری علم کدها و رمزهاست. یک هنر قدیمی است و برای قرن ها به منظور محافظت از پیغام‌هایی که بین فرماندهان، جاسوسان، عشاق و دیگران ردوبدل می‌شده، استفاده شده است تا پیغام‌های آنها محرمانه بماند. هنگامی که با امنیت دیتا سروکار داریم، نیاز به اثبات هویت فرستنده و گیرنده پیغام داریم و در ضمن باید از عدم تغییر محتوای پیغام مطمئن شویم. این سه موضوع یعنی محرمانگی، تصدیق هویت و جامعیت در قلب امنیت ارتباطات دیتای مدرن قرار دارند و می‌توانند از رمزنگاری استفاده کنند.

اغلب این مساله باید تضمین شود که یک پیغام فقط می‌تواند توسط کسانی خوانده شود که پیغام برای آنها ارسال شده است و دیگران این اجازه را ندارند. روشی که تامین کننده این مساله باشد "رمزنگاری" نام دارد. رمزنگاری هنر نوشتن بصورت رمز است بطوریکه هیچکس به غیر از دریافت کننده موردنظر نتواند محتوای پیغام را بخواند.

رمزنگاری مخفف‌ها و اصطلاحات مخصوص به خود را دارد. برای درک عمیق‌تر به مقداری از دانش ریاضیات نیاز است. برای محافظت از دیتای اصلی (که بعنوان Plaintext شناخته می‌شود)، آنرا با استفاده از یک کلید (رشته‌ای محدود از بیت‌ها) بصورت رمز در می‌آوریم تا کسی که دیتای حاصله را می‌خواند قادر به درک آن نباشد. دیتای رمز شده (که بعنوان Ciphertext شناخته می‌شود) بصورت یک سری بی‌معنی از بیت‌ها بدون داشتن رابطه مشخصی با دیتای اصلی به نظر می‌رسد. برای حصول متن اولیه دریافت‌کننده آنرا رمزگشایی می‌کند. یک شخص ثالث (مثلاً یک هکر) می‌تواند برای اینکه بدون دانستن کلید به دیتای اصلی دست یابد، کشف رمز نوشته (Cryptanalysis) کند. بخاطر داشتن وجود این شخص ثالث بسیار مهم است.

رمزنگاری دو جزء اصلی دارد، یک الگوریتم و یک کلید. الگوریتم یک مبدل یا فرمول ریاضی است. تعداد کمی الگوریتم قدرتمند وجود دارد که بیشتر آنها بعنوان استانداردها یا مقالات ریاضی منتشر شده‌اند. کلید، یک رشته از ارقام دودویی (صفر و یک) است که بخودی‌خود بی‌معنی است. رمزنگاری مدرن فرض می‌کند که الگوریتم شناخته شده است یا می‌تواند کشف شود. کلید است که باید مخفی نگاه داشته شود و کلید است که در هر مرحله پیاده‌سازی تغییر می‌کند. رمزگشایی ممکن است از همان جفت الگوریتم و کلید یا جفت متفاوتی استفاده کند.

دیتای اولیه اغلب قبل از رمزشدن بازچینی می‌شود؛ این عمل عموماً بعنوان Scrambling شناخته می‌شود. بصورت مشخص‌تر، Hashfunction ها بلوکی از دیتا را (که می‌تواند هر اندازه‌ای داشته باشد) به طول از پیش مشخص شده کاهش

می‌دهد. البته دیتای اولیه نمی‌تواند از Hashed value بازسازی شود. Hash function ها اغلب بعنوان بخشی از یک سیستم تایید هویت مورد نیاز هستند؛ خلاصه‌ای از پیام (شامل مهم‌ترین قسمت‌ها مانند شماره پیام، تاریخ و ساعت، و نواحی مهم دیتا) قبل از رمزنگاری خود پیام، ساخته و Hash می‌شود.

یک چک تایید پیام (Message Authentication Check) یا MAC یک الگوریتم ثابت با تولید یک امضاء بر روی پیام با استفاده از یک کلید متقارن است. هدف آن نشان دادن این مطلب است که پیام بین ارسال و دریافت تغییر نکرده است. هنگامی که رمزنگاری توسط کلید عمومی برای تایید هویت فرستنده پیام استفاده می‌شود، منجر به ایجاد امضای دیجیتال (digital signature) می‌شود.

۲-۲-۴-۱۸-۲- الگوریتم‌ها

طراحی الگوریتم‌های رمزنگاری مقوله‌ای برای متخصصان ریاضی است. طراحان سیستم‌هایی که در آنها از رمزنگاری استفاده می‌شود، باید از نقاط قوت و ضعف الگوریتم‌های موجود مطلع باشند و برای تعیین الگوریتم مناسب قدرت تصمیم‌گیری داشته باشند. اگرچه رمزنگاری از اولین کارهای شانون (Shannon) در اواخر دهه ۴۰ و اوایل دهه ۵۰ بشدت پیشرفت کرده است، اما کشف رمز نیز پایه‌های رمزنگاری به پیش آمده است و الگوریتم‌های کمی هنوز با گذشت زمان ارزش خود را حفظ کرده‌اند. بنابراین تعداد الگوریتم‌های استفاده شده در سیستم‌های کامپیوتری عملی و در سیستم‌های برپایه کارت هوشمند بسیار کم است.

۲-۲-۴-۱۸-۳- رمزنگاری کلید عمومی

در روش فوق از ترکیب یک کلید خصوصی و یک کلید عمومی استفاده می‌شود. کلید خصوصی صرفاً "متعلق به کامپیوتر فرستنده بوده و کلید عمومی توسط کامپیوتر فرستنده در اختیار هر یک از کامپیوترهایی که قصد برقراری ارتباط با یکدیگر را دارند، گذاشته می‌شود. برای رمزگشایی یک پیام رمز شده، کامپیوتر می‌بایست از کلید عمومی که توسط فرستنده ارائه شده، به همراه کلید خصوصی خود استفاده نماید.

یکی از متداول‌ترین برنامه‌های رمزنگاری در این رابطه Pretty Good (PGP) محرمانگی و امنیت است. با استفاده از PGP می‌توان هر چیز دلخواه را رمز نمود.

بمنظور پیاده‌سازی رمزنگاری کلید عمومی در مقیاس بالا نظیر یک سرویس دهنده وب، لازم است از رویکردهای دیگری در این خصوص استفاده گردد. "امضای دیجیتال" یکی از رویکردهای موجود در این زمینه است یک امضای دیجیتالی صرفاً شامل اطلاعات محدودی بوده که اعلام می‌نماید، سرویس دهنده وب با استفاده و بکارگیری یک سرویس مستقل با نام "امضای مجاز"، اطلاعات است. "امضای مجاز" بعنوان یک میانجی بین دو کامپیوتر ایفای وظیفه می‌نماید. هویت و مجاز

بودن هر یک از کامپیوترها برای برقراری ارتباط توسط سرویس‌دهنده انجام و برای هر یک کلید عمومی مربوطه را فراهم خواهد کرد.

یکی از متداولترین نمونه‌های پیاده‌سازی شده از رمزنگاری کلید عمومی، روش Secure Sockets Layer (SSL) است. روش فوق در ابتدا توسط "نت اسکپ" پیاده‌سازی گردید. SSL یک پروتکل امنیتی اینترنت بوده که توسط مرورگرها و سرویس‌دهندگان وب بمنظور ارسال اطلاعات حساس، استفاده می‌گردد.

SSL اخیراً بعنوان بخشی از پروتکل Transport Layer Security (TLS) در نظر گرفته شده است.

در مرورگر می‌توان زمان استفاده از یک پروتکل ایمن نظیر TLS را با استفاده از روش‌های متعدد اعلام کرد. استفاده از پروتکل "https" در عوض پروتکل "http" یکی از روش‌های موجود است. در چنین مواردی در بخش وضعیت پنجره مرورگر یک "Padlock" نشان داده خواهد شد.

رمزنگاری کلید عمومی، مدت زمان زیادی را صرف انجام محاسبات می‌نماید. بنابراین در اکثر سیستم‌ها از ترکیب کلید عمومی و متقارن استفاده می‌گردد. زمانی که دو کامپیوتر یک ارتباط ایمن را بایکدیگر برقرار می‌نمایند، یکی از کامپیوترها یک کلید متقارن را ایجاد و آن را برای کامپیوتر دیگر با استفاده از رمزنگاری کلید عمومی، ارسال خواهد کرد. در ادامه دو کامپیوتر قادر به برقرار ارتباط بکمک رمزنگاری کلید متقارن می‌باشند. پس از اتمام ارتباط، هر یک از کامپیوترها کلید متقارن استفاده شده را دور انداخته و در صورت نیاز به برقراری یک ارتباط مجدد، می‌بایست مجدداً فرآیند فوق تکرار گردد (ایجاد یک کلید متقارن و).

۲-۲-۴-۱۸-۴-مقدار Hash [46]

رمزنگاری مبتنی بر کلید عمومی بر پایه یک مقدار hash، استوار است. مقدار فوق، بر اساس یک مقدار ورودی که در اختیار الگوریتم hashing گذاشته می‌گردد، ایجاد می‌گردد. در حقیقت مقدار hash، فرم خلاصه شده‌ای از مقدار اولیه‌ای خود است. بدون آگاهی از الگوریتم استفاده شده تشخیص عدد ورودی اولیه بعید به نظر می‌رسد.

مثال زیر نمونه‌ای در این زمینه را نشان می‌دهد:

عدد ورودی الگوریتم Hash مقدار

10,667 Input # x 143 1,525,381

تشخیص اینکه عدد ۱,۵۲۵,۳۸۱ (مقدار hash) از ضرب دو عدد ۱۰,۶۶۷ و ۱۴۳ بدست آمده است، کار بسیار مشکلی است. در صورتیکه بدانیم که یکی از اعداد ۱۴۳ است، تشخیص عدد دوم کار بسیار ساده‌ای خواهد بود. (عدد ۱۰,۶۶۷) رمزنگاری مبتنی بر کلید عمومی به مراتب پیچیده‌تر از مثال فوق می‌باشند. مثال فوق صرفاً ایده اولیه در این خصوص را نشان می‌دهد.

کلیدهای عمومی عموماً از الگوریتم‌های پیچیده و مقادیر Hash بسیار بزرگ برای رمزنگاری استفاده می‌نمایند. در چنین مواردی اغلب از اعداد ۴۰ و یا حتی ۱۲۸ بیتی استفاده می‌شود. یک عدد ۱۲۸ بیتی دارای ۱۲۸۲ حالت متفاوت است.

۲-۲-۴-۱۸-۵- آیا شما معتبر هستید

همانگونه که در ابتدای بخش فوق اشاره گردید، رمزنگاری فرآیندی است که بر اساس آن اطلاعات ارسالی از یک کامپیوتر برای کامپیوتر دیگر، در ابتدا رمز و سپس ارسال خواهند شد. کامپیوتر دوم (گیرنده)، پس از دریافت اطلاعات می‌بایست، اقدام به رمزگشایی آنان نماید. یکی دیگر از فرآیندهای موجود بمنظور تشخیص ارسال اطلاعات توسط یک منبع ایمن و مطمئن، استفاده از روش معروف "اعتبار سنجی" است. در صورتیکه اطلاعات "معتبر" باشند، شما نسبت به هویت ایجاد کننده اطلاعات آگاهی داشته و این اطمینان را بدست خواهید آورد که اطلاعات از زمان ایجاد تا زمان دریافت توسط شما تغییر پیدا نکرده‌اند. با ترکیب فرآیندهای رمزنگاری و اعتبار سنجی می‌توان یک محیط ایمن را ایجاد کرد.

به منظور بررسی اعتبار یک شخص و یا اطلاعات موجود بر روی یک کامپیوتر از روش‌های متعددی استفاده می‌شود:

- **رمز عبور:** استفاده از نام و رمز عبور برای کاربران، متداولترین روش "اعتبار سنجی" است. کاربران نام و رمز عبور خود را در زمان مورد نظر وارد و در ادامه اطلاعات وارد شده فوق، بررسی می‌گردند. در صورتیکه نام و یا رمز عبور نادرست باشند، امکان دستیابی به منابع تعریف شده بر روی سیستم به کاربر داده نخواهد شد.

- **کارت‌های عبور:** این نوع کارت‌ها دارای مدل‌های متفاوتی می‌باشند. کارت‌های دارای لایه مغناطیسی (مشابه کارت‌های اعتباری) و کارت‌های هوشمند (دارای یک تراشه کامپیوتر است) نمونه‌هایی از کارت‌های عبور می‌باشند.

- **امضای دیجیتالی:** امضای دیجیتالی، روشی بمنظور اطمینان از معتبر بودن یک سند الکترونیکی (نظیر: نامه الکترونیکی، فایل‌های متنی و ...) است. استاندارد امضای دیجیتالی (DSS)، بر اساس نوع خاصی از رمزنگاری کلید عمومی و استفاده از الگوریتم امضای دیجیتالی (DSA) ایجاد می‌گردد. الگوریتم فوق شامل یک کلید عمومی (شناخته شده توسط صاحب اولیه سند الکترونیکی - امضاء کننده) و یک کلید عمومی است. کلید عمومی دارای چهار بخش است. در صورتیکه هر چیزی پس از درج امضای دیجیتالی به یک سند الکترونیکی، تغییر یابد، مقادیر مورد نظری که بر اساس آنها امضای دیجیتالی با آن مقایسه خواهد شد، نیز تغییر خواهند کرد.

سیستم‌های متعددی برای "اعتبار سنجی" تاکنون طراحی و عرضه شده است. اکثر سیستم‌های فوق از زیست سنجی برای تعیین اعتبار استفاده می‌نمایند. در علم زیست سنجی از اطلاعات زیست شناسی برای تشخیص هویت افراد استفاده می‌گردد. برخی از روش‌های اعتبارسنجی مبتنی بر زیست‌شناسی کاربران، به شرح زیر می‌باشند:

پیمایش اثر انگشت (انگشت نگاری)

پیمایش شبکیه چشم

پیمایش صورت

مشخصه صدا

یکی دیگر از مسائل مرتبط با انتقال اطلاعات، صحت ارسال اطلاعات از زمان ارسال و یا رمزنگاری است. می‌بایست این اطمینان بوجود آید که اطلاعات دریافت شده، همان اطلاعات ارسالی اولیه بوده و در زمان انتقال با مشکل و خرابی مواجه نشده‌اند. در این راستا از روش‌های متعددی استفاده می‌گردد.

● **Checksum:** یکی از قدیمی‌ترین روش‌های استفاده شده برای اطمینان از صحت ارسال اطلاعات است. Checksum، به دو صورت متفاوت محاسبه می‌گردد. فرض کنید Checksum یک بسته اطلاعاتی دارای طولی به اندازه یک بایت باشد، یک بایت شامل هشت بیت و هر بیت یکی از دو حالت ممکن (صفر و یا یک) را می‌تواند داشته باشد. در چنین حالتی ۲۵۶ وضعیت متفاوت می‌تواند وجود داشته باشد. با توجه به اینکه در اولین وضعیت، تمام هشت بیت مقدار صفر را دارا خواهند بود، می‌تواند حداکثر ۲۵۵ حالت متفاوت را ارائه نمود.

▪ در صورتیکه مجموع سایر بایت‌های موجود در بسته اطلاعاتی، ۲۵۵ و یا کمتر باشد، مقدار Checksum شامل اطلاعات واقعی و مورد نظر خواهد بود.

▪ در صورتیکه مجموع سایر بایت‌های موجود در بسته اطلاعاتی، بیش از ۲۵۵ باشد، Checksum معادل باقیمانده مجموع اعداد بوده مشروط بر اینکه آن را بر ۲۵۶ تقسیم نمائیم.

مثال زیر، عملکرد Checksum را نشان می‌دهد.

Byte 1 Byte 2 Byte 3 Byte 4 Byte 5 Byte 6 Byte 7 Byte 8 Total Checksum

۱۲۷ ۱،۱۵۱ ۸۰ ۱۷۹ ۱۵ ۲۴۴ ۱۳۵ ۵۴ ۲۳۲ ۲۱۲

$4,496 = 256 / 1,151 \text{ round to } 4$

$4 \times 256 = 1,024$

$127 = 1,024 - 1,151$

● **CRC (Cyclic Redundancy Check):** روش CRC در مفهوم مشابه روش Checksum است. روش فوق از تقسیم چند جمله‌ای برای مشخص کردن مقدار CRC استفاده می‌کند. طول CRC معمولاً ۱۶ و یا ۳۲ بیت است. صحت عملکرد روش فوق بسیار بالا است. در صورتیکه صرفاً یک بیت نادرست باشد، CRC با مقدار مورد نظر مطابقت نخواهد کرد. روش‌های Checksum و CRC امکانات مناسبی برای پیشگیری از بروز خطای تصادفی در ارسال اطلاعات می‌باشند، روش‌های فوق در رابطه با حفاظت اطلاعات و ایمن‌سازی اطلاعات در مقابل عملیات غیر مجاز بمنظور دستیابی و استفاده از اطلاعات، امکانات محدودتری را ارائه می‌نمایند. رمزنگاری متقارن و کلید عمومی، امکانات به مراتب مناسب تری در این زمینه می‌باشند.

به منظور ارسال و دریافت اطلاعات بر روی اینترنت و سایر شبکه‌های اختصاصی، از روش‌های متعدد ایمنی استفاده می‌گردد. ارسال اطلاعات از طریق شبکه نسبت به سایر امکانات موجود نظیر: تلفن، پست ایمن تر می‌باشد. برای تحقق امر فوق می‌بایست از روش‌های متعدد رمزنگاری و پروتکل‌های ایمنی بمنظور ارسال و دریافت اطلاعات در شبکه‌های کامپیوتری خصوصاً "اینترنت استفاده کرد.

۲-۲-۴-۱۸-۶-سیستم های کلید متقارن

یک الگوریتم متقارن از یک کلید برای رمزنگاری و رمزگشایی استفاده می‌کند. بیشترین شکل استفاده از رمزنگاری که در کارت‌های هوشمند و البته در بیشتر سیستم‌های امنیت اطلاعات وجود دارد data encryption algorithm یا DEA است که بیشتر بعنوان DES شناخته می‌شود. DES یک محصول دولت ایالات متحده است که امروزه بطور وسیعی بعنوان یک استاندارد بین‌المللی شناخته می‌شود. بلوک‌های ۶۴ بیتی دیتا توسط یک کلید تنها که معمولاً ۵۶ بیت طول دارد، رمزنگاری و رمزگشایی می‌شوند. DES از نظر محاسباتی ساده است و به راحتی می‌تواند توسط پردازنده‌های کند (بخصوص آنهایی که در کارتهای هوشمند وجود دارند) انجام گیرد.

این روش بستگی به مخفی بودن کلید دارد. بنابراین برای استفاده در دو موقعیت مناسب است: هنگامی که کلیدها می‌توانند به یک روش قابل اعتماد و امن توزیع و ذخیره شوند یا جایی که کلید بین دو سیستم مبادله می‌شوند که قبلاً هویت یکدیگر را تایید کرده‌اند عمر کلیدها بیشتر از مدت تراکنش طول نمی‌کشد. رمزنگاری DES عموماً برای حفاظت دیتا از شنود در طول انتقال استفاده می‌شود.

کلیدهای DES ۴۰ بیتی امروزه در عرض چندین ساعت توسط کامپیوترهای معمولی شکسته می‌شوند و بنابراین نباید برای محافظت از اطلاعات مهم و با مدت طولانی اعتبار استفاده شود. کلید ۵۶ بیتی عموماً توسط سخت‌افزار یا شبکه‌های بخصوصی شکسته می‌شوند. رمزنگاری DES سه‌تایی عبارتست از کد کردن دیتای اصلی با استفاده از الگوریتم DES که در سه مرتبه انجام می‌گیرد (دو مرتبه با استفاده از یک کلید به سمت جلو (رمزنگاری) و یک مرتبه به سمت عقب (رمزگشایی) با یک کلید دیگر).

این عمل تاثیر دو برابر کردن طول مؤثر کلید را دارد، بعدا خواهیم دید که این یک عامل مهم در قدرت رمزکنندگی است. الگوریتم‌های استاندارد جدیدتر مختلفی پیشنهاد شده‌اند. الگوریتم‌هایی مانند Blowfish و IDEA برای زمانی مورد استفاده قرار گرفته‌اند اما هیچکدام پیاده‌سازی سخت‌افزاری نشدند، بنابراین بعنوان رقیبی برای DES برای استفاده در کاربردهای میکروکنترلی مطرح نبوده‌اند. پروژه استاندارد رمزنگاری پیشرفته دولتی ایالات متحده (AES) الگوریتم Rijndael را برای جایگزینی DES بعنوان الگوریتم رمزنگاری اولیه انتخاب کرده است. الگوریتم Twofish مشخصا برای پیاده‌سازی در پردازنده‌های توان پایین مثلا در کارت‌های هوشمند طراحی شد.

در سال ۱۹۹۸ وزارت دفاع ایالات متحده تصمیم گرفت که الگوریتم‌ها Skipjack و مبادله کلید را که در کارت‌های Fortezza استفاده شده بود، از محرمانگی خارج سازد. یکی از دلایل این امر تشویق برای پیاده‌سازی بیشتر کارت‌های هوشمند برپایه این الگوریتم‌ها بود.

برای رمزنگاری جریانی (streaming encryption) (که رمزنگاری دیتا در حین ارسال صورت می‌گیرد بجای اینکه دیتای کد شده در یک فایل مجزا قرار گیرد) الگوریتم RC4 سرعت بالا و دامنه‌ای از طول کلیدها از ۴۰ تا ۲۵۶ بیت فراهم می‌کند. RC4 که متعلق به امنیت دیتای RSA است، بصورت عادی برای رمزنگاری ارتباطات دوطرفه امن در اینترنت استفاده می‌شود.

۲-۲-۴-۱۸-۷-سیستمهای کلید نامتقارن

سیستم‌های کلید نامتقارن از کلید مختلفی برای رمزنگاری و رمزگشایی استفاده می‌کنند. بسیاری از سیستم‌ها اجازه می‌دهند که یک جزء (کلید عمومی یا public key) منتشر شود در حالیکه دیگری (کلید اختصاصی یا private key) توسط صاحبش حفظ شود. فرستنده پیام، متن را با کلید عمومی گیرنده کد می‌کند و گیرنده آن را با کلید اختصاصی خودش رمزنگاری می‌کند. بعبارتی تنها با کلید اختصاصی گیرنده می‌توان متن کد شده را به متن اولیه صحیح تبدیل کرد. یعنی حتی فرستنده نیز اگرچه از محتوای اصلی پیام مطلع است اما نمی‌تواند از متن کد شده به متن اصلی دست یابد، بنابراین پیام کد شده برای هرگیرنده‌ای بجز گیرنده مورد نظر فرستنده بی‌معنی خواهد بود. معمول ترین سیستم نامتقارن بعنوان RSA شناخته می‌شود (حروف اول پدیدآورندگان آن یعنی Rivest، Shamir و Adleman است). اگرچه چندین طرح دیگر وجود دارند. می‌توان از یک سیستم نامتقارن برای نشان دادن اینکه فرستنده پیام همان شخصی است که ادعا می‌کند استفاده کرد که این عمل اصطلاحا امضاء نام دارد. RSA شامل دو تبدیل است که هرکدام احتیاج به بتوان‌رسانی ماجولار با توان‌های خیلی طولانی دارد:

امضاء، متن اصلی را با استفاده از کلید اختصاصی رمز می‌کند؛ رمزگشایی عملیات مشابه‌ای روی متن رمز شده اما با استفاده از کلید عمومی است. برای تایید امضاء بررسی می‌کنیم که آیا این نتیجه با دیتای اولیه یکسان است؛ اگر اینگونه است، امضاء توسط کلید اختصاصی متناظر رمز شده است.

به بیان ساده‌تر چنانچه متنی از شخصی برای دیگران منتشر شود، این متن شامل متن اصلی و همان متن اما رمز شده توسط کلید اختصاصی همان شخص است. حال اگر متن رمز شده توسط کلید عمومی آن شخص که شما از آن مطلعید رمزگشایی شود، مطابقت متن حاصل و متن اصلی نشان‌دهنده صحت فرد فرستنده آن است، به این ترتیب امضای فرد تصدیق می‌شود. افرادی که از کلید اختصاصی این فرد اطلاع ندارند قادر به ایجاد متن رمز شده نیستند بطوریکه با رمزگشایی توسط کلید عمومی این فرد به متن اولیه تبدیل شود.

اساس سیستم RSA این فرمول است: $X = Yk \bmod r$

که X متن کد شده، Y متن اصلی، k کلید اختصاصی و r حاصلضرب دو عدد اولیه بزرگ است که با دقت انتخاب شده‌اند. برای اطلاع از جزئیات بیشتر می‌توان به مراجعی که در این زمینه وجود دارد رجوع کرد. این شکل محاسبات روی پردازنده‌های بایتی بخصوص روی ۸ بیتی‌ها که در کارت‌های هوشمند استفاده می‌شود بسیار کند است. بنابراین، اگرچه RSA هم تصدیق هویت و هم رمزنگاری را ممکن می‌سازد، در اصل برای تایید هویت منبع پیام از این الگوریتم در کارت‌های هوشمند استفاده می‌شود و برای نشان دادن عدم تغییر پیام در طول ارسال و رمزنگاری کلیدهای آتی استفاده می‌شود.

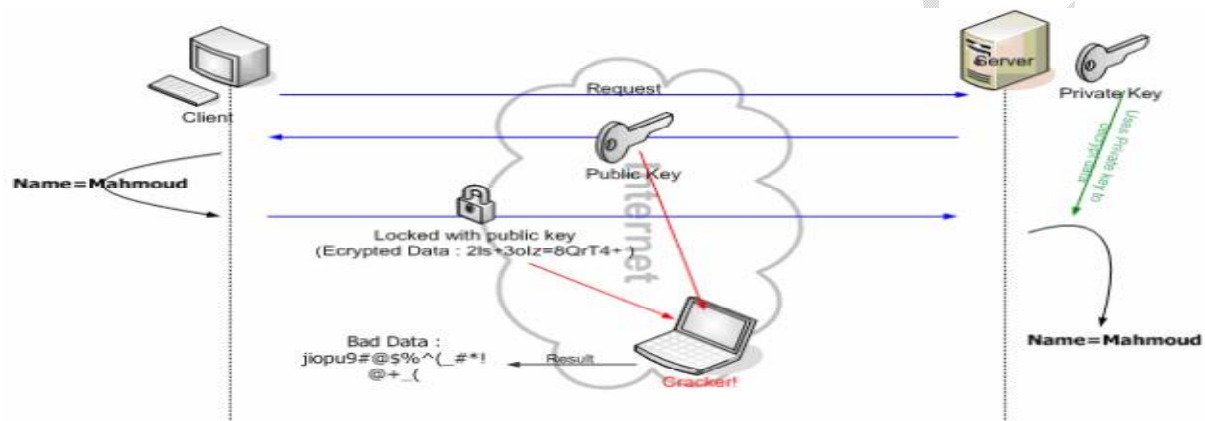
سایر سیستم‌های کلید نامتقارن شامل سیستم‌های لگاریتم گسسته می‌شوند مانند Diffie-Hellman، ElGamal و سایر طرح‌های چندجمله‌ای و منحنی‌های بیضوی. بسیاری از این طرح‌ها عملکردهای یک طرفه‌ای دارند که اجازه تایید هویت را می‌دهند اما رمزنگاری ندارند. یک رقیب جدیدتر الگوریتم RPK است که از یک تولیدکننده مرکب برای تنظیم ترکیبی از کلیدها با مشخصات مورد نیاز استفاده می‌کند. RPK یک پروسه دو مرحله‌ای است: بعد از فاز آماده‌سازی در رمزنگاری و رمزگشایی (برای یک طرح کلید عمومی) رشته‌هایی از دیتا بطور استثنایی کاراست و می‌تواند براحتی در سخت‌افزارهای رایج پیاده‌سازی شود، بنابراین بخوبی با رمزنگاری و تصدیق‌هویت در ارتباطات سازگار است.

طول‌های کلیدها برای این طرح های جایگزین بسیار کوتاهتر از کلیدهای مورد استفاده در RSA است که آنها برای استفاده در چپ‌کارت‌ها مناسب‌تر است. اما RSA محکی برای ارزیابی سایر الگوریتم ها باقی مانده است؛ حضور و بقای نزدیک به سه‌دهه از این الگوریتم، تضمینی در برابر ضعف های عمده بشمار می‌رود.

اساس رمز‌گذاری‌ها وجود کلیدها می‌باشند. بدین معنی که شما اطلاعات مورد نظر خود را توسط کلید قفل می‌کنید و سپس برای رمزگشایی آن مجدداً از کلید استفاده می‌کنید. در رمزگشایی با کلید متقارن، هر دو کلیدی که برای قفل و باز کردن اطلاعات استفاده می‌شود یکسان می‌باشد. بدین معنی که هر دو طرف از یک کلید یکسان بهره می‌برند که باید نزد خودشان امن باشد. توجه کنید که مفهوم کلید در مباحث مرتبط، عموماً یک آرایه از بایت‌ها می‌باشد که بر اساس نوع امنیت طول متفاوتی دارد. مثلاً ۰۱۱۰۱۱۰۰۱۱۰۰۱۱۰۰۱۱۰۰۱۱ می‌تواند یک کلید باشد. البته عموماً کلیدها در مبنای ۱۶ نمایش داده می‌شوند. اما نوعی دیگر از رمزگذاری وجود دارد که اساس SSL نیز می‌باشد. در این رمزگذاری که رمزگذاری نا متقارن یا رمزگذاری کلید عمومی نامیده می‌شود، دو نوع کلید وجود دارد:

کلید عمومی در این رمز گذاری گفته می شود که اگر داده ای با یک کلید قفل شد، با همان کلید باز نمی شود و فقط امکان باز شدن آن با کلید متناظر آن وجود دارد. این کلید متناظر نزد طرف مقابل است و امکان بدست آوردن آن از کلید دیگر وجود ندارد. به عبارت ساده تر اگر شما در خانه تان را با کلید A قفل نمودید، تنها امکان باز شدن آن با کلید متناظر B وجود دارد و این در حالیست که امکان فهمیدن آنکه کلید B چگونه ساخته شده است برای شما نیز وجود ندارد. حال اگر کلید خود را درون در نیز جا بگذارید، مساله ای نیست!

حال به بحث باز می گردیم: شما درخواست داده ای از یک سرور امن می کنید، سرور کلید عمومی را برای شما ارسال می کند. شما داده های خود را با این کلید قفل می کنید و برای سرور ارسال می کنید. حال اگر این وسط کسی خواست داده ها را ببیند، نمی تواند، چراکه این داده ها با کلید عمومی باز نمی شوند. در طرف مقابل سرور با کلید خصوصی خود داده ها را رمز گشایی می کند و از آن استفاده می کند. شکل زیر روند ذکر شده را می رساند:



شکل ۲-۱۷- سیستمهای کلید نامتقارن [45]

توجه: در امضای دیجیتالی روند برعکس است. به عبارت دیگر امضای دیجیتالی چیزی جز رمز گذاری داده ها با کلید خصوصی فرستنده نیست. ما در امضای دیجیتالی می خواهیم ببینیم که آیا داده های ارسال شده واقعاً از طرف شخصی است که ادعا می کند یا خیر؟

به طور ساده کاربر نام خود را با کلید خصوصی خود رمز گذاری می کند. در این حالت همه با کلید عمومی وی می توانند نام وی را رمز گشایی کنند و این صحیح است. چراکه هیچ کس دیگر قادر نیست داده ای تولید کند که نتیجه باز شدن آن با کلید عمومی شخص امضا کننده برابر باشد.

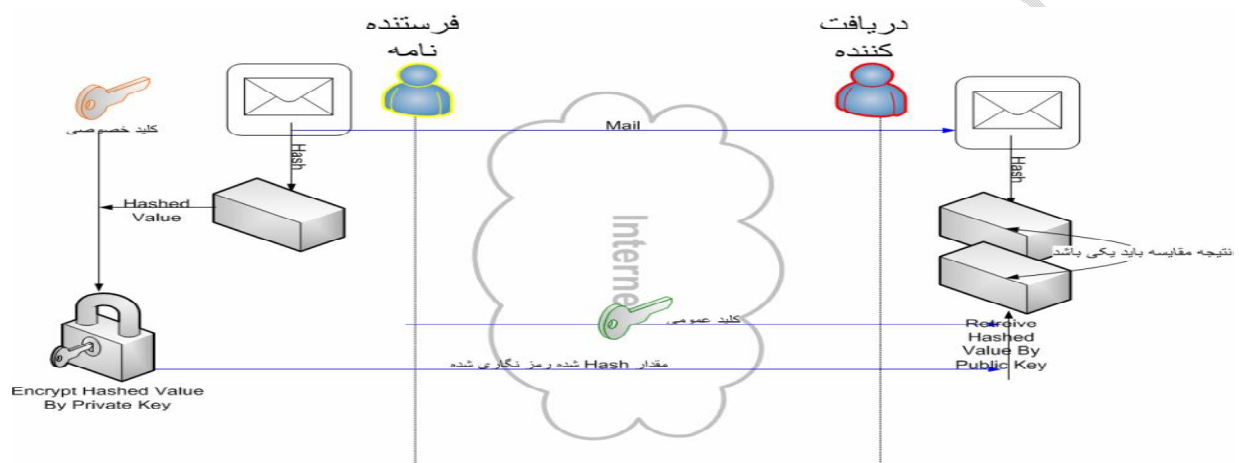
البته در عمل بهتر است از توابع Hash استفاده می شود. چراکه در حالت فوق، اولاً نام کاربر را باید فقط کاربر و سرور بدانند و دیگر آنکه از کجا معلوم که داده ارسالی همانی است که امضای دیجیتالی کاربر با آن بوده است (به عبارت دیگر شاید در میان راه متن اطلاعات تغییر کرد).

همانطور که ذکر شد، در این مورد از توابع Hash که یک طرفه هستند استفاده می‌شود. بدین معنی که اگر داده‌ای Hash شد، دیگر به هیچ عنوان و توسط هیچ کلیدی قابل برگشت نیست.

بدین منظور متن نامه ابتدا Hash می‌گردد و سپس توسط کلید خصوصی امضا می‌شود.

سپس امضا و متن نامه ارسال می‌شود. در طرف سرور هم با کلید عمومی داده Hash شده بدست می‌آید. متن ارسالی هم Hash می‌شود. حال اگر این دو نتیجه یکسان بود، داده‌ها واقعا از طرف کسی که مدعی آن است ارسال شده است. چرا که اگر متن نامه عوض شود، نتیجه Hash آن هم متفاوت و مقایسه نتیجه یکسانی را بر نمی‌گرداند.

در نمودار زیر، روند کار را مشاهده می‌کنید (قطعه‌های خاکستری رنگ نشان دهنده Hash شدن متن نامه می‌باشند).



شکل ۲-۱۸- ساختار نهایی سیستمهای کلید نامتقارن [45]

۲-۲-۴-۱۹- ساختار و روند آغازین پایه گذاری یک ارتباط امن

در این پروتکل قبل از آنکه اطلاعاتی مابین درخواست دهنده و سرور رد و بدل شود، می‌بایست ابتدا سرور تصدیق گردد. به طور کلی مرحله آغازین شروع ایجاد ارتباط امن از دو فاز تشکیل شده است: تصدیق هویت سرور و مرحله اختیاری تصدیق هویت مشتری. در فاز تصدیق هویت سرور سرور در جواب درخواست مشتری گواهینامه خود و فرمول رمز گذاری خود را برای مشتری ارسال می‌کند. سپس مشتری یک کلید اصلی که با کلید عمومی سرور رمز گذاری شده است را تولید می‌کند و سپس این کلید رمز گذاری شده را به سرور ارسال می‌کند. سرور کلید اصلی را بازیابی می‌کند و خودش را با فرستادن پیغامی به مشتری تصدیق می‌نماید. درخواست های بعدی با کلید هایی که از کلید اصلی مشتق شده‌اند رمز گذاری و تصدیق می‌شوند. در فاز دوم که اختیاری بود، سرور یک چالش را برای مشتری ایجاد می‌کند ارسال می‌کند. مشتری نیز خودش را برای سرور با ارسال امضای دیجیتالی و گواهینامه کلید عمومی خود نسبت به تصدیق خود اقدام می‌نماید.

الگوریتم‌های زیادی جهت پنهان‌سازی در SSL استفاده می‌شوند. در مرحله آغازین شروع ایجاد ارتباط امن از الگوریتم RSA public-key cryptosystem استفاده می‌شود. بعد از رد و بدل شدن کلیدها نیز الگوریتم‌های متفاوتی استفاده می‌شوند. از جمله: RC۲، RC۴، IDEA، DES، triple-DES و MD۵. گواهینامه‌های کلید عمومی هم از قوانین X.۵۰۹ پیروی می‌کنند (ساختار درختی CAها و امضای گواهینامه‌ها که در ادامه ذکر خواهد شد، همگی بر اساس این استاندارد است).

۲-۲-۴-۲۰- پروتکل‌های مشابه

TLS هم پروتکلی است که بسیار مشابه ۳,۰ SSL می‌باشد. همچنین پروتکل WTLS که مخصوص شبکه‌های بی سیم است و در WAP استفاده می‌گردد.

۲-۲-۴-۲۱- مفهوم گواهینامه در پروتکل SSL

در اینجا نیاز است که یک بحث کلی در مورد گواهینامه مورد نیاز این پروتکل صورت گیرد. به طور عموم (غیر از بحث SSL) گواهینامه‌ها جنبه اعتبار سنجی دارند. بدین معنی که اگر شما در یک بحث خاص دارای گواهینامه باشید، به شما اعتماد بیشتری می‌کنند. اما ممکن است گواهینامه نداشته باشید ولی کار خود را هم به نحو احسن انجام دهید. به طور مثال شما قهرمان مسابقات فرمول ۱ جهان هستید، اما در صورتی که گواهینامه نداشته باشید، هرگز اجازه نخواهید داشت که در شهر تردد کنید!

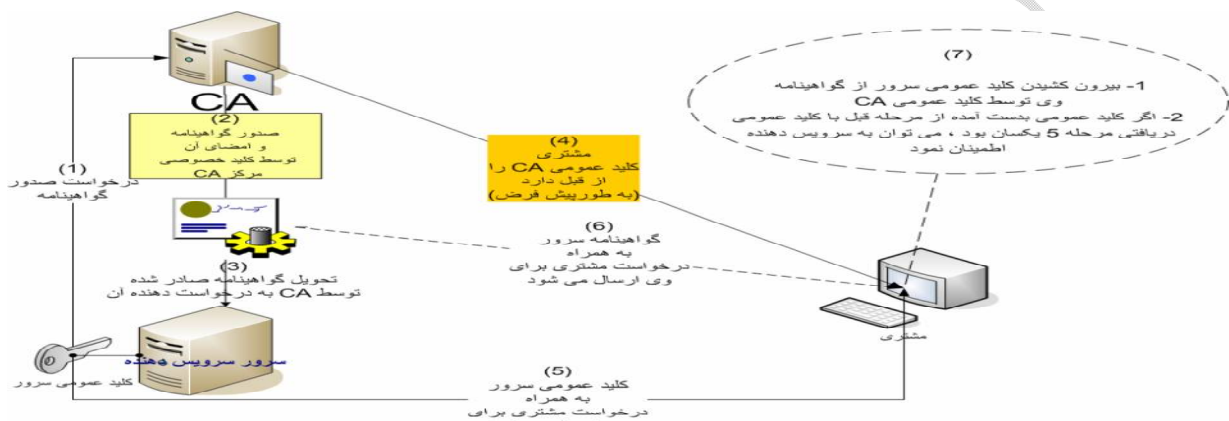
در مورد SSL هم تقریباً بحث به همین گونه است با این تفاوت که ذات این پروتکل با توجه به بحث گواهینامه‌ها طراحی شده است بدین معنی که اگر دارای گواهینامه نباشید، قادر نخواهید بود که یک پیاده‌سازی از این پروتکل را داشته باشید. شاید در عالم راندن اتومبیل بدین صورت تعبیر شود که در صورتی که شما دارای گواهینامه نباشید، قادر به راندگی هم نیستید! این تشابه از جهاتی صحیح و از جهاتی غلط است. شاید برداشت صحیح تر به این صورت باشد که اگرچه قادر نخواهید بود بدون گواهینامه راندگی کنید، اما قادر هستید که خود برای خود یک گواهینامه صادر کرده و سپس به راندگی بپردازید. (هرچند این گواهینامه از نظر دیگران کاملاً بی‌ارزش است).

طبق بحث فوق، شما قادر خواهید بود بدون پرداخت هیچ هزینه‌ای یک پروتکل SSL را راه اندازی و استفاده نمایید. نمونه بارز این استفاده در شبکه‌های داخلی یا Intranet می‌باشد.

۲-۲-۴-۲۲- مراکز صدور گواهینامه [46]

در SSL به مراکزی که اقدام به صدور گواهینامه می‌کنند "مراکز صدور گواهینامه" یا به اختصار CA گفته می‌شود. این پروتکل از یک شخص ثالث (که همان CA می‌باشد) برای تشخیص هویت طرفین یک تراکنش استفاده می‌کند. در واقع یک گواهینامه معین می‌کند که آیا شخصی که دارنده آن است، واقعا همانی است که ادعا می‌کند یا خیر؟

در شکل زیر می‌توانید یک روند درخواست صدور گواهینامه توسط یک سرویس دهنده (قدم های ۲، ۳ و ۴) و در ادامه آن درخواست کاربر برای یک سرور دارای گواهینامه و چگونگی مطمئن شدن وی از معتبر بودن آن سرور را ببینید (قدم های ۵، ۶، ۷).



شکل ۲-۱۹- مراکز صدور گواهینامه [46]

۲-۲-۴-۲۳- مراحل کلی برقراری و ایجاد ارتباط امن در وب

به طور ساده مراحل که در ایجاد یک ارتباط امن SSL در Http طی می‌شود، به صورت زیر می‌باشد:

- ۱- کاربر درخواست خود را از طریق مرورگر به یک صفحه امن ارسال می‌کند (آدرس این صفحه معمولاً با `https://` شروع می‌شود)
- ۲- وب سرور کلید عمومی خود را به همراه گواهینامه خود برای کاربر ارسال می‌کند.
- ۳- مرورگر چک می‌کند که آیا این گواهینامه توسط یک مرکز مورد اطمینان صادر شده است و اینکه آیا این گواهینامه هنوز اعتبار دارد و همچنین آیا این گواهینامه مرتبط با سایت درخواستی می‌باشد.
- ۴- سپس مرورگر از این کلید عمومی دریافت شده از طرف سرور استفاده می‌کند سپس یک کلید متقارن را رمز گذاری می‌کند. در نهایت هم داده‌های رمز URL تصادفی را تولید می‌کند و توسط آن تمام داده‌ها و گذاری شده را به همراه خود کلید متقارن تولیدی، مجدداً توسط کلید عمومی سرور رمز گذاری کرده و نتیجه را به سرور ارسال می‌کند.

۵- وب سرور توسط کلید خصوصی خود، کلید متقارن رمز گذاری شده را رمزگشایی و با استفاده از آن سایر داده ها و URL را نیز رمزگشایی می نماید.

۶- وب سرور، html درخواستی را با کمک کلید متقارن رمز گذاری و به کاربر باز می گرداند.

۷- مرورگر نیز داده های دریافتی را با کمک کلید متقارن خود بازگشایی کرده و به کاربر نمایش می دهد.

همانطور که از مرحله ۳ پیداست، در این مرحله است که میزان اعتبار CA مشخص می شود. در صورتی که این CA به هر دلیل از نظر مرورگر دارای اعتبار و شرایط خاصی نباشند، هشدار مبنی بر عدم امن بودن سایت مورد نظر به کاربر ارائه می دهد. توجه کنید که در این مورد تنها به هشدار بسنده می شود، اطمینان به آن به شما و شرایط شما بستگی دارد. در ضمن آنکه این هشدار هرگز نمی تواند به معنای قطعی عدم وجود امنیت باشد. حال اگر شما یک CA اینترنت راه اندازی کردید، مسلماً هیچ کدام از مرورگرها شما را نمی شناسند و بنابراین گواهی های صادر شده از طرف شما را نا امن می پندارند. از آنجا که کاربران عادی اینترنت نیز این هشدارها را جدی در نظر می گیرند، از ادامه تراکنش با سایت شما صرف نظر خواهند کرد.

۲-۲-۴-۲۴- نکاتی در مورد گواهینامه ها

شما در صورتی به یک سایت با یک گواهینامه معین اعتماد می کنید که آنرا یک CA معتبر (حداقل نزد شما) امضا کرده باشد. در واقع این اعتماد شما ضمنی است. به این روند، درخت اعتبار گواهینامه یا مسیر گواهینامه گفته می شود. معمولاً مرورگرها تعدادی از CA های معروف را برای خود در نظر می گیرد.

ای متفاوتی در اینترنت وجود دارد که شاید مشهورترین verisign آن باشد. به هر حال قرار نیست شما همیشه، با توجه به تراکنش خود، به تمام CA ها یا به عبارت بهتر به انواع گواهینامه آنها اعتماد کنید یک راه مناسب برای تشخیص این موضوع میزان مبلغی است که گواهینامه مورد نظر تراکنش شما را بیمه می کند. به طور مثال حداکثر مبلغی که iranSSL تراکنش شما را بیمه می کند ۱۰,۰۰۰ دلار می باشد. اما Verisign گواهینامه ای دارد که تا ۲۵۰,۰۰۰ دلار تراکنش شما را بیمه می نماید.

پروتکل SSL بر اساس میزان امن بودن دسته بندی می شوند. این دسته بندی بر اساس مقدار bit های تولیدی به ازاء هر بخش از داده ای است که رمز گذاری می شود. مسلماً هرچه تعداد این bit های تولیدی بیشتر باشد، رمزگشایی آن بدون کلید، بسیار سخت تر و با استفاده از کلید نیز زمان برتر خواهد بود. به عنوان نمونه یک SSL با ۴۰ یا ۵۶ بیت که یک رمز گذاری ضعیف می باشد می تواند توسط یک هکر با ابزار کافی، در عرض چند دقیقه شکسته شود. اما همین هکر برای مقابله با SSL ۱۲۸ بیتی، نیاز به ۲۸۸ بار زمان بیشتر دارد و این بدین معنی است که SSL ۱۲۸ بیتی نسبت به حالت ۴۰ یا ۵۶ بیتی ترلیون ترلیون بار امن تر و غیر قابل نفوذتر است!

یک بحث دیگر اینجا مطرح می شود و آن اینکه اگر یک هکر در میان راه کلید عمومی خود را جایگزین کلید عمومی سرور کرد. در این حالت عملاً هکر به راحتی به اطلاعات کاربر دسترسی خواهد داشت. در واقع این CA ها کلید عمومی سرور را با

کلید خصوصی خود امضا می‌کنند. مرورگر هم CAهای قابل اعتماد را می‌شناسد (کلید عمومی آنها را دارد). این کلید عمومی سرور که توسط کلید خصوصی CA رمز گذاری شده است همان گواهینامه می‌باشد. از آنجا که سرور می‌بایست گواهینامه خود را ارسال کند، در سمت مرورگر سعی می‌شود که توسط کلیدهای عمومی CAهایی را که می‌شناسد، آن گواهینامه را رمز گشایی کند. اگر موفق شد و نتیجه با کلید عمومی سرور یکسان بود در واقع گواهینامه قابل اعتماد است. در این صورت امکان استفاده از گواهینامه دیگران هم وجود ندارد. دقیقاً همان بحث امضای دیجیتالی است.

۲-۲-۴-۲۵- تشخیص هویت [46]

یکی از مباحث مهم و اصول در ارتباطات ایمن، تشخیص هویت متقابل از هر دو طرف Client و Server می‌باشد. در یک ارتباط، می‌باشد هویت اصلی سرور برای کاربران و برعکس مشخص شود زیرا در غیر این صورت هر سروری قادر به ایجاد اعتماد در کاربران خواهد بود. هر سرور باید دارای گواهینامه دیجیتالی باشد که این گواهینامه، نشان دهنده هویت اصلی آن است و توسط شرکت‌هایی مانند Verisign و Thawte ارائه می‌گردد. در این گواهینامه الکترونیکی اطلاعاتی از قبیل: کلید عمومی (برای مخفی سازی اطلاعات)، شماره سریال، نام دامنه، امضای دیجیتالی و تاریخ شروع و انقضای اعتبار گواهینامه درج می‌شود.

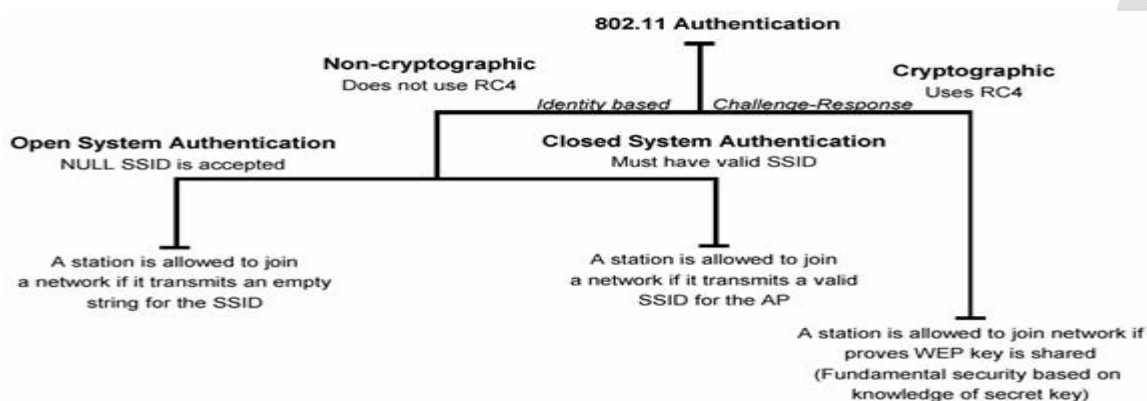
کاربر به راحتی می‌تواند مشخصات گواهینامه سرور را بررسی نماید. به عنوان مثال فرض کنید که برای خرید یک کالا به صورت On-line به یکی از سایت های مربوطه متصل شده‌اید، در ابتدا پیغامی مبنی بر ایجاد یک ارتباط با استفاده از SSL را ملاحظه می‌کنید، که بعد از تأیید آن، اگر به پایین پنجره مرورگر خود از سمت راست (Staus Bar) دقت نمایید، آیکونی (به شکل یک قفل) را مبنی بر یک ارتباط ایمن مشاهده خواهید کرد که با دو بار کلیک کردن بر روی آن می‌توانید اطلاعاتی گواهینامه سرور را بطور کامل مشاهده نمایید. البته باید توجه داشته باشید که حتماً مرورگر وب شما قابلیت پشتیبانی از SSL را داشته باشد و یا آن را غیرفعال نکرده باشید. برای اطمینان از فعال بودن این پروتکل، در Internet Explorer از منوهای بالا به منوی Tools > Internet Options رفته و از پنجره ظاهر شده، Tab مربوط به Advanced را انتخاب کرده و از انتخاب گزینه‌ای با عنوان Use SSL^۳ اطمینان حاصل کنید. پیشنهاد می‌کنم که حتماً قبل از استفاده از Credit Card خود در اینترنت، گواهینامه سرور را از نظر تاریخ انقضا و نام دامنه مورد بررسی قرار دهید.

۲-۲-۴-۲۶- سرویس‌های امنیتی WEP – Authentication [47]

در قسمت قبل به معرفی پروتکل WEP که عملاً تنها روش امن سازی ارتباطات در شبکه‌های بی‌سیم بر مبنای استاندارد ۸۰۲.۱۱ است پرداختیم و در ادامه سه سرویس اصلی این پروتکل را معرفی کردیم. در این قسمت به معرفی سرویس اول، یعنی Authentication، می‌پردازیم.

استاندارد ۸۰۲٫۱۱ دو روش برای احراز هویت کاربرانی که درخواست اتصال به شبکه‌ی بی‌سیم را به نقاط دسترسی ارسال می‌کنند، دارد که یک روش بر مبنای رمزنگاری ست و دیگری از رمزنگاری استفاده نمی‌کند.

شکل زیر شمایی از فرایند Authentication را در این شبکه‌ها نشان می‌دهد:



شکل ۲-۲۰- تشخیص هویت

همان‌گونه که در شکل نیز نشان داده شده است، یک روش از رمزنگاری RC4 استفاده می‌کند و روش دیگر از هیچ تکنیک رمزنگاری استفاده نمی‌کند.

۲-۲-۴-۲۷- Authentication بدون رمزنگاری

در روشی که مبتنی بر رمزنگاری نیست، دو روش برای تشخیص هویت مخدوم وجود دارد. در هر دو روش مخدوم متقاضی پیوستن به شبکه، درخواست ارسال هویت از سوی نقطه‌ی دسترسی را با پیامی حاوی یک SSID (Service Set Identifier) پاسخ می‌دهد.

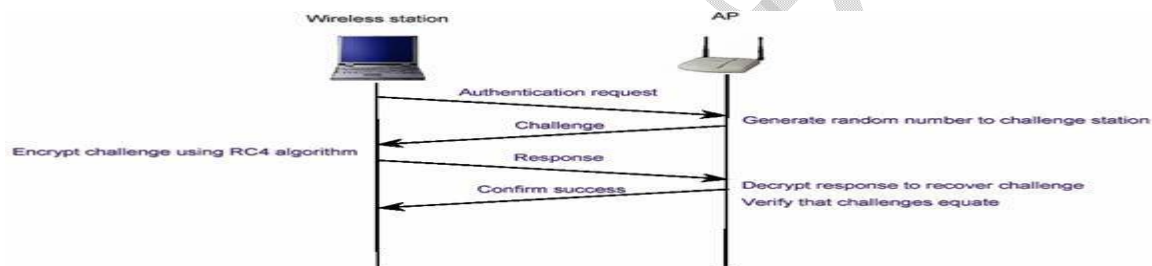
در روش اول که به Open System Authentication موسوم است، یک SSID خالی نیز برای دریافت اجازه‌ی اتصال به شبکه کفایت می‌کند. در واقع در این روش تمامی مخدوم‌هایی که تقاضای پیوستن به شبکه را به نقاط دسترسی ارسال می‌کنند با پاسخ مثبت روبه‌رو می‌شوند و تنها آدرس آن‌ها توسط نقطه‌ی دسترسی نگاه‌داری می‌شود. به همین دلیل به این روش NULL Authentication نیز اطلاق می‌شود.

در روش دوم از این نوع، بازهم یک SSID به نقطه‌ی دسترسی ارسال می‌گردد با این تفاوت که اجازه‌ی اتصال به شبکه تنها در صورتی از سوی نقطه‌ی دسترسی صادر می‌گردد که SSIDی ارسال شده جزو SSIDهای مجاز برای دسترسی به شبکه باشند. این روش به Closed System Authentication موسوم است.

نکته‌ای که در این میان اهمیت بسیاری دارد، توجه به سطح امنیتی‌ست که این روش در اختیار ما می‌گذارد. این دو روش عملاً روش امنی از احراز هویت را ارائه نمی‌دهند و عملاً تنها راهی برای آگاهی نسبی و نه قطعی از هویت درخواست‌کننده هستند. با این وصف از آنجایی که امنیت در این حالات تضمین شده نیست و معمولاً حملات موفق بسیاری، حتی توسط نفوذگران کم‌تجربه و مبتدی، به شبکه‌هایی که بر اساس این روش‌ها عمل می‌کنند رخ می‌دهد، لذا این دو روش تنها در حالتی کاربرد دارند که یا شبکه‌یی در حال ایجاد است که حاوی اطلاعات حیاتی نیست، یا احتمال رخداد حمله به آن بسیار کم است. هرچند که با توجه پوشش نسبتاً گسترده‌ی یک شبکه‌ی بی‌سیم که مانند شبکه‌های سیمی امکان محدودسازی دسترسی به صورت فیزیکی بسیار دشوار است اطمینان از شانس پایین رخ دادن حملات نیز خود تضمینی ندارد!

۲-۲-۴-۲۸- Authentication با رمزنگاری RC4

این روش که به روش «کلید مشترک» نیز موسوم است، تکنیکی کلاسیک است که بر اساس آن، پس از اطمینان از اینکه مخدوم از کلیدی سری آگاه است، هویتش تأیید می‌شود. شکل زیر این روش را نشان می‌دهد:



شکل ۲-۲۱- Authentication با رمزنگاری RC4

در این روش، نقطه‌ی دسترسی (AP) یک رشته‌ی تصادفی تولید کرده و آن را به مخدوم می‌فرستد. مخدوم این رشته‌ی تصادفی را با کلیدی از پیش تعیین شده (که کلید WEP نیز نامیده می‌شود) رمز می‌کند و حاصل را برای نقطه‌ی دسترسی ارسال می‌کند. نقطه‌ی دسترسی به روش معکوس پیام دریافتی را رمزگشایی کرده و با رشته‌ی ارسال شده مقایسه می‌کند. در صورت هم‌سانی این دو پیام، نقطه‌ی دسترسی از اینکه مخدوم کلید صحیحی را در اختیار دارد اطمینان حاصل می‌کند. روش رمزنگاری و رمزگشایی در این تبادل روش RC4 است.

در این میان با فرض اینکه رمزنگاری RC4 را روشی کاملاً مطمئن بدانیم، دو خطر در کمین این روش است:

الف) در این روش تنها نقطه‌ی دسترسی‌ست که از هویت مخدوم اطمینان حاصل می‌کند. به بیان دیگر مخدوم هیچ دلیلی در اختیار ندارد که بداند نقطه‌ی دسترسی که با آن در حال تبادل داده‌های رمزیت نقطه‌ی دسترسی اصلی‌ست.

ب) تمامی روش‌هایی که مانند این روش بر پایه‌ی سؤال و جواب بین دو طرف، با هدف احراز هویت یا تبادل اطلاعات حیاتی، قرار دارند با حملاتی تحت عنوان man-in-the-middle در خطر هستند. در این دسته از حملات نفوذگر میان دو طرف قرار می‌گیرد و به‌گونه‌ی هریک از دو طرف را گمراه می‌کند.

۲-۲-۴-۲۹- محرمانگی و امنیت

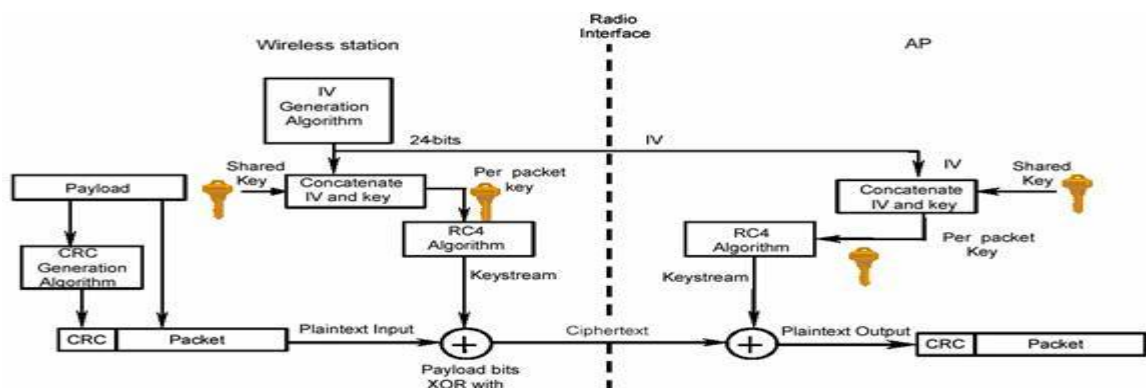
این سرویس که در حوزه‌های دیگر امنیتی اغلب به عنوان Confidentiality از آن یاد می‌گردد به معنای حفظ امنیت و محرمانه نگاه داشتن اطلاعات کاربر یا گره‌های در حال تبادل اطلاعات با یکدیگر است. برای رعایت محرمانگی عموماً از تکنیک‌های رمزنگاری استفاده می‌گردد، به‌گونه‌ای که در صورت شنود اطلاعات در حال تبادل، این اطلاعات بدون داشتن کلیدهای رمز، قابل رمزگشایی نبوده و لذا برای شنودگر غیرقابل سوء استفاده است.

در استاندارد 802.11b، از تکنیک‌های رمزنگاری WEP استفاده می‌گردد که برپایه‌ی RC4 است. RC4 یک الگوریتم رمزنگاری متقارن است که در آن یک رشته‌ی نیمه تصادفی تولید می‌گردد و توسط آن کل داده رمز می‌شود. این رمزنگاری بر روی تمام بسته‌ی اطلاعاتی پیاده می‌شود. به بیان دیگر داده‌های تمامی لایه‌های بالای اتصال بی‌سیم نیز توسط این روش رمز می‌گردند، از IP گرفته تا لایه‌های بالاتری مانند HTTP. از آنجایی که این روش عملاً اصلی‌ترین بخش از اعمال سیاست‌های امنیتی در شبکه‌های محلی بی‌سیم مبتنی بر استاندارد 802.11b است، معمولاً به کل پروسه‌ی امن‌سازی اطلاعات در این استاندارد به اختصار WEP گفته می‌شود.

کلیدهای WEP اندازه‌هایی از ۴۰ بیت تا ۱۰۴ بیت می‌توانند داشته باشند. این کلیدها با IV (مخفف Initialization Vector یا بردار اولیه) ۲۴ بیتی ترکیب شده و یک کلید ۱۲۸ بیتی RC4 را تشکیل می‌دهند. طبیعتاً هرچه اندازه‌ی کلید بزرگ‌تر باشد امنیت اطلاعات بالاتر است. تحقیقات نشان می‌دهد که استفاده از کلیدهایی با اندازه‌ی ۸۰ بیت یا بالاتر عملاً استفاده از تکنیک brute-force را برای شکستن رمز غیرممکن می‌کند. به عبارت دیگر تعداد کلیدهای ممکن برای اندازه‌ی ۸۰ بیت (که تعداد آن‌ها از مرتبه‌ی ۲۴ است) به اندازه‌ی بالاست که قدرت پردازش سیستم‌های رایانه‌ی کنونی برای شکستن کلیدی مفروض در زمانی معقول کفایت نمی‌کند.

هرچند که در حال حاضر اکثر شبکه‌های محلی بی‌سیم از کلیدهای ۴۰ بیتی برای رمزکردن بسته‌های اطلاعاتی استفاده می‌کنند ولی نکته‌ی این که اخیراً، بر اساس یک سری آزمایشات به دست آمده است، این است که روش تأمین محرمانگی توسط WEP در مقابل حملات دیگری، غیر از استفاده از روش brute-force، نیز آسیب‌پذیر است و این آسیب‌پذیری ارتباطی به اندازه‌ی کلید استفاده شده ندارد.

نمایی از روش استفاده شده توسط WEP برای تضمین محرمانه‌گی در شکل زیر نمایش داده شده است:



شکل ۲-۲۲- روش استفاده شده توسط WEP برای تضمین محرمانه‌گی

۲-۲-۳- Integrity

مقصود از Integrity صحت اطلاعات در حین تبادل است و سیاست‌های امنیتی که Integrity را تضمین می‌کنند روش‌هایی هستند که امکان تغییر اطلاعات در حین تبادل را به کم‌ترین میزان تقلیل می‌دهند.

در استاندارد 802.11b نیز سرویس و روشی استفاده می‌شود که توسط آن امکان تغییر اطلاعات در حال تبادل میان مخدوم‌های بی‌سیم و نقاط دسترسی کم می‌شود. روش مورد نظر استفاده از یک کد CRC است. همان‌طور که در شکل قبل نیز نشان داده شده است، یک CRC-32 قبل از رمز شدن بسته تولید می‌شود. در سمت گیرنده، پس از رمزگشایی، CRC داده‌های رمزگشایی شده مجدداً محاسبه شده و با CRC نوشته شده در بسته مقایسه می‌گردد که هرگونه اختلاف میان دو CRC به معنای تغییر محتویات بسته در حین تبادل است. متأسفانه این روش نیز مانند روش رمزنگاری توسط RC4، مستقل از اندازه‌ی کلید امنیتی مورد استفاده، در مقابل برخی از حملات شناخته شده آسیب‌پذیر است.

متأسفانه استاندارد 802.11b هیچ مکانیزمی برای مدیریت کلیدهای امنیتی ندارد و عملاً تمامی عملیاتی که برای حفظ امنیت کلیدها انجام می‌گیرد باید توسط کسانی که شبکه‌ی بی‌سیم را نصب می‌کنند به صورت دستی پیاده‌سازی گردد. از آنجایی که این بخش از امنیت یکی از معضله‌های اساسی در رمزنگاری است، با این ضعف عملاً روش‌های متعددی برای حمله به شبکه‌های بی‌سیم قابل تصور است. این روش‌ها معمولاً بر سهل انگاری‌های انجام‌شده از سوی کاربران و مدیران شبکه مانند تغییر ندادن کلید به صورت مداوم، لودادن کلید، استفاده از کلیدهای تکراری یا کلیدهای پیش فرض کارخانه و دیگر بی توجهی‌ها نتیجه‌ای جز درصد نسبتاً بالایی از حملات موفق به شبکه‌های بی‌سیم ندارد. این مشکل از شبکه‌های بزرگ‌تر بیش‌تر خود را نشان می‌دهد. حتا با فرض تلاش برای جلوگیری از رخداد چنین سهل‌انگاری‌هایی، زمانی که تعداد

مخدوم‌های شبکه از حدی می‌گذرد عملاً کنترل کردن این تعداد بالا بسیار دشوار شده و گاهی خطاهایی در گوشه و کنار این شبکه‌ی نسبتاً بزرگ رخ می‌دهد که همان باعث رخنه در کل شبکه می‌شود.

۲-۲-۴-۳۱-ضعف‌های اولیه‌ی امنیتی WEP

در قسمت‌های قبل به سرویس‌های امنیتی استاندارد 802.11 پرداختیم. در ضمن ذکر هر یک از سرویس‌ها، سعی کردیم به ضعف‌های هریک اشاره‌ی داشته باشیم. در این قسمت به بررسی ضعف‌های تکنیک‌های امنیتی پایه‌ی استفاده شده در این استاندارد می‌پردازیم. همان‌گونه که گفته شد، عملاً پایه‌ی امنیت در استاندارد 802.11 بر اساس پروتکل WEP استوار است. WEP در حالت استاندارد بر اساس کلیدهای ۴۰ بیتی برای رمزنگاری توسط الگوریتم RC4 استفاده می‌شود، هرچند که برخی از تولیدکننده‌گان نگارش‌های خاصی از WEP را با کلیدهایی با تعداد بیت‌های بیش‌تر پیاده‌سازی کرده‌اند. نکته‌ای که در این میان اهمیت دارد قائل شدن تمایز میان نسبت بالارفتن امنیت و اندازه‌ی کلیدهاست. با وجود آن که با بالارفتن اندازه‌ی کلید (تا ۱۰۴ بیت) امنیت بالاتر می‌رود، ولی از آن‌جاکه این کلیدها توسط کاربران و بر اساس یک کلمه‌ی عبور تعیین می‌شود، تضمینی نیست که این اندازه تماماً استفاده شود. از سوی دیگر همان‌طور که در قسمت‌های پیشین نیز ذکر شد، دستیابی به این کلیدها فرایند چندان سختی نیست، که در آن صورت دیگر اندازه‌ی کلید اهمیتی ندارد. متخصصان امنیت بررسی‌های بسیاری را برای تعیین حفره‌های امنیتی این استاندارد انجام داده‌اند که در این راستا خطراتی که ناشی از حملاتی متنوع، شامل حملات غیرفعال و فعال است، تحلیل شده است. حاصل بررسی‌های انجام شده فهرستی از ضعف‌های اولیه‌ی این پروتکل است:

۱. استفاده از کلیدهای ثابت WEP

یکی از ابتدایی‌ترین ضعف‌ها که عموماً در بسیاری از شبکه‌های محلی بی‌سیم وجود دارد استفاده از کلیدهای مشابه توسط کاربران برای مدت زمان نسبتاً زیاد است. این ضعف به دلیل نبود یک مکانیزم مدیریت کلید رخ می‌دهد. برای مثال اگر یک کامپیوتر کیفی یا جیبی که از یک کلید خاص استفاده می‌کند به سرقت برود یا برای مدت زمانی در دسترس نفوذگر باشد، کلید آن به راحتی لو رفته و با توجه به تشابه کلید میان بسیاری از ایستگاه‌های کاری عملاً استفاده از تمامی این ایستگاه‌ها ناامن است.

از سوی دیگر با توجه به تشابه بودن کلید، در هر لحظه کانال‌های ارتباطی زیادی توسط یک حمله نفوذپذیر هستند.

۲. Initialization Vector (IV)

این بردار که یک فیلد ۲۴ بیتی است در قسمت قبل معرفی شده است. این بردار به صورت متنی ساده فرستاده می‌شود. از آن‌جایی که کلیدی که برای رمزنگاری مورد استفاده قرار می‌گیرد بر اساس IV تولید می‌شود، محدوده‌ی IV عملاً

نشان‌دهنده‌ی احتمال تکرار آن و در نتیجه احتمال تولید کلیدهای مشابه است. به عبارت دیگر در صورتی که IV کوتاه باشد در مدت زمان کمی می‌توان به کلیدهای مشابه دست یافت. این ضعف در شبکه‌های شلوغ به مشکلی حاد مبدل می‌شود. خصوصاً اگر از کارت شبکه‌ی استفاده شده مطمئن نباشیم. بسیاری از کارت‌های شبکه از IVهای ثابت استفاده می‌کنند و بسیاری از کارت‌های شبکه‌ی یک تولید کننده‌ی واحد IVهای مشابه دارند. این خطر به همراه ترافیک بالا در یک شبکه‌ی شلوغ احتمال تکرار IV در مدت زمانی کوتاه را بالاتر می‌برد و در نتیجه کافیست نفوذگر در مدت زمانی معین به ثبت داده‌های رمز شده‌ی شبکه بپردازد و IVهای بسته‌های اطلاعاتی را ذخیره کند. با ایجاد بانکی از IVهای استفاده شده در یک شبکه‌ی شلوغ احتمال بالایی برای نفوذ به آن شبکه در مدت زمانی نه چندان طولانی وجود خواهد داشت.

۳. ضعف در الگوریتم

از آنجایی که IV در تمامی بسته‌های تکرار می‌شود و بر اساس آن کلید تولید می‌شود، نفوذگر می‌تواند با تحلیل و آنالیز تعداد نسبتاً زیادی از IVها و بسته‌های رمز شده بر اساس کلید تولید شده بر مبنای آن IV، به کلید اصلی دست پیدا کند. این فرایند عملی زمان بر است ولی از آنجاکه احتمال موفقیت در آن وجود دارد لذا به عنوان ضعفی برای این پروتکل محسوب می‌گردد.

۴. استفاده از CRC رمز نشده

در پروتکل WEP، کد CRC رمز نمی‌شود. لذا بسته‌های تأییدی که از سوی نقاط دسترسی بی‌سیم به سوی گیرنده ارسال می‌شود بر اساس یک CRC رمز نشده ارسال می‌گردد و تنها در صورتی که نقطه‌ی دسترسی از صحت بسته اطمینان حاصل کند تأیید آن را می‌فرستد. این ضعف این امکان را فراهم می‌کند که نفوذگر برای رمزگشایی یک بسته، محتوای آن را تغییر دهد و CRC را نیز به دلیل این که رمز نشده است، به راحتی عوض کند و منتظر عکس‌العمل نقطه‌ی دسترسی بماند که آیا بسته‌ی تأیید را صادر می‌کند یا خیر.

ضعف‌های بیان شده از مهم‌ترین ضعف‌های شبکه‌های بی‌سیم مبتنی بر پروتکل WEP هستند. نکته‌ای که در مورد ضعف‌های فوق باید به آن اشاره کرد این است که در میان این ضعف‌ها تنها یکی از آن‌ها (مشکل امنیتی سوم) به ضعف در الگوریتم رمزنگاری باز می‌گردد و لذا با تغییر الگوریتم رمزنگاری تنها این ضعف است که برطرف می‌گردد و بقیه‌ی مشکلات امنیتی کماکان به قوت خود باقی هستند.

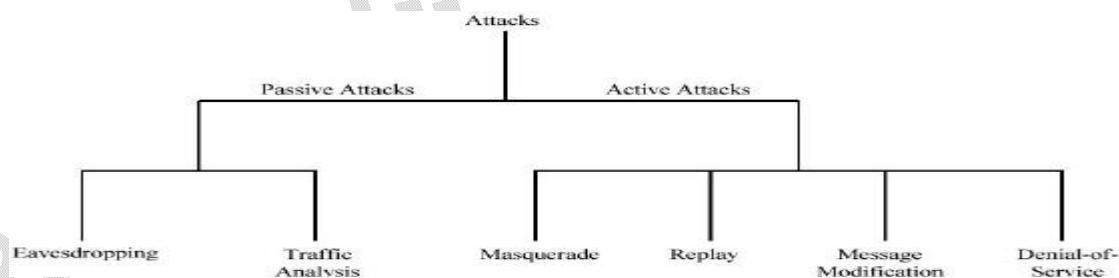
جدول زیر ضعف‌های امنیتی پروتکل WEP را به اختصار جمع‌بندی کرده است:

Security Issue / Vulnerability	Remarks
1. Security features in vendor products are frequently not enabled.	Security features, albeit poor in some cases, are not enabled when shipped, and users do not enable when installed. Bad security is generally better than no security.
2. IVs are short (or static).	24-bit IVs cause the generated key stream to repeat. Repetition allows easy decryption of data for a moderately sophisticated adversary.
3. Cryptographic keys are short.	40-bit keys are inadequate for any system. It is generally accepted that key sizes should be greater than 80 bits in length. The longer the key, the less likely a compromise is possible from a brute-force attack.
4. Cryptographic keys are shared.	Keys that are shared can compromise a system. A fundamental tenant of cryptography is that the security of a system is largely dependent on the secrecy of the keys.
5. Cryptographic keys cannot be updated automatically and frequently.	Cryptographic keys should be changed often to prevent brute-force attacks.
6. RC4 has a weak key schedule and is inappropriately used in WEP.	The combination of revealing 24 key bits in the IV and a weakness in the initial few bytes of the RC4 keystream leads to an efficient attack that recovers the key. Most other applications of RC4 do not expose the weaknesses of RC4 because they do not reveal key bits and do not restart the key schedule for every packet. This attack is available to moderately sophisticated adversaries.
7. Packet integrity is poor.	CRC32 and other linear block codes are inadequate for providing cryptographic integrity. Message modification is possible. Linear codes are inadequate for the protection against advertent attacks on data integrity. Cryptographic protection is required to prevent deliberate attacks. Use of noncryptographic protocols often facilitates attacks against the cryptography.
8. No user authentication occurs.	Only the device is authenticated. A device that is stolen can access the network.
9. Authentication is not enabled; only simple SSID identification occurs.	Identity-based systems are highly vulnerable particularly in a wireless system.
10. Device authentication is simple shared-key challenge-response.	One-way challenge-response authentication is subject to "man-in-the-middle" attacks. Mutual authentication is required to provide verification that users and the network are legitimate.

شکل ۲-۲۲-ضعف‌های اولیه امنیتی WEP

۲-۲-۴-۳۲-خطرهای حملات و ملزومات امنیتی

همان گونه که گفته شد، با توجه به پیشرفت‌های اخیر، در آینده‌ی نه چندان دور باید منتظر گسترده‌گی هرچه بیش‌تر استفاده از شبکه‌های بی‌سیم باشیم. این گسترده‌گی، با توجه به مشکلاتی که از نظر امنیتی در این قبیل شبکه‌ها وجود دارد نگرانی‌هایی را نیز به همراه دارد. این نگرانی‌ها که نشان دهنده‌ی ریسک بالای استفاده از این بستر برای سازمان‌ها و شرکت‌های بزرگ است، توسعه‌ی این استاندارد را در ابهام فرو برده است. در این قسمت به دسته‌بندی و تعریف حملات، خطرهای و ریسک‌های موجود در استفاده از شبکه‌های محلی بی‌سیم بر اساس استاندارد IEEE 802.11x می‌پردازیم. شکل زیر نمایی از دسته‌بندی حملات مورد نظر را نشان می‌دهد:



شکل ۲-۲۳-خطرهای حملات و ملزومات امنیتی [47]

مطابق درخت، حملات امنیتی به دو دسته‌ی فعال و غیرفعال تقسیم می‌گردند.

- حملات غیرفعال

در این قبیل حملات، نفوذگر تنها به منبعی از اطلاعات به نحوی دست می یابد ولی اقدام به تغییر محتوای اطلاعات منبع نمی کند. این نوع حمله می تواند تنها به یکی از اشکال شنود ساده یا آنالیز ترافیک باشد.

- شنود

در این نوع، نفوذگر تنها به پایش اطلاعات ردوبدل شده می پردازد. برای مثال شنود ترافیک روی یک شبکه ی محلی یا یک شبکه ی بی سیم (که مد نظر ما است) نمونه هایی از این نوع حمله به شمار می آیند.

- آنالیز ترافیک

در این نوع حمله، نفوذگر با کپی برداشتن از اطلاعات پایش شده، به تحلیل جمعی داده ها می پردازد. به عبارت دیگر بسته یا بسته های اطلاعاتی به همراه یکدیگر اطلاعات معناداری را ایجاد می کنند.

- حملات فعال

در این نوع حملات، برخلاف حملات غیرفعال، نفوذگر اطلاعات مورد نظر را، که از منابع به دست می آید، تغییر می دهد، که تبعاً انجام این تغییرات مجاز نیست. از آن جایی که در این نوع حملات اطلاعات تغییر می کنند، شناسایی رخ داد حملات فرایندی امکان پذیر است. در این حملات به چهار دسته ی مرسوم زیر تقسیم بندی می گردند:

- تغییر هویت

در این نوع حمله، نفوذگر هویت اصلی را جعل می کند. این روش شامل تغییر هویت اصلی یکی از طرف های ارتباط یا قلب هویت و یا تغییر جریان واقعی فرایند پردازش اطلاعات نیز می گردد.

- پاسخ های جعلی

نفوذگر در این قسم از حملات، بسته هایی که طرف گیرنده ی اطلاعات در یک ارتباط دریافت می کند را پایش می کند. البته برای اطلاع از کل ماهیت ارتباط یک اتصال از ابتدا پایش می گردد ولی اطلاعات مفید تنها اطلاعاتی هستند که از سوی گیرنده برای فرستنده ارسال می گردند. این نوع حمله بیش تر در مواردی کاربرد دارد که فرستنده اقدام به تعیین هویت گیرنده می کند. در این حالت بسته های پاسخی که برای فرستنده به عنوان جواب به سؤالات فرستنده ارسال می گردند به معنای پرچمی برای شناسایی گیرنده محسوب می گردند. لذا در صورتی که نفوذگر این بسته ها را ذخیره کند و در زمانی که یا گیرنده فعال نیست، یا فعالیت یا ارتباط آن به صورت آگاهانه به روشی توسط نفوذگر قطع شده است، می تواند مورد سوءاستفاده قرار گیرد. نفوذگر با ارسال مجدد این بسته ها خود را به جای گیرنده جازده و از سطح دسترسی مورد نظر برخوردار می گردد.

- تغییر پیام

در برخی از موارد مرسوم‌ترین و متنوع‌ترین نوع حملات فعال تغییر پیام است. از آن جایی که گونه‌های متنوعی از ترافیک بر روی شبکه رفت و آمد می‌کنند و هریک از این ترافیک‌ها و پروتکل‌ها از شیوه‌ای برای مدیریت جنبه‌های امنیتی خود استفاده می‌کنند، لذا نفوذگر با اطلاع از پروتکل‌های مختلف می‌تواند برای هر یک از این انواع ترافیک نوع خاصی از تغییر پیام‌ها و در نتیجه حملات را اتخاذ کند. با توجه به گسترده‌گی این نوع حمله، که کاملاً به نوع پروتکل بستگی دارد، در این جا نمی‌توانیم به انواع مختلف آن پردازیم، تنها به یادآوری این نکته بسنده می‌کنیم که این حملات تنها دستیابی به اطلاعات را هدف نگرفته است و می‌تواند با اعمال تغییرات خاصی، به گمراهی دو طرف منجر شده و مشکلاتی را برای سطح مورد نظر دسترسی که می‌تواند یک کاربر عادی باشد فراهم کند.

- حمله‌های Denial-of-Service - DoS

این نوع حمله، در حالات معمول، مرسوم‌ترین حملات را شامل می‌شود. در این نوع حمله نفوذگر یا حمله‌کننده برای تغییر نحوه‌ی کارکرد یا مدیریت یک سامانه‌ی ارتباطی یا اطلاعاتی اقدام می‌کند. ساده‌ترین نمونه سعی در از کارانداختن خادم‌های نرم‌افزاری و سخت‌افزاری است. پیرو چنین حملاتی، نفوذگر پس از از کارانداختن یک سامانه، که معمولاً سامانه‌ای است که مشکلاتی برای نفوذگر برای دسترسی به اطلاعات فراهم کرده است، اقدام به سرقت، تغییر یا نفوذ به منبع اطلاعاتی می‌کند. در برخی از حالات، در پی حمله‌ی انجام شده، سرویس مورد نظر به طور کامل قطع نمی‌گردد و تنها کارایی آن مختل می‌گردد. در این حالت نفوذگر می‌تواند با سوءاستفاده از اختلال ایجاد شده به نفوذ از طریق همان سرویس نیز اقدام کند. تمامی ریسک‌هایی که در شبکه‌های محلی، خصوصاً انواع بی‌سیم، وجود دارد ناشی از یکی از خطرات فوق است.

۲-۲-۴-۳۳-مشکلات و معایب SSL [48]

۲-۲-۴-۳۳-۱-مشکل امنیتی در SSL

با وجود اینکه این پروتکل امروزه در سایتهای تجارت الکترونیکی مورد استفاده گسترده قرار می‌گیرد ولی نمی‌توان منکر معایب و نواقص آن شد. همانطور که می‌دانید کلید اصلی مربوط به ارتباطات SSL بصورت تصادفی ایجاد می‌شود، متأسفانه طراحی سیستم ایجاد کننده کلید جلسه (Session Key) این پروتکل که توسط شرکت Netscape ایجاد شده، ضعیف می‌باشد و یک هکر ماهر به راحتی قادر به پیدا کردن این کلید خواهد بود. نسخه‌های قبلی SSL از کلیدهای ۴۰ بیتی استفاده می‌کردند و نسخه ۳ این پروتکل از کلید ۱۲۸ بیتی استفاده می‌کند، لازم به ذکر است که تمامی نسخه‌ها این پروتکل به غیر نسخه ۳، توسط مهاجمان، Crack شده و نا امن است، البته هنوز نسخه ۳ کرک نشده، ولی کارشناسان احتمال وقوع این امر را در آینده‌ای نزدیک می‌دهند که در این صورت می‌بایست تحولات بنیادی در زیر بنای این پروتکل ایجاد شود.

۲-۲-۴-۳۳-۲- مشکلات تجارت الکترونیکی در ایران

اولین نکته هیچگاه به همه سایت ها اعتماد نکنید و شماره اعتباری خود را در اختیارشان قرار ندهید. بعضی سایت ها به بهانه Adult Check و بهانه هایی از قبیل، شماره کارت اعتباری شما را گرفته و از آن سوء استفاده می کنند. حتی بعضی سایت ها گواهینامه های دیجیتالی صحیح و تثبیت شده ای به شما نشان می دهند ولی امکان بروز مشکل همچنان وجود دارد. همیشه از سایت های معتبر که سیستم های تست شده ای را ارائه می دهند و مورد استفاده عموم قرار گرفته اند استفاده کنید. در این بین، امکان کلاهبرداری از کاربران ایرانی در اینترنت چند برابر می باشد. زیرا قوانینی برای حمایت از کشورهایی که در اقتصاد جهانی دارای محدودیت هستند وجود ندارد و نظارتی به روی این معاملات انجام نمی گیرد. همچنین خیلی از اجناس خریداری شده به ایران ارسال نمی گردد، ولی در کشورهای خارجی در صورتی که کالایی بعد از خرید Online به مقصد نرسد بلافاصله توسط مراجع قانونی مورد پیگیری بین المللی قرار خواهد گرفت. یکی از مشکلات مهم دیگر عدم دسترسی به کارتهای اعتباری بین المللی است، اگر چه گام های موثر و مثبتی در جهت رفع این مشکل توسط سازمانهای خصوصی و واسطه ای انجام گرفته و حتی در بعضی معاملات از کارتهای اعتباری داخلی استفاده می شود ولی تجارت الکترونیکی در ایران نیازمند حمایت بیشتری از طرف مسئولین امر می باشد.

فصل سوم

روش و ابزار تحقیق

۳-۱- ابزار مورد استفاده در شبیه سازی

ما جهت شبیه سازی راهکارهای امنیتی از نرم افزار NS2 استفاده نموده ایم. این نرم افزار محیطی است برای شبیه سازی پروژه های شبکه محور که قابلیت و قدرت مانور فوق العاده ای را در اختیار کاربر قرار می دهد. برای نصب این نرم افزار ابتدا لازم است که سیستم عامل لینوکس را نصب و پس از آن NS2 را بر روی این سیستم عامل نصب کنیم.

۳-۲- نصب NS-2 در لینوکس Fedora

با روش زیر و طی مراحل پایین می توان ns-2 را نصب کرد:

۱- گام اول: ابتدا باید Vmware workstation را باید در محیط ویندوز نصب کنیم.

بعد در داخل این نرم افزار لینوکس Fedora را نصب کرده و در مرحله بعد از لینک زیر ns-allinone-2.34 را دانلود می کنیم

<http://bit.ly/downloadns>

فایل را در پوشه که بنام admin ذخیره کرده و بعد وارد قسمت applications/accessories/terminal شده و دستورات زیر را وارد می کنیم. برای خارج کردن فایل از حالت زیپ دستور زیر را تایپ می کنیم.

```
tar -zxvf ns-allinone-2.34.tar.gz
```

حال صبر می کنیم تا فایلها از حالت زیپ خارج شوند.

۲- گام دوم: در قسمت Terminal مسیر را به مسیر زیر تغییر می دهیم. با دستور زیر:

```
cd ns-allinone-2.34 یا cd /home/erfan/ns-allinone-2.34
```

۳- گام سوم: تمام وابستگی ها را نصب می کنیم. با دستور زیر:

```
sudo apt-get install build-essential autoconf automake libxmu-dev gcc-4.3
```

حال صبر می کنیم تا این مرحله تمام شود. نکته قابل توجه اینکه رمزی را باید در این مرحله وارد کنیم همان رمزی است که ابتدا در نصب لینوکس وارد کرده بودیم.

۴- گام چهارم: تغییرات زیر را در فایل `makefile.in` در مسیر زیر اعمال کرده و از طریق مسیر گرافیکی لینوکس این کار را انجام می دهیم.
تغییرات را در پایان همان فایل وارد و فایل رل `save` می کنیم.

Find the line that says:

`CC= @CC@`

and change it to:

`CC= gcc-4.3`

۵- گام پنجم: به محیط Terminal برگشته و دستور زیر را در مسیری که قرار داریم وارد می کنیم.

```
sudo su $
install/.#
```

این مرحله وقت گیر و طولانی است کمی صبر می کنیم. در ادامه فایل `bashrs` را با دستور زیر فعال نموده و تغییرات زیر را در آخر فایل وارد می کنیم. با دستور مقابل فایل را مشاهده خواهیم کرد `sudo gedit /home/erfan/.bashrc` این تغییرات را در فایل وارد و فایل را `save` می کنیم.

```
# LD_LIBRARY_PATH
OTCL_LIB=/home/erfan/ns-allinone-2.34/otcl-1.13
NS2_LIB=/home/erfan/ns-allinone-2.34/lib
X11_LIB=/usr/X11R6/lib
USR_LOCAL_LIB=/usr/local/lib
export
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$OTCL_LIB:$NS2_LIB:$X11_LIB:$USR_LOCAL_LIB
# TCL_LIBRARY TCL_LIB=/home/erfan/ns-allinone-2.34/tcl8.4.18/library
USR_LIB=/usr/lib
export TCL_LIBRARY=$TCL_LIB:$USR_LIB
# PATH
XGRAPH=/home/erfan/ns-allinone-2.34/bin:/home/erfan/ns-allinone-
2.34/tcl8.4.18/unix:/home/erfan/ns-allinone-2.34/tk8.4.18/unix
#the above two lines beginning from xgraph and ending with unix should come on the same line
NS=/home/erfan/ns-allinone-2.34/ns-2.34/
NAM=/home/erfan/ns-allinone-2.34/nam-1.14/
PATH=$PATH:$XGRAPH:$NS:$NAM
```

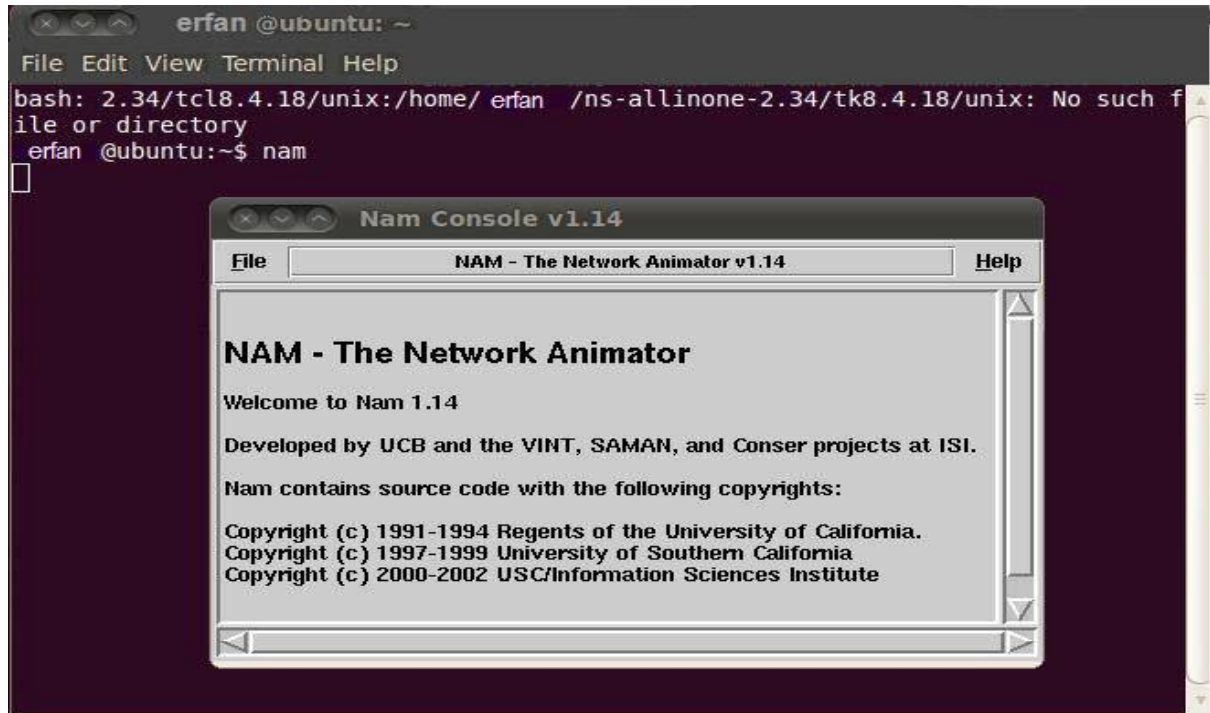
درگام بعد این دستورات را انجام می دهیم تا تغییرات اعمال شوند.

```
$ sudo su
# source /home/micman/.bashrc
```

حال Terminal را بسته و دوباره آن را باز می کنیم. اگر مشکلی وجود نداشته باشد ما با اجرای دستور زیر متوجه می شویم که با موفقیت مراحل نصب را انجام داده ایم.

nam

پس دستور را در همان خط اعلان Terminal وارد می کنیم که در شکل نیز نشان داده شده است.



شکل ۳-۱- تصویر خط اعلان Terminal

فصل چهارم

نتیجه گیری

نتیجه گیری

پژوهش‌های انجام شده کنونی در مورد راه‌حل‌های پیشنهادی هنوز از سیستم‌های تشخیص و جلوگیری از نفوذ ایده‌آل برای محاسبات ابری خیلی دورند. چون نه تنها فاقد ویژگی‌های مدنظر سیستم‌های تشخیص و جلوگیری از نفوذ هستند بلکه به ویژگی‌های سیستم‌های ابری دست نیافته‌اند، با این حال آنها می‌توانند ویژگی‌های الاستیکی، قابلیت اطمینان و دسترس پذیری پردازش ابری را تا حدی دارا باشد. کاربران محیط ابر نیازمند حفاظت از برنامه‌های کاربردی و داده‌های خود در برابر انواع مختلف حملات سایبری می‌باشند و در محاسبات ابری امنیت به عنوان سرویس از طریق ارائه دهنده در اختیار آنها قرار می‌گیرد ولی کنترل کامل روی مولفه‌های مختلف سرویس ارائه‌دهنده سیستم‌های تشخیص نفوذ را ندارند و نمی‌توانند سطوح امنیت را برای داده‌ها و برنامه‌های کاربردی خود سفارشی‌سازی نمایند.

با توجه به گستردگی محیط‌های ابری، سیستم تشخیص نفوذ می‌بایست قابلیت خود مدیریتی، خود انطباقی و یادگیری را داشته باشد و بتواند بدون نظارت انسان بر عناصر شبکه کنترل داشته و حملات غیرقابل پیش‌بینی را بصورت بلادرنگ تشخیص داده، عکس‌المعل مناسبی در قبال آنها داشته باشد. همچنین جهت ارائه یک محیط پردازش ابری امن، ارائه دهنده سرویس می‌بایست به مسائل امنیت داده، امنیت شبکه، جامعیت داده، امنیت برنامه کاربردی وب، دسترسی داده، احراز هویت و دیگر فاکتورهای مهم را در نظر بگیرد.

همانطور که پیش‌تر ذکر شد، پژوهش‌های مختلفی در زمینه تشخیص نفوذ صورت گرفته است و روش‌های متنوع تشخیص آنومالی و سوءاستفاده طراحی و پیاده‌سازی شده و در محیط محاسبات ابری بکار گرفته شده‌اند ولی همچنان قابلیت پیشگیری از نفوذ را در سیستم‌های پیشنهادی خود نادیده گرفته‌اند.

۴-۱- راه حل های پیشنهادی ممکن جهت حملات راهکارهای امنیتی رایانش ابری:

الف: راه حل حمله بسته SOAP (WrappingAttack)

همانطور که در حمله Wrap بیان شد مهاجم از طریق دستکاری بدنه بسته SOAP یا استفاده از IP معتبر به ابر حمله می کند. حال چنانچه سر پیام بسته فوق علامت گذاری شود دیگر مهاجم نمی تواند با ارائه IP معتبر به سرور عمل کند. این کار با استفاده از تعریف کلید RSA از طریق فراهم آورنده برای کاربر صورت می گیرد. معمول ترین و مشهورترین الگوریتم نامتقارن به عنوان RSA شناخته می شود.

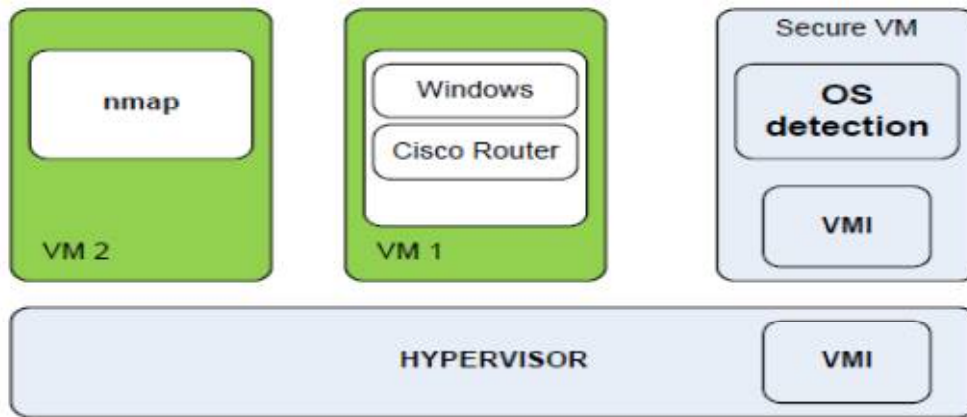
RSA مخفف حروف اول نام پدیدآورندگان آن است. می توان از یک سیستم نامتقارن برای نشان دادن اینکه فرستنده پیام همان شخصی است که ادعا می کند، استفاده کرد. این عمل اصطلاحاً امضای دیجیتال نام دارد. امضا، متن اصلی را با استفاده از کلید اختصاصی رمز می کند، رمزگشایی عملیات مشابهی روی متن رمز شده اما با استفاده از کلید عمومی است. برای تایید امضا بررسی می کنیم که آیا این نتیجه با اطلاعات اولیه یکسان است یا خیر. به بیان ساده تر چنانچه متنی از شخصی برای دیگران منتشر شود، این متن شامل متن اصلی و همان متن اما رمز شده توسط کلید اختصاصی همان شخص است. حال اگر متن رمز شده توسط کلید عمومی آن شخص که شما از آن مطلع هستید رمزگشایی شود، مطابقت متن حاصل و متن اصلی نشان دهنده صحت فرد فرستنده آن است، به این ترتیب امضای فرد تصدیق می شود. افرادی که از کلید اختصاصی این فرد اطلاع ندارند قادر به ایجاد متن رمز شده نیستند، به طوری که با رمزگشایی توسط کلید عمومی این فرد به متن اولیه تبدیل شود. بدین ترتیب فرد فرستنده نمی تواند منکر فرستادن متن شود، زیرا کسی به جز او نمی تواند آن متن را به شکل مطلوب امضا کند. در این صورت هر کاربر RSA منحصر به فرد خود را برای ارتباط با سرور در اختیار دارد.

ب: راه حل حمله از طریق کدهای مخرب (Malware-Injection)

هنگامی که کاربر حسابی را از طریق فراهم کنندگان سرویس ابر به خود اختصاص می دهد فراهم آورنده نهایی یک تصویر از ماشین مجازی کاربر در منبع تصویری سیستم ابر برای کاربر ساخته می شود.

پس از آن به هنگام ارسال درخواست سمت سرور از طریق کاربر برنامه های کاربردی کاربر به صورت شنیدن درخواست در حال اجرا و کاملاً یکپارچه بر روی ماشین مجازی قرار می گیرند. حال به دلیل دشوار بودن حمله به لایه زیرساخت به عنوان سرویس برای مهاجم، یکپارچگی فوق باید در سطح ماشین مجازی پیاده سازی شود. راه حل ارائه شده در این مقاله جهت مبارزه با ایجاد کدهای مخرب استفاده از جدول تخصیص فایل FAT است، که توسط همه سیستم عامل های موجود بر روی ماشین مجازی پشتیبانی می باشد. با کمک جدول تخصیص فایل می توان به برنامه در حال اجرای کاربر پی برد. با این کار تاریخچه برنامه در حال اجرای کاربر و مراحل قبل و بعد آن را می توان مشخص نمود. جهت تحقق این هدف به یک Hypervisor که روی سیستم نهایی پیاده سازی می شود نیاز خواهیم داشت.

همانطور که در شکل ذیل نشان داده شده است Hypervisor قرار گرفته شده بر روی سیستم انتهایی مسئول زمان‌بندی همه درخواست‌های در حال اجرای کاربر می‌باشد. باید به این نکته توجه داشت که قبل از زمان‌بندی درخواست‌ها کنترل یکپارچگی آنها از طریق جدول تخصیص فایل صورت می‌پذیرد. بنابراین با توجه به مطالب بیان شده می‌توان نتیجه گرفت که جدول تخصیص فایل جهت کنترل یکپارچگی یک برنامه در حال اجرای کاربر به کار برده می‌شود.



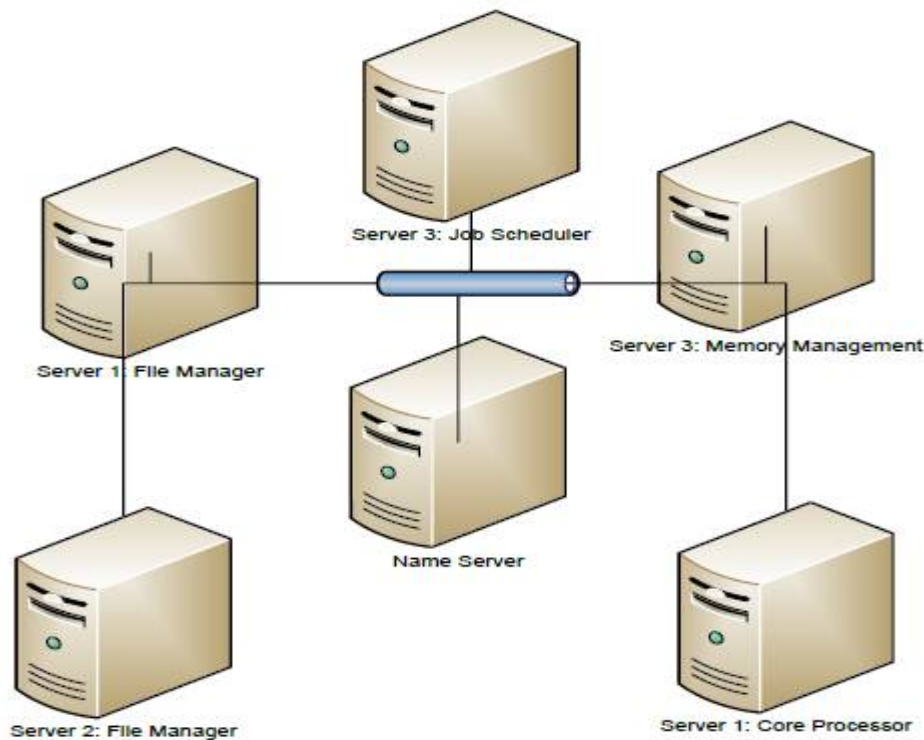
شکل ۴-۱- Hypervisor اجرای برنامه‌ها توسط

ج: راه حل حملات سیل آسا (Flooding Attack)

راه‌حل پیشنهادی برای مقابله با حملات سیل آسا ایجاد ناوگانی از سرورها همانند شکل زیر می‌باشد که در آن هر ناوگان جهت انجام کار خاصی در نظر گرفته شده است که با یکدیگر و سرور نام در ارتباط هستند. به طور مثال تعدادی از سرورها عمل مدیریت حافظه و تعدادی جهت مدیریت فایل در نظر گرفته می‌شوند. حال در این طراحی جدید چنانچه بار روی یک سرور بالا رود سرور جدید وارد عمل شده، بارگذاری جدید به آن منتقل شده و بدین ترتیب جهت جدول موجود در سرور نام به روز رسانی می‌شود.

د: راه‌حل سرقت اطلاعات (Data Stealing)

در پایان هر استفاده کاربر از ابر، ارائه دهنده ایمیلی حاوی میزان استفاده و مانده حساب را به کاربر ارسال می‌کند. بدین ترتیب کاربر اطلاعات کاملی را از سرویس‌گیری خود دریافت کرده و چنانچه سرقت اطلاعات از طریق مهاجمی صورت گیرد وی با بررسی حساب خود می‌تواند به آن پی ببرد.



شکل ۴-۲- پیام بین سرورها

۴-۲- معیارهای مقایسه مورد استفاده در شبیه سازی و ارتباط هریک از آنها به امنیت ابری به تفکیک

۴-۲-۱- معیار Delay Time

Delay Time یا نرخ تاخیر بین نودها شامل مواردی است که در آن مهاجم با به دست آوردن تاخیرهای مربوط به روترها و اعمال آن بر روی الگوی خاصی که خودش طراحی کرده یک خروجی را محاسبه و سعی در یافتن مکان سرور جهت نفوذ می نماید. در نتیجه هرچه میزان تاخیر (Delay) بالاتر برود قدرت نفوذ مهاجم بیشتر و امنیت پایین تر است.

۴-۲-۲- معیار Throughput Security

به معنی توان عملیاتی و در واقع متوسط نرخ ارسال موفق پکت ها در یک کانال ارتباطی از مبدا را بیان می کند. حال هرچه حجم و تعداد پکت های موفق بیشتر باشد در نتیجه سرور مجبور است توان و زمان پردازشی بیشتری را صرف احراز هویت این پکت ها بکند. در نتیجه هرچه توان عملیاتی (Throughput Security) بیشتر باشد میزان امنیت ممکن است کاهش یابد.

۴-۲-۳- معیار Response Time

به معنی زمان پاسخ دهی بین نودها از زمان ارسال یک پیام تا زمان دریافت پاسخ آن می باشد که این تایم بیش از حد کوتاه است و ممکن است بدلیل رسوخ بدافزار به پکت باشد که قبل از پردازش توسط سرور موجب ارسال پاسخ ساختگی شود بنابراین هرچه میزان زمان پاسخ دهی (Response Time) کمتر باشد امنیت نیز کاهش می یابد.

۴-۲-۴- معیار Traffic Ratio

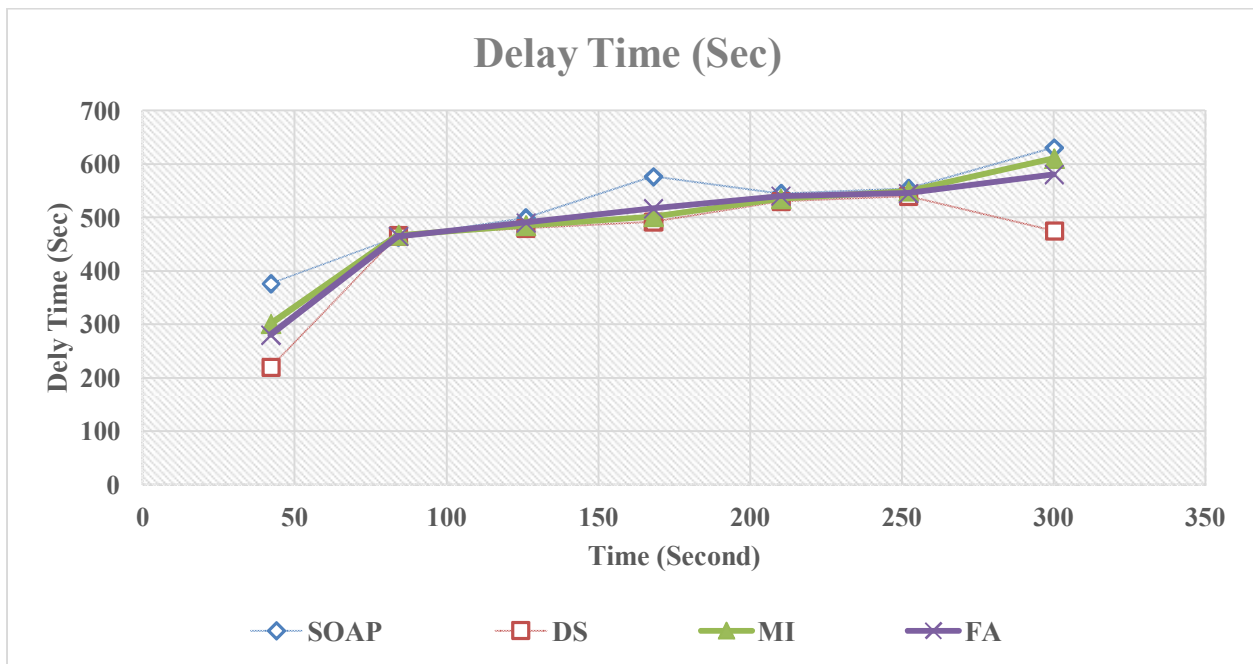
شامل مواردی است که در آن مهاجم یک ترافیک مصنوعی معادل 300 G/S بر روی سرور ایجاد می کند. در این حالت چندین هزار کامپیوتر در سراسر دنیا بدون اینکه متوجه باشند توسط این بدافزار شروع به تولید ترافیک مصنوعی کرده و سرور را کند یا بطور کلی از کار می اندازند. بنابراین هرچه ترافیک بیشتر باشد احتمال ترافیک مصنوعی نیز بیشتر و در نتیجه امنیت کمتر است. بزرگترین جمله تاریخ اینترنت مربوط به Cloud Fair نیز از طریق همین روش بوده است.

۴-۳-۳- نتایج به دست آمده از شبیه سازی راهکارهای امنیتی با نرم افزار NS2

۴-۳-۱- Delay Time (Sec): خروجی DE را برای چهار راهکار امنیتی را با زمان های مختلف از ۴۲ تا ۳۰۰ نشان می دهد.

Time (Sec)	SOAP	DS	MI	FA
42	376.317	220.082	301.215	280.191
84	463.871	466.461	467.402	464.801
126	499.486	480.548	485.345	490.501
168	576.886	492.054	501.752	517.201
210	545.357	530.145	535.213	540.357
252	554.633	540.412	549.601	545.633
300	630.841	475.571	610.452	580.841

جدول ۴-۱- مقایسه Delay Time چهار راهکار امنیتی با زمان های ۴۲ تا ۳۰۰



شکل ۴-۳- نمودار مقایسه Delay Time چهار راهکار امنیتی با زمان های ۴۲ تا ۳۰۰

همانگونه که در نمودار فوق ملاحظه می کنید بالاترین زمان تاخیر هر نود بین گره ها در ارسال و دریافت داده هر گره را در بین راهکارهای امنیتی راهکار حمله به بسته یا همان SOAP دارد و پس از آن به ترتیب راهکارهای حمله کدهای مخرب (MI)، حمله سیل آسا (FA)، حمله سرقت اطلاعات (DS).

۴-۳-۱- نتیجه گیری از شبیه سازی معیار Delay Time

با توجه به اینکه هرچه Delay Time یا تاخیر بین نودها در ارسال و دریافت بیشتر باشد در نتیجه امنیت کمتر است. لذا:

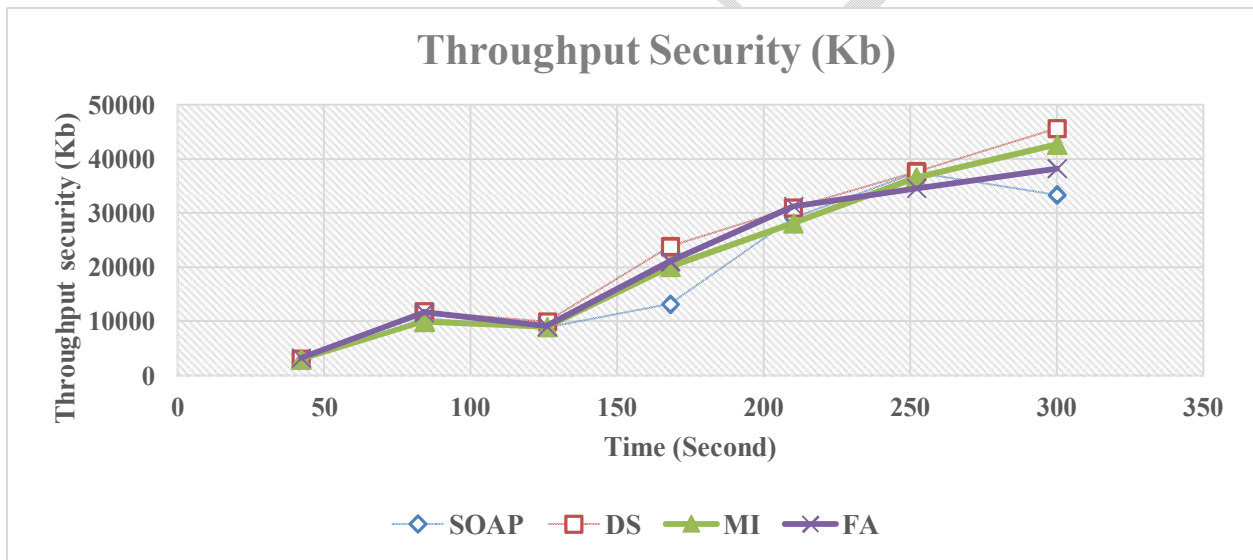
امتیاز	میزان امنیت	مقایسه معیار Delay Time
۰	کمترین	راهکار حمله به بسته
۴		راهکار حمله کدهای مخرب
۷		راهکار حمله سیل آسا
۱۰	بیشترین	راهکار حمله سرقت اطلاعات

جدول ۴-۲- نتیجه معیار مقایسه Delay Time

۴-۳-۲-Throughput Security (Kb): خروجی Throughput را برای چهار راهکار امنیتی را با زمان های مختلف از ۴۲ تا ۳۰۰ نشان می دهد.

Time (Sec)	SOAP	DS	MI	FA
42	3050	3136.63	3045.21	3293.64
84	10554.1	11820.84	10012.51	11701.1
126	8908.89	9991.21	9001.34	9099.78
168	13212.08	23842.82	20145.2	21056.85
210	29139.33	30990.54	28156.41	31286.13
252	37441.04	37658.87	36598.24	34589.64
300	33383.79	45599.51	42653.28	38256.15

جدول ۴-۳-مقایسه Throughput Security چهار راهکار امنیتی با زمان های ۴۲ تا ۳۰۰



شکل ۴-۴- نمودار مقایسه Throughput Security چهار راهکار امنیتی با زمان های ۴۲ تا ۳۰۰

همانگونه که در نمودار فوق ملاحظه می کنید بالاترین تعداد بسته ها که در واحد زمان بصورت موفقیت آمیز از مبدا فرستاده شده است را در بین راهکارهای امنیتی راهکار حمله سرقت اطلاعات (DS) دارد و پس از آن به ترتیب راهکارهای حمله کدهای مخرب (MI)، حمله به بسته (SOAP)، حمله سیل آسا (FA).

۴-۳-۱- نتیجه گیری از شبیه سازی معیار **Throughput Security**

با توجه به اینکه هرچه **Throughput Security** یا تعداد بسته‌هایی که در واحد زمان بصورت موفقیت آمیز از مبدا فرستاده می شود بیشتر باشد در نتیجه امنیت کمتر است. لذا :

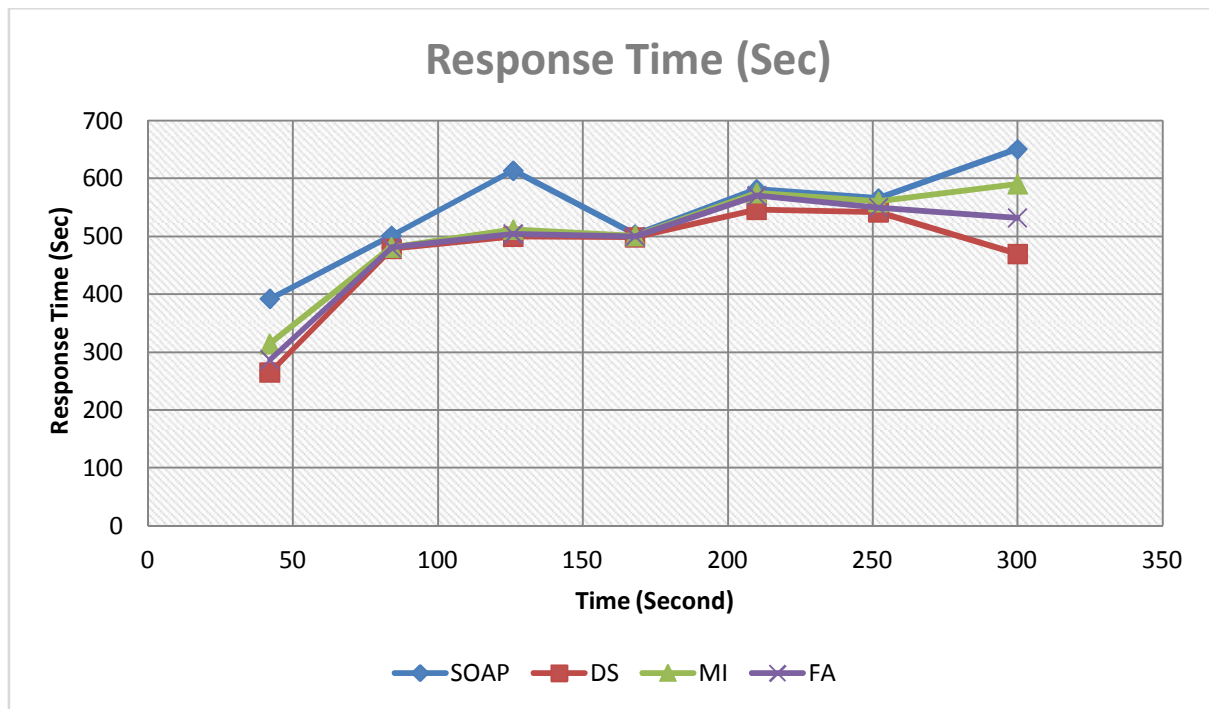
امتیاز	میزان امنیت	مقایسه معیار Throughput Security
۰	کمترین	راهکار حمله سرقت اطلاعات
۴		راهکار حمله کدهای مخرب
۷		راهکار حمله به بسته
۱۰	بیشترین	راهکار حمله سیل آسا

جدول ۴-۴- نتیجه معیار مقایسه **Throughput Security**

۴-۳-۳- **Response Time (Sec)**: خروجی E2E را برای چهار راهکار امنیتی را با زمان‌های مختلف از ۴۲ تا ۳۰۰ نشان می دهد.

Time (Sec)	SOAP	DS	MI	FA
42	392.451	265.156	314.325	287.194
84	501.205	478.494	481.412	480.801
126	613.487	499.354	512.146	504.211
168	503.215	498.254	501.12	500.021
210	581.285	546.248	575.202	570.302
252	565.701	542.214	560.032	549.708
300	650.705	470.128	590.401	532.081

جدول ۴-۵- مقایسه **Response Time** چهار راهکار امنیتی با زمان های ۴۲ تا ۳۰۰



شکل ۴-۵- نمودار مقایسه Response Time چهار راهکار امنیتی با زمان های ۴۲ تا ۳۰۰

همانگونه که در نمودار فوق ملاحظه می کنید بالاترین زمان پاسخ دهی بین نودها از زمان ارسال یک پیام تا زمان دریافت پاسخ آن را در بین راهکارهای امنیتی راهکار حمله به بسته یا همان SOAP دارد و پس از آن به ترتیب راهکارهای حمله کدهای مخرب (MI)، حمله سیل آسا (FA)، حمله سرقت اطلاعات (DS).

۴-۳-۳-۱- نتیجه گیری از شبیه سازی معیار Time Response

با توجه به اینکه هرچه Time Response یا زمان پاسخ دهی بین نود ارسالی و دریافت پاسخ بیشتر باشد در نتیجه امنیت بیشتر است. لذا:

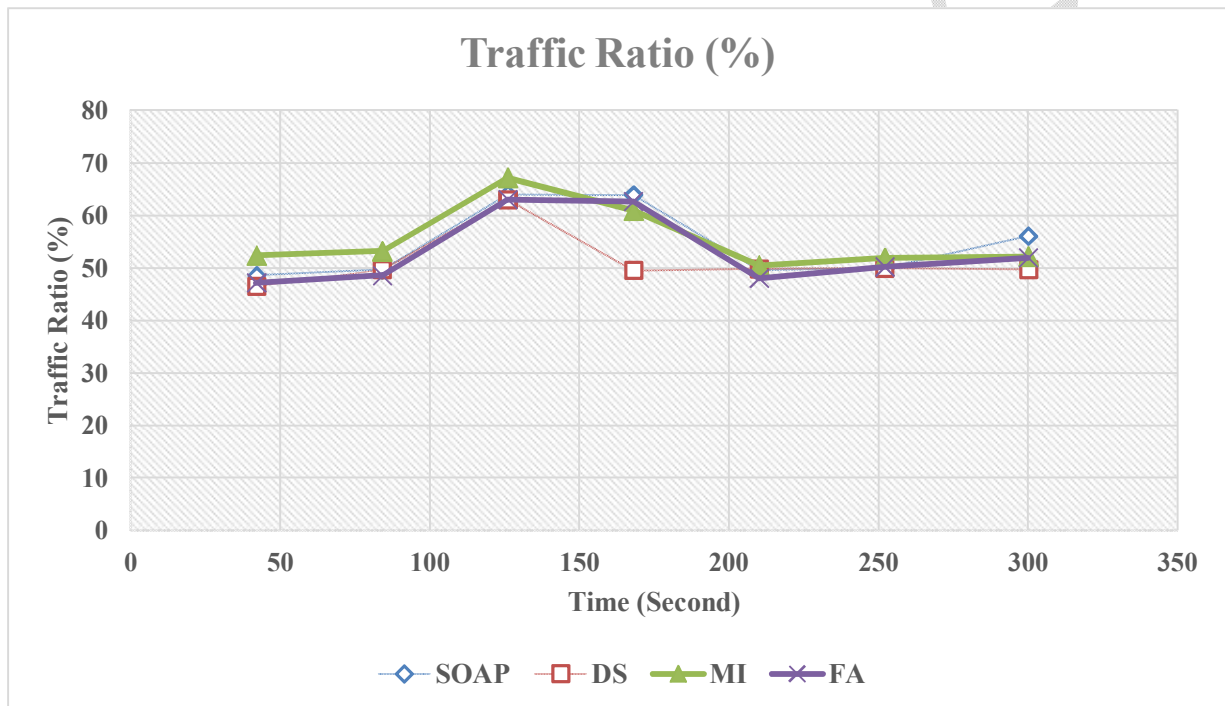
امتیاز	میزان امنیت	مقایسه معیار Time Response
۱۰	بیشترین	راهکار حمله به بسته
۷		راهکار حمله کدهای مخرب
۴		راهکار حمله سیل آسا
۰	کمترین	راهکار حمله سرقت اطلاعات

جدول ۴-۶- نتیجه معیار مقایسه Time Response

۴-۳-۴- **Packet Traffic Ratio (%)**: خروجی PDR را برای 4 راهکار امنیتی را با زمان های مختلف از ۴۲ تا ۳۰۰ نشان می دهد.

Time (Sec)	SOAP	DS	MI	FA
42	48.48	46.44	52.33	47.13
84	49.59	49.61	53.14	48.5
126	63.96	62.94	67.14	63.01
168	63.89	49.5	60.89	62.62
210	49.52	49.81	50.46	48.02
252	49.89	49.9	51.87	50.14
300	56.01	49.65	52.14	51.92

جدول ۴-۷- مقایسه Packet Traffic Ratio چهار راهکار امنیتی با زمان های ۴۲ تا ۳۰۰



شکل ۴-۶- نمودار مقایسه Packet Traffic Ratio چهار راهکار امنیتی با زمان های ۴۲ تا ۳۰۰

همانگونه که در نمودار فوق ملاحظه می کنید بالاترین نرخ تحویل بسته، درصدی از بسته ها که با موفقیت در مقصد دریافت شده است را در بین راهکارهای امنیتی راهکار حمله سیل آسا (FA) دارد و پس از آن به ترتیب راهکارهای حمله به بسته یا همان SOAP، حمله کدهای مخرب (MI)، حمله سرقت اطلاعات (DS).

۴-۳-۱- نتیجه گیری از شبیه سازی معیار Traffic Ratio

با توجه به اینکه هرچه Traffic Ratio یا تعداد بسته هایی که در واحد زمان بصورت موفقیت آمیز در مقصد دریافت می شود بیشتر باشد در نتیجه امنیت کمتر است. لذا :

امتیاز	میزان امنیت	مقایسه معیار Traffic Ratio
۰	کمترین	راهکار حمله سیل آسا
۴		راهکار حمله به بسته
۷		راهکار حمله کدهای مخرب
۱۰	بیشترین	راهکار حمله سرقت اطلاعات

جدول ۴-۸- نتیجه معیار مقایسه Traffic Ratio

۴-۴- نتیجه گیری کلی از شبیه سازی و مقایسه راهکارهای امنیتی ابر

امتیاز	میزان امنیت	مقایسه بر اساس مجموع هر چهار معیار
۲۲	بیشترین	راهکار حمله کدهای مخرب
۲۱		راهکار حمله به بسته
۲۱		راهکار حمله سیل آسا
۲۰	کمترین	راهکار حمله سرقت اطلاعات

جدول ۴-۹- نتیجه کلی مقایسه معیارها

فصل پنجم

جمع بندی و پیشنهادات

جمع بندی

محاسبات ابری در آینده توجه بسیاری از کاربران و شرکت‌ها را بسوی خود جلب خواهد کرد. خیلی از سازمانها مایل به مهاجرت به ابر جهت کاهش هزینه‌ها و استفاده از مزایای آن هستند. فراهم کنندگان سرویس ابر باید برای جذب تعداد کاربر بیشتر به مسائل مرتبط با حفظ حریم خصوصی که یکی از دغدغه‌های کاربران در محاسبات ابری می باشد توجه بیشتری نموده و مسائل پیش رو مرتبط با حفظ حریم خصوصی را در نظر بگیرند.

۵-۱- حفاظت از داده‌ها

فراهم کنندگان سرویس ابر باید در مورد محافظت از داده‌ها پاسخگو باشند و این اطمینان خاطر را به کاربران بدهند که به کمک تکنیک‌های رمزگذاری از داده‌های آنها محافظت می شود.

۵-۲- مکان فیزیکی

کاربران ابر این حق را دارند که از محل ذخیره‌سازی داده‌هایشان اطلاع داشته باشند، لذا فراهم کننده سرویس ابر باید اطلاعات لازم در این خصوص را در اختیار کاربران قرار دهد.

۵-۳- از بین رفتن داده‌ها

فرض کنیم اگر داده‌های کاربران از بین بروند، فراهم کننده سرویس ابر باید مسئولیت این خطا را بپذیرد و رضایت او را جلب نماید.

۵-۴- کنترل دسترسی

فراهم کننده محاسبات ابر باید مکانیزم‌های لازم را جهت جلوگیری از دسترسی‌های غیرمجاز به داده‌های کاربران را در نظر بگیرد.

۵-۵-قوانین حفظ حریم خصوصی

همانطوریکه بیان شد مفهوم حریم خصوصی در میان جوامع و کشورهای مختلف، متفاوت می‌باشد لذا فراهم کننده محاسبات ابر باید کل قوانین مربوط به حفظ حریم خصوصی که از آن پیروی می‌کند را به کاربر بطور شفاف بیان کند.

۵-۶-پیشنهادهای برای بهبود حفظ حریم خصوصی

۵-۶-۱- برای کاربران ابر

کاربران ابر باید قبل از ذخیره‌سازی داده‌هایشان در ابر، به دقت سیاست‌های حفظ حریم خصوصی ارائه شده توسط فراهم کننده سرویس محاسبات ابری را مطالعه نمایند.

اگر کاربر هر یک از سیاست‌ها را به وضوح درک نکند (شفاف نباشد) کاربر باید از ارائه کننده ابر بخواهد با توضیحات بیشتر او را توجیه کند.

کاربران محاسبات ابری باید درک کاملی از حقوق مربوط به استفاده، افشاء و استفاده خصوصی از داده‌های خود را داشته باشد.

فرض کنید کاربر می‌خواهد داده‌های خود را از ابر جابجا کند سرویس دهنده ابر باید اقدامات و همکاری لازم را انجام دهد (کاربر ابر باید از تعهدات سرویس دهنده ابر کاملاً آگاه باشد)، کاربر ابر این حق را دارد که پس از جابجایی داده‌هایش بررسی‌های لازم را جهت حذف کامل اطلاعات از فراهم کننده سرویس ابر قبلی را انجام دهد. به کاربران محاسبات ابری پیشنهاد می‌شود از گذاشتن اطلاعات سری یا تجاری مهم در ابر حد امکان خوداری نمایند.

۵-۶-۲- برای سرویس دهنده های ابر

۱- سرویس دهنده ابر باید مطمئن شود که هیچ گونه سیاست حفظ حریم خصوصی را نقض نمی‌کند.

۲- سرویس دهنده ابر باید به مکان فیزیکی داده‌های کاربران توجه بیشتری نمایند و امنیت لازم را فراهم سازند.

۳- سرویس دهنده ابر باید مکانیزم حفاظت از داده‌های کاربر را برای کاربر بیان کند و این اطمینان را به او بدهد که به نحوه احسن از داده‌های او محافظت می‌کند.

۴- سرویس دهنده ابر باید مکانیزمی را برای بازگرداندن اطلاعات کاربر مخصوصاً در موقعی که کاربر رمز عبور خود را فراموش کرده داشته باشد (پیشنهاد می‌شود که برای ریکاوری از حداقل سه مرحله استفاده کند: ۱- با پرسیدن اطلاعاتی که قبلاً از کاربر گرفته ۲- ارسال کد امنیتی به ایمیل یا موبایل کاربر ۳- ریست پسورد و گرفتن پسورد جدید).

۵- سرویس دهنده ابر باید لیست قوانین و قطعنامه‌های بین‌المللی که از آنها در حفظ حریم خصوصی حفاظت می‌کنند و این سرویس دهنده ملزم به اجرای آن است را به کاربر نشان دهند (مثل قطعنامه مادرید (۲۰۰۹) یا قطعنامه حفظ حریم خصوصی داده‌های کاربر در اروپا)

۶- سرویس دهنده ابر باید این تضمین را به کاربر بدهد که تحت هیچ فشاری اطلاعات او را به دولت‌ها یا افراد دیگری نخواهند داد.

۷- فراهم کننده ابر در صورت تغییر قوانین مربوط به حفظ حریم خصوصی بلافاصله کاربران را از این تغییرات آگاه سازد.

- [1] Ahmed Patel , M.T., K Bakhtiyari , J Celestino Junior, An intrusion detection and prevention system in cloud computing: A systematic review. Journal of Network and Computer Applications, 2013.
- [2] Amirreza Zarrabi, Alireza Zarrabi. "Internet Intrusion Detection System Service in a Cloud." IJCSI International Journal of Computer Science Issues 9 (September 2012).
- [3] Abdul Nasir Khan, M.L. Mat Kiah , Samee U. Khan, Sajjad A. Madani. "Towards Secure Mobile Cloud Computing: A Survey." Future Generation Computer Systems (11 August 2012): 22.
- [4] K Scarfone, P Mell. "Guide to Intrusion Detection and Prevention Systems ." edited by Commerce, 127. U.S. Department of Commerce: National Institute of Standards and Technology(NIST), 2007.
- [5] Irfan Gul, M. Hussain. "Distributed Cloud Intrusion Detection Model." International Journal of Advanced Science and Technology 34 (September, 2011).
- [6] C Modi, D Patel, H Patel, B Borisaniya, A Patel, M Rajarajan. "A Survey of Intrusion Detection Techniques in Cloud." Journal of Network and Computer Applications (2012): 14.
- [7] Chunming Rong , Son T. Nguyen , Martin Gilje Jaatun "Beyond Lightning: A Survey on Security Challenges in Cloud Computing." Computers and Electrical Engineering (2012).
- [8] Niroshinie Fernando , Seng W. Loke , Wenny Rahayu. "Mobile Cloud Computing: A Survey." Future Generation Computer Systems (2012): 23.
- [9] CENTRE, CYBER SECURITY OPERATIONS. "Cloud Computing Security Considerations." edited by Department of Defence: Australian Government, 2012.
- [10] Dhage, Sudhir N. "Intrusion Detection System in Cloud Computing Environment." Int. J. Cloud Computing 1 (2012): 22.
- [11] Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande. "Intrusion Detection System for Cloud Computing." International Journal of Scientific & Technology Research 1, no. 4 (May 2012): 5.
- [12] G.Hemaprabha, Visalatchi.R. "Intrusion Detection for Smart Phone Using Cloud." International Journal of Computational Engineering Research (
- [13] Hassen Mohammed Alsafi , Wafaa Mustafa Abdullallah and Al-Sakib Khan Pathan.: An Integrated Intrusion Handling Model for Cloud Computing Environment."
- [14] A. K. Ghosh, A Schwartzbard, M Schatz. "Learning Program Behavior Profiles for Intrusion Detection
- [15] Basappa B. Kodada, Ramesh Nayak, Raghavendra Prabhu, Suresha D. "Intrusion Detection System inside Grid Computing Environment (Ids-Igce)." International Journal of Grid Computing & Applications (IJGCA) 2 (No.4, December 2011): 10.

- [16] Herve' Debar, Marc Dacier , Andreas Wespi. "Towards a Taxonomy of Intrusion-Detection Systems." Computer Networks (1999): 18.
- [17] Irfan Gul, M. Hussain. "Distributed Cloud Intrusion Detection Model." International Journal of Advanced Science and Technology 34 (September, 2011).
- [18] Jayaraj Poroor, Bharat Jayaraman. "C2I: A Formal Policy Language for Secure Cloud Configurations." In The 3rd International Conference on Ambient Systems, Networks and Technologies(ANT): Elsevier Ltd., 2012.
- [19] Loganayagi.B , S.Sujatha. "Enhanced Cloud Security by Combining Virtualization and Policy Monitoring Techniques." In The International Conference on Communication Technology and System Design 2011: Elsevier Ltd., 2011.
- [20] M KUZHALISAI , G GAYATHRI. "Enhanced Security in Cloud with Multi-Level Intrusion Detection System." International Journal of Computer & Communication Technology (IJCCT) 3 (2012): 4.
- [21] Md. Tanzim Khorshed, A.B.M. Shawkat Ali , Saleh A. Wasimi. "A Survey on Gaps, Threat Remediation Challenges and Some Thoughts for Proactive Attack Detection in Cloud Computing." Future Generation Computer Systems 28 (18 January 2012 2012): 19.
- [22] N Nagenthiran , R Jayasekara , S Jayasekara. "Intrusion Detection & Intrusion Prevention Systems." 26, 2010.
- [23] Niroshinie Fernando , Seng W. Loke , Wenny Rahayu. "Mobile Cloud Computing: A Survey." Future Generation Computer Systems (2013 2012): 23.
- [24] Roesch, Martin. "S N O R T — L I G H T W E I G H T I N T R U S I O N D E T E C T I O N F O R N E T W O R K S." Paper presented at the Proceedings of LISA '99: 13th Systems Administration Conference, Seattle, Washington, USA, November 7–12, 1999 1999.
- [25] Yizhang Guan, Jianghong Bao. "A Cp Intrusion Detection Strategy on Cloud Computing." Paper presented at the Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09), Nanchang, P. R. China, May 22-24, 2009.
- [26] D Anderson, T Frivold , A Valdes. "Next-Generation Intrusion Detection Expert System (Nides)a Summary." 1995.
- [27] Anup." Paper presented at the Proceedings of the Workshop on Intrusion Detection and Network Monitoring, Santa Clara, California, USA, April 9–12, 1999 .
- [28] ALHARKAN, T., IDSAAS: INTRUSION DETECTION SYSTEM AS A SERVICE IN PUBLIC CLOUDS, 2013: Kingston, Ontario, Canada.
- [29] Al-Hoby, M.O., Intrusion Detection Management as a Service in Cloud Computing Environments, 2011.

- [30] Neethu Mariam, Joseph ,Esther Daniel ,N. A. Vasanthi,” Survey on privacy -Preserving Methods for Storage in Cloud Computing
- [31] Siani Pearson, “Taking Account of privacy When Designing Cloud Computing Services”, HP Laboratories, Tech. Rep. HPL- 2009-54, 2009
- [32] Niroshinie Fernando, Seng W. Loke , Wenny Rahayu , “Mobile cloud computing A survey”,journal Elsevier ,Future Generation Computer Systems 29 (2013) 84–106
- [33] “Cloud Security and privacy An Enterprise Perspective on Risks and Compliance” By Tim Mather, Subra Kumaraswamy, Shahed Latif, Publisher O'Reilly Media Released September 2009 First Edition
- [34] Zhifeng Xiao and Yang Xiao,” Security and privacy in Cloud Computing “ , 1553-877 IEEE 2012
- [35] kowsalyadevi prakash , “ A Survey On Security And privacy In Cloud Computing “ , International Journal of Engineering Research & Technology (IJERT) ISSN 2278-0181 Vol. 2 Issue 2, February- 2013
- [36] jian wang ,yan zhao,shuo jiang,jiajin le , “providing privacy preserving in cloud computing “978-1-4244-7562-9/10/\$26.00 ©2010 IEEE
- [37] Rajeev Bedi, Mohit Marwaha, Tajinder Singh, Harwinder Singh, and Amritpal Singh”ANALYSIS OF DIFFERENT privacy PRESERVING CLOUD STORAGE FRAMEWORKS”, International Journal of Computer Science & Information Technology (IJCSIT) Vol 3, No 6, Dec 2011
- [38] Ruangchaijatupon, P. Krishnamurthy,"Encryption and Power Consumption inWireless LANs-N,” The Third IEEEWorkshop on Wireless LANs –September 27-28, 2001- Newton, Massachusetts.
- [39] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall , 2005,PP. 58-309 .
- [40] N Nagenthiran , R Jayasekara , S Jayasekara. "Intrusion Detection & Intrusion Prevention Systems." 26, 2010.
- [41] Al-Hoby, M.O., Intrusion Detection Management as a Service in Cloud Computing Environments, 2011.
- [42] Siani Pearson, “Taking Account of privacy When Designing Cloud Computing Services”, HP Laboratories, Tech. Rep. HPL- 2009-54, 2009
- [43] “Cloud Security and privacy An Enterprise Perspective on Risks and Compliance” By Tim Mather, Subra Kumaraswamy, Shahed Latif, Publisher O'Reilly Media Released September 2009 First Edition
- [44] <http://fa.wikipedia.org>
- [45] <http://pariyana.com/id/about-cloud-computing-01>

[46] <http://www.webopedia.com/TERM/S/SSL.html>

[47] <http://www.fekrinejat.com>

[48] <http://www.hamkelasy.com>

[49] <http://www.wikipedia.com>

[50] <http://www.sgnetway.com>

منابع
پایان
پژوهش

Abstract

according to the future of cloud computing and its applications and the benefits of this technology, has also

challenges for users, one of the most controversial and the challenges of privacy. according to data storage and private users of commercial companies in cloud computing, privacy is a very important for the users of cloud computing and cloud of service providers. of the four major attack cloud attacks, which includes the torrential attack, an attack on a package of malicious code, and stealing information that at the beginning of the attacks and ways of dealing with them and, ultimately, the report we are using the simulation four security strategy proposed cloud computing NS2 in software and compare the results achieved to consider the issues of privacy in the clouds and the challenges ahead and proposals for users and providers.

Keywords

cloud computing, security, privacy, detection systems, digital signature



ISLAMIC AZAD UNIVERSITY

SCIENCE AND RESEARCH BRACH

**Faculty of Technology and Engineering Department of Computer
Thesis for receiving «M.Sc» degree on Software**

Subject:

Evaluate, compare and simulation security solutions in cloud computing

Thesis Advisor:

M.Mousavi Ph.D.

Consulting Advisor:

H.Naderi Ph.D.

By:

Erfan Niazi

Summer 201۴