بسم الله الرحمن الرحیم

پژوهشکده

فناوری اطلاعات و ارتباطات

عنوان طرح:

توسعه و پیاده سازی سامانه ی تماس مقیاس پذیر

گزارش فاز دوم

مجری: محمد تقی پور

ویرایش: اول

تاریخ تهیه: اسفند 1395

پیشگفتار

جامعه بشری شاهد سیر تکامل در حوزه های مختلف از جمله دوران ماقبل تاریخ به جامعه کشاورزی، سپس جامعه صنعتی و فرا صنعتی بوده است. در عرصه مخابرات نیز روال به هم این صورت بوده و با تغییرات و تحولات شگرفی روبرو بوده است. مخابرات و سیستم های مخابراتی دیگر نه به عنوان ابزاری برای ارائه سرویس سنتی تلفن بلکه حلقه ای از زنجیره ی تولید و پردازش، انتقال و ذخیره و بازیابی اطلاعات است. پیشرفت های انجام گرفته در زمینه صنعت الکترونیک، روشهای پردازش، علوم کامپیوتر، تکنیکهای نرم افزاری وسیستم های دیجیتال حاکی از آن است که دیگر نمی توان مرز مشخصی بین کامپیوتر ومخابرات قائل بود و این دو در هم آمیخته شده و عصر نوینی را در زندگی بشر رقم زده اند. حال گذر به سیستم های دیجیتال نسبت به سیستم های آنالوگ قدیمی شبکه های PSTN خود دارای مزیت هایی از جمله سهولت در پیاده سازی با فناوری های مدرن، یکپار چگی سیستم های انتقال و سوئیچینگ ، مصونیت در برابر تداخل، سهولت در بازسازی و رمز کردن سیگنال می باشد.

از جهش های سرویس های تلفنی، سیستم های پاسخگویی تلفنی می باشد که توانسته سرمایه گزاران تجاری را به این حوزه جذب کند. از چشم اندازهای این حوزه، توسعه سامانه IVR پیشرفته مبتنی بر نیاز کاربر است که بتوان جزیره های مجزای سرویس های الکترونیکی را به یکدیگر متصل نمود. بدین ترتیب پژوهشکده فناوری اطلاعات و ارتباطات جهاد دانشگاهی با توجه به سوابق خود در این حوزه، پای در توسعه این فناوری نهاده است. بر همین اساس پس از مطالعه ی میدانی در این حوزه و پیاده سازی نرم افزارهای متن باز مختلف، به مقایسه و ارزیابی ویژگی‌های هرکدام بپردازیم. سپس به صورت عملیاتی طرح منتخب را پیاده سازی، اصلاح و تکمیل نماییم.

این گزارش براساس طرح مصوب، حاوی نتایج اولیه مطالعات، راه اندازی و پیاده سازی راهکارهای متن باز در زمینه سیستم های IVR مبتنی بر VOIPاست. بدیهی است با عملیاتی شدن و کسب تجربه در کار با نرم افزارهای متن باز، به نقاط ضعف و قوت شفاف تری دست خواهیم یافت.

پژوهشکده فناوری اطلاعات و

ارتباطات جهاددانشگاهی (ICT)

فهرست مطالب

فهرست شکل ها

فهرست جداول

1. مقدمه

پیرو فعالیت های انجام گرفته در مقطع اول پروژه توسعه و پیاده سازی سامانه ی تماس مقیاس پذیر، تحقیقات عملیاتی با نگرش بوجود آوردن ظرفیت اجرای پروژه های مختلف کارفرمایی بزرگ، در کنار ارائه سرویس های مبتنی برVOIP به شرکتهای کوچک و متوسط انجام گرفت. حال در این مقطع نهایی به تهیه محصولی بومی سازی شده می‌پردازیم.

در مقطع قبل مطالعات تطبیقی حول فن آوری های روز سیستم های IVR مبتنی بر VOIP انجام گرفت. نرم افزارهای متن باز مختلف مورد بررسی و تحلیل قرار گرفت و به نقاط ضعف و قوت هریک دست یافتیم (تمامی نتایج مقایسه در گزارش فاز اول لیست گردید). حال در مقطع دوم پروژه به طراحی سیستمی پرداخته شد که بتواند جوابگوی نیازها و چالش های پیش رو در ارائه سرویس های IVR باشد.

به همین خاطر به تحلیل و بررسی اجزای مختلف سیستم، با توجه به تجربیات و نتایج مندرج در مقالات و متون معتبر علمی پرداخته شد. از سوی دیگر با مشاوره متخصصین داخلی، سعی به کسب تجربیات عملیاتی پروژه های مقیاس بزرگ گردید. بدین ترتیب با بررسی های انجام شده، ویژگی های محصول بومی سازی شده مدنظر قرار گرفت. پلتفرم های مختلف نیز مورد بازبینی قرار گرفت که نتایج آن در فصول پیش روی آورده شده است. راهکارهای مبتنی بر VOIP مختلف که در پروژه های مختلف پیشنهاد شده نیز مورد مطالعه قرار گرفت. در آخر به پیاده سازی سیستم مورد نظر در پژوهشکده اقدام گردید.

برای پیاده سازی نیازهای سخت افزاری مانند مودم و خط SIP Trunk که با درخواست و پیگیری مکرر با پیش شماره "43416" از طرف مخابرات به پژوهشکده فناوری اطلاعات و ارتباطات اختصاص داده شد. سپس به محک سیستم مورد نظر پرداخته شد. بدیهی است، توسعه و راه اندازی پایلوت سیستم ، تست و بررسی سامانه و اصلاح مشکلات احتمالی بدنبال دارد و به اصلاح و منطبق سازی محصول با ویژگی ها و نیازمندیهای کشور پرداخته شد.

2. نگاهی اجمالی بر نتایج مقطع اول

1,2 رویکردها و اهداف کلی مقطع اول

به منظور ارائه سرویس های IVR سرور تماس ، بایستی پلتفرمی جامع با مجموعه ای از ویژگیهای مختلف طراحی شود. ویژگیهای مربوطه بایستی توانایی پوشش نیازهای مختلف را داشته باشند. در این مرحله، به بررسی کلی محصولات انتخاب شده پرداخته شد و ویژگیهای کلی این محصولات با توجه به مطالب ارائه شده در وب سایت ها استخراج شد. ویژگهای استخراج شده تحت لیستی که نشان دهنده نقاط قوت و ضعف هر یک از محصولات می باشد، ارائه شد. این لیست حاوی قابلیت ها و ویژگیها پلتفرم های مختلف پرتال صوتی بود.

سپس بررسی عمیق تری بر روی محصولات منتخب انجام شد و با توجه به مجموعه عملکردها و ویژگیهای آنها، مطالعه عمیق تری درباره این محصولات انجام شد. این مطالعه نمایانگر این حقیقت بود که کدام محصول یا محصولات توانایی ارائه ویژگیهای مذبور را در پایلوت عملیاتی دارند. در این میان ویژگیهای بالقوه آنها با ویژگیهای محیط عملیاتی مورد بررسی قرار گرفت. سپس بر اساس کارایی ارائه شده این محصولات در محیط تست، یک محصول به عنوان برترین کاندید انتخاب گردید. البته لازم به ذکر است که محصول انتخاب شده از منظر قابلیت انعطاف کافی برای توسعه نیز مورد بررسی قرار گرفت.

2,2 نتایج تحقیقاتی و پژوهشی مقطع اول

در میان مقالات معتبر در این حوزه پژوهشی 14 مقاله به عنوان مقالات پژوهشی برتر که دارای نوآوری و طرح معماری قابل توجهی هستند انتخاب شد و به بررسی آنها پرداخته شد. برخی مقالات سرویس دهی بهداشتی و آموزشی خاصی را مدنظر قرار داده بودند که یک سامانه ارائه میشود که نقش یک یادآور را بازی مینماید و بازخوردهای بلادرنگی را در زمانهایی که بیمار باید رژیم دارویی مشخصی را رعایت نماید، در اختیار ارائه دهندگان خدمات مراقبتی قرار میدهد. همچنین مقالات دیگری در مورد سامانه‌های پاسخ صوتی تعاملی را جهت کاربرد در صنایع مختلف مانند ارتباطات راه‌دور و بانکداری مورد بررسی قرار دادند.

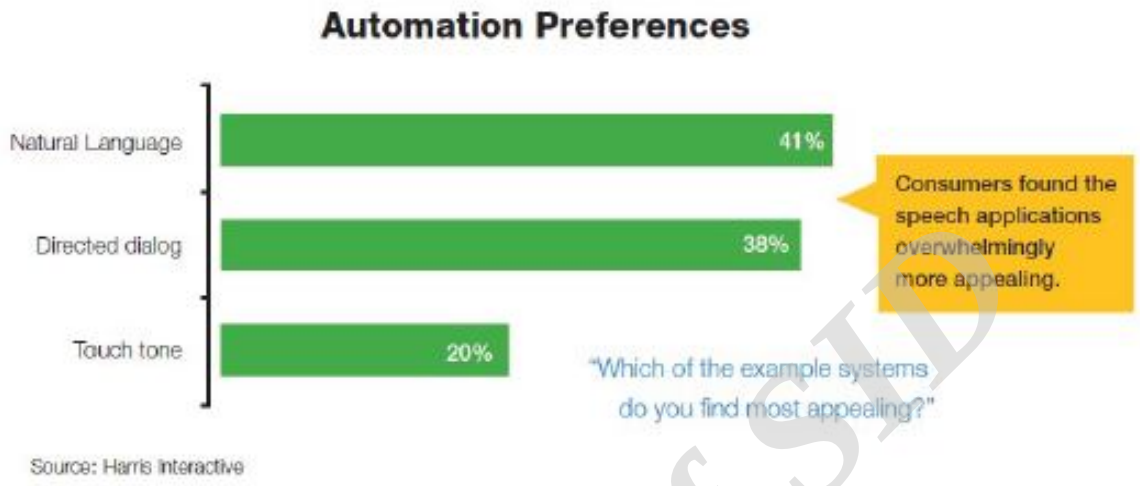
تعدادی از مقالات نیز به مباحث ساختاری و طراحی معماری سامانه با روش هایی مانند شبکه عصبی پرداخته بودند. حتی مقاله هایی به لایه های زیرین توجه بیشتری داشتند و اصل ایده خود را بر بهبودی و کارامدی هرچه بیشتر لایه‌های زیرین مانند آشکارساز کلید، ضبط‌کننده ومدیریت مکالمه قرار دادند. بنابراین از مهمترین اهداف طراحی این سامانه ها این است که کاربردهای سامانه پاسخ صوتی تعاملی در دامنه‌های مختلف باید قادر به اشتراک‌گذاری منابع موجود در لایه‌های زیرین باشند. همچنین برخی دیگر از محققین توجه خود را معطوف به یک سامانه پاسخ صوتی تعاملی شخصی‌سازی‌شده به منظور ارائه‌ی خودخدمتی به مشتریان نمودند. در این سامانه ها ، مشتری قادر است منوی سامانه‌ی خود را بر اساس نیازهای خود سفارشی نماید.

در این بخش نتایج چندین مقاله که در سال های اخیر به تحلیل کاربردهای عملی سیستم IVR پرداخته اند مورد بررسی قرار می گیرد:

در یکی از مقالات پیاده سازی مبتنی بر تکنولوژی IVR و امکان سرویس دهی به مشتری را به صورت 24 ساعته مورد بررسی قرار دارد. با وجود قابلیت های بسیار در سیستم IVR ، برای وارد کردن اطلاعات در این سیستم نیازمند استفاده از کلیدهای تلفن هستیم که این موضوع باعث ایجاد محدودیت در نوع اطلاعات ورودی می شود. به همین دلیل ممکن است مشتری ها ترجیح بدهند که به جای استفاده از سرویس IVR مستقیماً با یک منشی صحبت کنند.نیاز به صحبت با یک فرد، به خصوص در کشورهایی که دارای چندین زبان هستند بیشتر احساس می شود و پیاده سازی آن دشوارتر به نظر می رسد.راهکار IVR مبتنی بر صحبت نه تنها تمامی مزایای IVR سنتی را دارند بلکه قابلیت مقیاس پذیری و انطباق در شرایط نیاز به چندین زبان را هم فراهم می کنند.

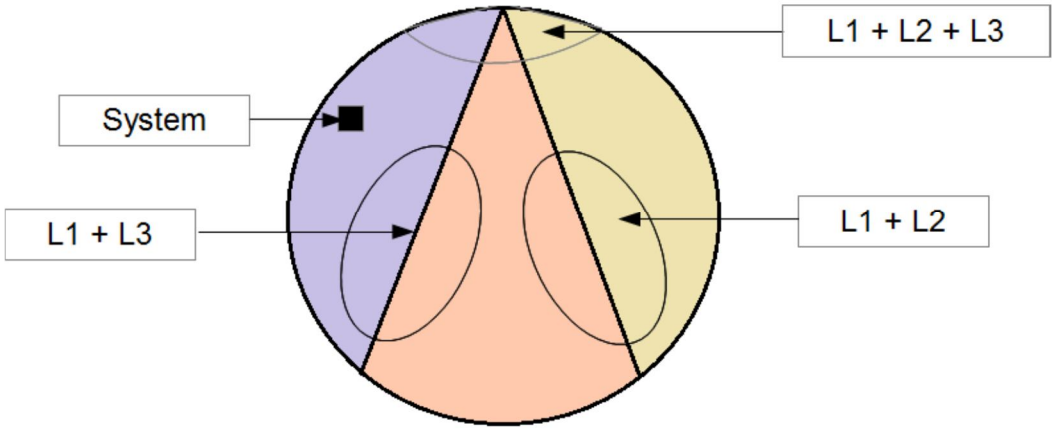
شرکت هایی که مشتریان زیادی دارند به طور پیوسته در جستجوی روشی هستند که شیوه ی ارتباطات خود با مشتریان را از نظر کیفیت و سرعت پاسخگویی با کمترین هزینه بهبود ببخشند.در چنین شرایطی، پلتفرم های IVR مبتنی بر صحبت بهترین گزینه هستند.این سیستم ها با وجود برتری در زمینه ی قابلیت دسترسی 24 ساعته و در تمام روزهای هفته، دارای نقصی هستند که آن هم عدم امکان برخی اطلاعات به صورت شماره و از طریق دکمه های تلفن است.در مقایسه با سیستم IVR سنتی، سیستم IVR مبتنی بر صحبت نه تنها قادر است کارهای پیچیده تری را مدیریت کند بلکه با ساده سازی عمل ارسال اطلاعات برای

کاربر، سطح customer experience را ارتقا می دهد.شکل زیر به وضوح نشان گر این است که کاربران تمایل بیشتری نسبت به IVR مبتنی بر صحبت در مقایسه با IVR سنتی دارند:



شکل*2-1* ترجیح کاربران در استفاده از سیستم های IVR مختلف

به وضوح در کشورهایی که به چندین زبان صحبت می شود با یک سیستم واحد نمی توان تمامی نیازها را برطرف نمود چرا که پیاده سازی این امر نیازمند سیستمی بسیار پیچیده است. پیچیدگی بیشتر زمانی حاصل می گردد که چندین زبان به صورت ترکیبی مورد استفاده قرار بگیرند.به عنوان مثال L_1 و L_2 و L_3 سه زبان مختلف‌اند که در مناطق مختلف یک کشور با آن ها صحبت می شود. طراحی سیستمی که بتواند همه ی این زبان ها را پوشش به طور همزمان پوشش بدهد با توجه به پیشرفت گسترده ی حوزه ی تشخیص گفتار کار سختی نیست اما مناسب به نظر نمی رسد. به عنوان مثال با توجه به شکل 2– 2 در همه ی حالت ها همواره بین زبان ها در نواحی مرزی هم پوشانی وجود دارد.همچنین علاوه بر چالش های مربوط به زبان، در زمینه ی افراد و تکنولوژی مورد استفاده نیز چالش هایی وجود دارد که باید به آن ها پرداخت.اما باید توجه داشت که موفقیت در پیاده سازی چنین سیستمی تنها وابسته به توانایی موتور بازشناسی گفتار نیست و بلکه به میزان کاربردی بودن آن هم مرتبط است.



شکل 2-2 کاربرد زبان های ترکیبی در یک کشور

نمونه ی عملی: سیستم پاسخگویی راه آهن

ایده ی این سرویس این است که برای همه قابل استفاده باشد و به راحتی قابل دسترس برای همگان باشد.طراحی سیستم به نحوی است که11 زبان صحبت شده در یک کشور را پوشش می دهد.در این سیستم اطلاعات خطوط راه آهن به صورت آنی به زبان های انگلیسی، هندی و چندین زبان دیگر برای قطارهای مختلف ارائه می گردد.استفاده از هر گونه سیستم IVR مبتنی بر صحبت در چنین حالتی مستلزم ارتباط یکپارچه ی بین کاربران و پلتفرم است.

ساختار عملیاتی این سیستم شامل رابطی است که از یک سو با کاربر و از سمت دیگر با منابع اطلاعاتی سیستم راه آهن در ارتباط است تا بتواند به صورت آنی اطلاعات مورد تقاضا را به درستی برای کاربر پخش نماید.

پلتفرم IVR مبتنی بر گفتار کاربردی

یک تعریف کلی از customer experience به صورت مجموع ارتباطاتی است که مشتری در طول یک بازه‌ی زمانی مشخص در ارتباط با تأمین کننده ی خدمات خود دارد. این ارتباطات شامل اطلاع رسانی، جذب،روابط متقابل ، خرید، استفاده و سایر موارد می باشد.خدماتی که دارای سطح customer experience بالاتری باشند، موفق تر خواهند بود.اما به هر حال هر پلتفرم مبتنی بر گفتار، برای رسیدن به نقطه ی عملکرد بهینه، نیازمند طی کردن یک دوره ی یادگیری است.مسأله ی دیگری که باید به آن توجه نمود این است که اگر این سیستم

در کشورهایی پیاده شود که فناوری گفتار در آن ها نو باشد ، احتمال از دست دادن اطمینان از سوی کاربران در صورت برآورده نشدن نیازهای آنان وجود دارد. علاوه بر افزایش کیفیت سیستم بازشناسی گفتار ASR که در واقع هسته ی اصلی این پلتفرم است، برای دستیابی به عملکرد قابل قبول می توان با طراحی تعاملی و به روزرسانی دقیق اطلاعات و کالیبره کردن آن ها سطح رضایت مشتری customer experience را بالا برد.

سطح رضایت مشتری

پاسخ دهی دقیق در این سیستم زمانی تعریف می شود که 1- هدف صحبت های مشتری به درستی تشخیص داده شود.2- در صورت وجود نقص در سیستم، تعامل بین مشتری و سیستم به شکل صحیح انجام پذیرد.3- اطلاعات به درستی از کاربر دریافت شود و به درستی هم برای او پخش بشود.اگر چنانچه هر کدام از موارد فوق برقرار نشود سطح customer experience تنزل می یابد.

سیستم های بازشناسی گفتار یک نوع سیستم دارای هوش مصنوعی هستند که عملکرد آن ها به شدت وابسته به الگویی است که برای آموزش موتور آنها مورد استفاده قرار گرفته است.در برخی کشورها الگوی خاصی برای طراحی این سیستم وجود ندارد بنابراین این تکنولوژی همچنان در حال توسعه است و برای چنین سیستمی نیازمند دقت بسیار بالایی هستیم.

یک سیستم متن به گفتار (TTS) ، بخش دیگری از سیستم تلفن گویا است که باید برای تعامل یکپارچه مورد استفاده قرار گیرد. توانایی سیستم برای پخش پاسخ صحیح به کاربر به صورت آنی بسیار مهم است. TTS زبانی است با ملاحظات و طراحی دقیق خاص و بر اساس نیاز و هنجارهای زبانی و فرهنگی از کاربران است.هنگامی که یک وابستگی به یک منبع خارجی اطلاعات وجود دارد برای پاسخگویی به یک کاربر، یک سیستم CX خوب باید قادربه مدیریت پاسخ در زمان غیرفعال بودن منبع خارجی باشد. این نیاز به رسیدگی ممکن است ،در برخی پیاده سازی ها با یک مکانیسم SMS خروجی پاسخ داده شده که کاربر با اطلاعات به روز شده ازپایگاه داده ی محتوی جزییات تمام تماس ها به پاسخ خود می رسد.

همانطور که قبلا ذکر شد، ساخت یک راهکار جامع در یک کشور چند زبانه نه تنها مشکل است به دلیل مشکلات تکنولوژی تشخیص گفتار برای زبان های برخی کشورها بلکه چون ساخت چنین سیستمی به لحاظ کاربرد بسیار پیچیده و هزینه بر است. برای مثال، یک سیستم مستقر که مسئولیت رسیدگی به زبان L_1 را دارد ممکن است برای منطقه ای که به زبان های L_2 و L_3 صحبت می شود کارایی نداشته باشد.

راه حل این مشکل این است که یک سیستم با کاربرد مشابه را به چندین صورت پیاده سازی نماییم.به عنوان مثال بسته به تنوع زبان های مختلفی که در یک منطقه صحبت می شوند، تنها IVR به همان زبان انتخاب و مورد استفاده قرار بگیرد.همچنین نیازی نیست که در همه ی مناطق، همه ی اطلاعات مورد استفاده قرار بگیرند و ارائه شوند.

در واقع نکته ی اصلی این است که چنانچه یک سیستم IVR به یک زبان موجود باشد، فراهم کردن این امکان که زبان های دیگر را هم پشتیبانی کند کار بسیار دشواری به نظر می رسد اما اگر چنانچه این دو زبان در یک منطقه صحبت شوند و دارای هم پوشانی با یکدیگر باشند این امر راحت تر قابل انجام خواهد بود.

یک طراحی ساده ی سیستم به این صورت خواهد بود که یک دیالوگ بین کاربر و سیستم تعیین شود.دیالوگ در واقع نشان دهنده ی تعامل بین کاربر و پلتفرم IVR می باشد.کیفیت این دیالوگ را درجه ی سادگی در کاربرد و نیز راحتی کاربر در انتقال اطلاعات خود به سیستم معین می کند.برای تست کردن این ویژگی می توان یک دیالوگ ساده به چندین کاربر داد و از آنها خواست که اطلاعات آن را به سیستم منتقل کنند تا کیفیت درک سیستم از آن مشخص شود.به عنوان مثال دیالوگ زیر:

Please call 1800xxxxxx and seek the cost of travel from Vadodara to Bhavnagar by Bhavnagar express.

زیرساخت مورد نیاز

طراحی زیرساخت بهینه و مناسب برای پیاده سازی یک پلتفرم IVR مبتنی بر گفتار امری بسیار ضروری و مهم است.طراحی نامناسب نه تنها باعث کاهش موفقیت در عملکرد می شود بلکه ممکن است در تماس های طولانی حتی تماس کاربر با قطعی مواجه شود و سیستم قادر به پاسخگویی صحیح نباشد.همچنین باید توجه داشت که فراهم کردن ظرفیت بالا بدون اینکه به آن نیازی باشد هم باعث افزوده شدن بر میزان هزینه های طرح می گردد و بهینه نیست.بهتر است که ابتدا بر اساس نسبت ارلانگ تخمینی از تعداد تماس های مورد انتظار در طول روز، تعداد تماس ها در زمان اوج، تعداد ساعاتی که به عنوان زمان اوج در نظر گرفته می شود و همچنین میانگین طول هر تماس به دست آورده شود.چنانچه سیستم بر اساس آمار واقعی و آنی پیاده سازی شود می توان بعدها این مقادیر را مجدداً کالیبره نمود.[1]

کاربرد IVR در مانیتورینگ پایبندی پزشکی بیماران

پایبندی پزشکی بدین معناست که آیا بیمار داروهای تجویز شده را به درستی مصرف می کند یا خیر.در صورتی که بیمار به دستورات پزشکی اش توجه نکند و آنها را انجام ندهد نتایج ناگواری به بار می آید و هم چنین باعث ایجاد هزینه های پزشکی فراوانی خواهد شد.تکنولوژی IVR در حال حاضر در حوزه های مختلفی چون مخابرات و شبکه مورد استفاده قرار می گیرد و به عنوان مثال برای افزایش اعتبار سرویس ها کاربرد دارد.کاربرد دیگر آن در سیستم های اقتصادی به عنوان بانکداری تلفنی در موسسات است.مسأله ی پایبندی پزشکی یک موضوع چندوجهی است که در تمام مناطق دنیا تحت عنوان یک چالش مطرح است.از طریق سیستم IVR می توان ساختاری طراحی کرد که برای رعایت رژیم های دارویی با بیماران در ارتباط باشد و در صورت نیاز موارد لازم را به آن ها یادآوری نماید.

تعریف دقیق پایبندی پزشکی میزان هم پوشانی رفتار دارویی بیمار با تجویز پزشک یا مرکز درمانی او است که شامل انطباق، پایبندی و دوام می باشد.همه ی این ها مواردی هستند که کارکنان مراکز پزشکی برای توضیح موارد پزشکی و دارویی به بیماران خود از آن ها استفاده می کنند.

عواقب بسیاری ممکن است در نتیجه ی عدم پایبندی پزشکی بیمار به وجود آید از جمله افزایش تست های آزمایشگاهی، افزایش تعداد ویزیت های پزشکان، عدم موفقیت درمان و یا مقاومت دارویی.

عوامل متعددی وجود دارد که میزان پایبندی پزشکی را تحت تأثیر خود قرار می دهد.این عوامل چنانچه دست به دست هم دهند به ویژه برای بیماران مسن در صورت عدم رعایت رژیم دارویی بسیار خطرساز می شوند.عوامل موثر را می توان در پنج دسته تقسیم بندی نمود:اجتماعی و اقتصادی، سیستم مراکز درمانی، عوامل مربوط به شرایط بیمار، عوامل مرتبط با شیوه ی درمان و عوامل مرتبط با خود بیمار.این عوامل در شکل زیر به نمایش درآمده است:

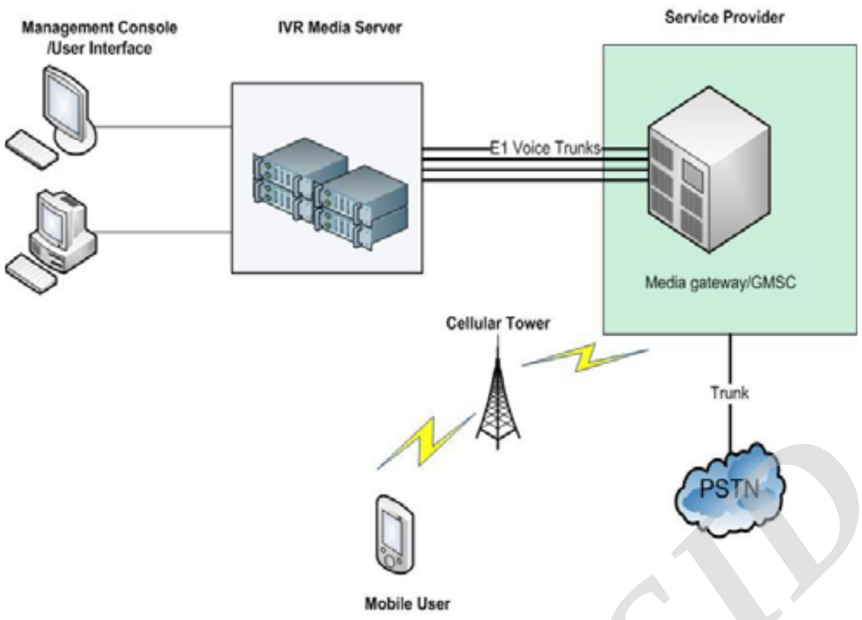
شکل2 -3 جنبه های مختلف پایبندی پزشکی

ساختار سیستم

کنسول مدیریت یا رابط کاربری

این بخش از سیستم امکان وارد شدن پرسنل پزشکی برای دسترسی به اطلاعات بیماران را فراهم می کند.این کنسول به طور مستقیم با IVR مرتبط است تا بتواند بر اساس رژیم های دارویی بیماران تماس های مورد نیاز را تنظیم و زمان بندی نماید. مدیریت حساب کاربران هم از دیگر وظایف این کنسول می باشد.کاربران این بخش در واقع پرسنل بیمارستانی هستند که در فرآیند درمانی یک بیمار و تجویز دارو به او درگیر بوده اند.اپراتور مورد نظر از طریق رابط کاربری زمان دقیق شروع و پایان تماس را برای هر کاربر تنظیم می نماید.همچنین مدیر این بخش می تواند از طریق رابط کاربری، اطلاعات بیمار را نیز وارد سیستم کند.

شکل زیر معماری ساختار سیستم را نمایش می دهد:



شکل2 – 4 معماری سیستم IVR مورد استفاده

کارگزار رسانه ی IVR

کارگزار رسانه ی IVR در واقع بخش اصلی سیستم می باشد.هدف اصلی کارگزار رسانه ی IVR این است که صداهای ضبط شده ای را که کاربر در هنگام برقراری تماس نیاز به شنیدن آن ها دارد در مکانی مناسب ذخیره نماید و در هنگام برقراری تماس از سوی بیمار، آن ها را فراخوانی کند.تمامی صداهای ضبط شده ی مورد نیاز در این سرور بارگزاری و ذخیره می شوند.مکان دقیق این سرور به احتمال زیاد در همان مرکز درمانی است و از طریق اتصال مایکروویو به سوریس متصل می شود.کارگزار رسانه را همچنین می توان از طریق یک ترانک SIP به سرویس متصل نمود.در روش اتصال از طریق ترانک SIP برای ارتباط چندین service provider به یکدیگر می توان از بستر اینترنت استفاده نمود و به راحتی از طریق یک VPN این اتصال را برقرار نمود.

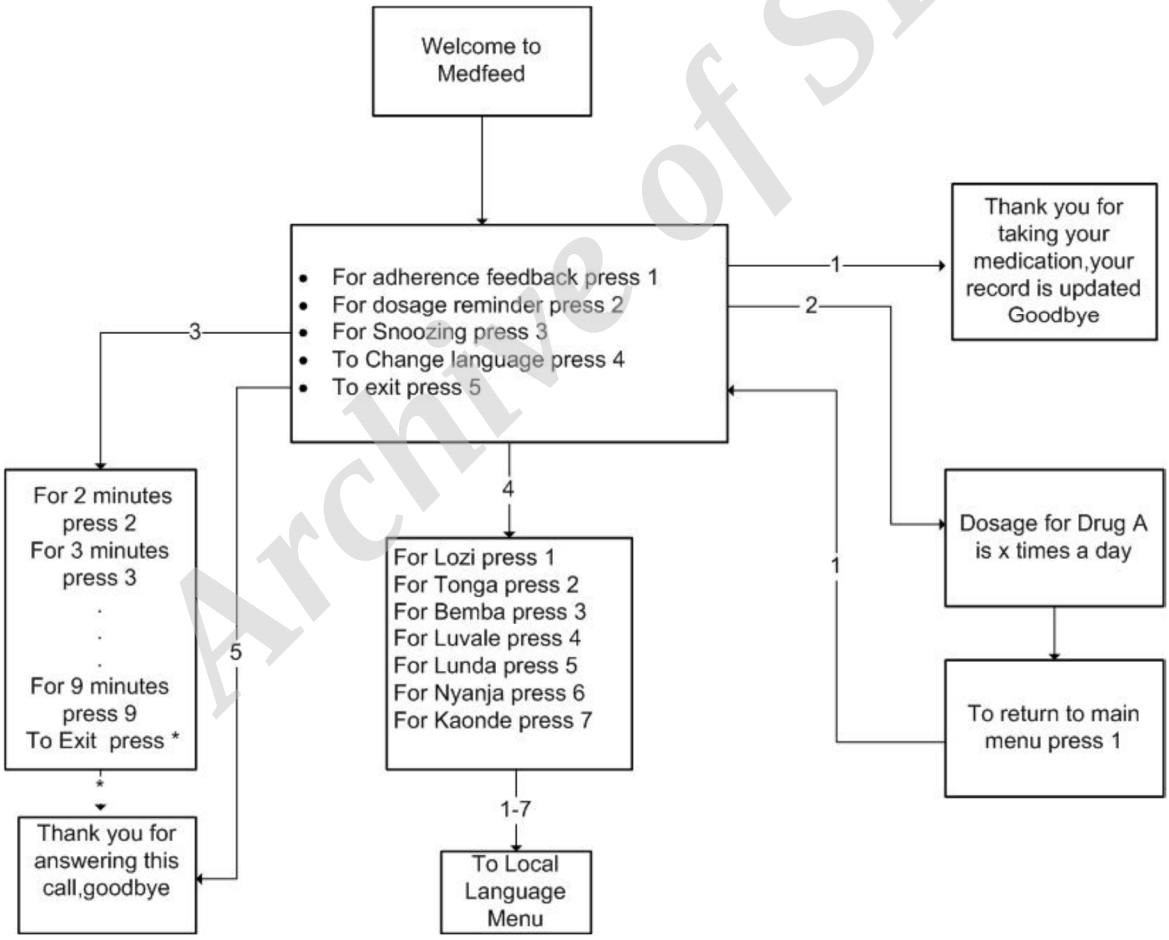
Service Provider

Service provider در واقع نقش حیاتی در پیاده سازی سیستم ایفا می کند.در عمل، رسانه ی IVR به service provider به جهت دریافت خدمات صوتی از طریق شبکه ی ثابت و یا موبایل متصل می شود.این service provider در واقع رابطی را مبتنی بر خطوط E۱ به کاربران خود عرضه می نماید.همچنین می توان از خطوط SIP برای کارگزار رسانه ی IVR استفاده نمود که از طریق اتصال به درگاه یا مرکز سوییچ service

provider از خدمات آن استفاده می کند.سپس service provider گزینه های DTMF را که بیمار از طریق تلفن خود وارد کرده به کارگزار رسانه ی IVR منتقل می کند و عمل مورد نظر انجام می پذیرد.

فلوچارت تماس IVR

شکل زیر تماس های ورودی از سیستم به بیمار را نمایش می دهد.هنگامی که بیمار گوشی را برمی دارد ابتدا سیستم به او خوش آمد می گوید و سپس منوی اصلی سیستم به همراه گزینه های مرتبط جهت شماره گیری به او اعلام می شود.گزینه ها شامل بازخورد میزان پایبندی پزشکی بیمار، یادآوری دوز مصرف دارو و تغییر زبان هستند.

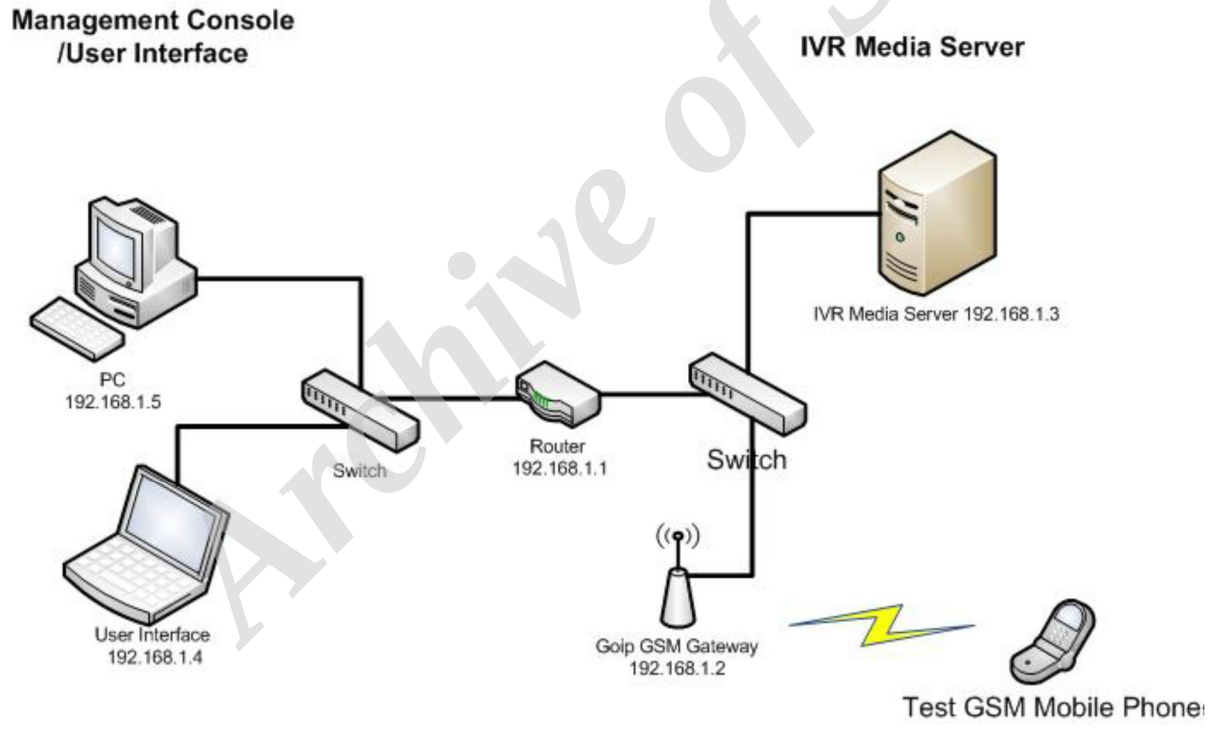


شکل2 -5 فلوچارت تماس IVR

بیمار به منظور تأیید پایبندی پزشکی خود عدد 1 را وارد می کند و در غیر این صورت سیستم تشخیص می دهد که بیمار پایبندی پزشکی و دارویی نداشته است.گزینه ی دیگری برای بیمار وجود دارد که بتواند این عمل را به تأخیر بیندازد و بعد از مدتی از مصرف دارو و رعایت رژیم دارویی خود به این سوال پاسخ بدهد. منوی اصلی سیستم همچنین این امکان را به کاربر می دهد که زبان مورد نظر خود را انتخاب نماید. همه ی اطلاعات وارد شده توسط بیمار در سیستم IVR ذخیره شده و بعدها برای تحلیل رفتار دارویی و پرونده ی پزشکی او مورد استفاده و استناد قرار می گیرند.

پیاده سازی سیستم

شکل 2-6 ساختار پیاده سازی شده ی سیستم را نشان می دهد:



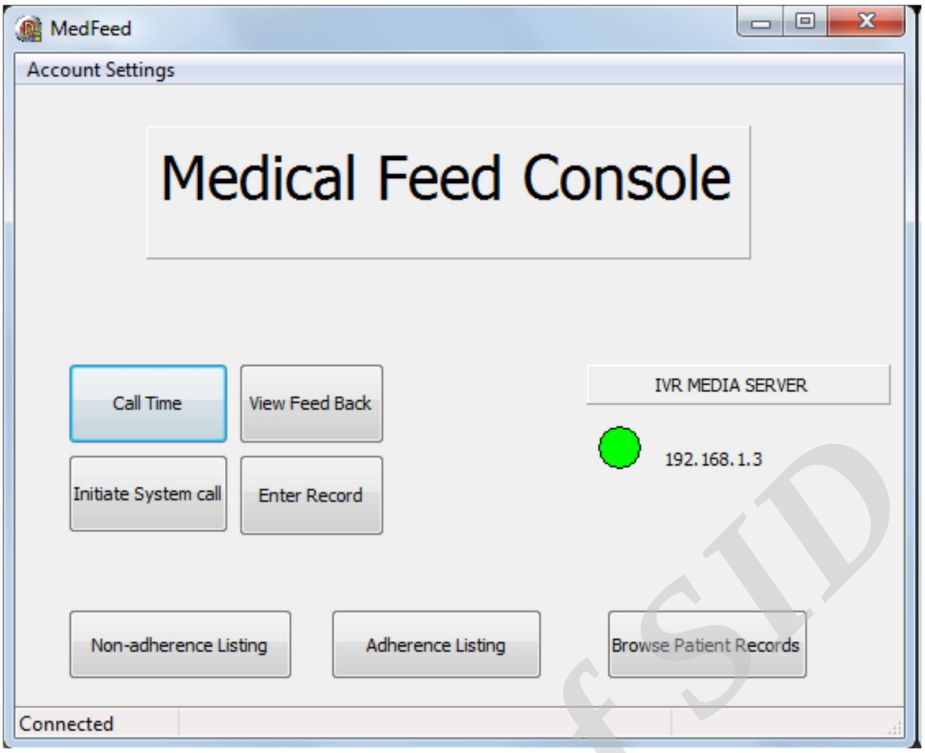
شکل 2-6 ساختار پیاده سازی سیستم IVR

سخت افزار

سخت افزار این سیستم شامل دو کامپیوتر با سیستم عامل ویندوز به عنوان رابط کاربری، دو روتر و دو سوییچ است.مشخصات کارگزار رسانه ی سیستم IVR به صورت 4 گیگابایت رم و CPU ۱،٦ GHz Intel (Dual core) و مقدار فضای دیسک 320 گیگابایت است.برای این که بتوان تماس های ورودی و خروجی را به طور همزمان داشت نیاز به استفاده از یک درگاه GSM VOIP وجود دارد.این درگاه از طریق یک سوییچ اترنت به کارگزار رسانه متصل می شود. ارتباط بین درگاه GSM و کارگزار رسانه از طریق یک ترانک SIP برقرار می شود. برای تست کردن عملکرد سیستم IVR از طریق موبایل تماس گرفته شد و پیام صوتی که کاربر دریافت می کند شنیده شد. تمامی تجهیزات سخت افزاری بر اساس اترنت و در یک شبکه ی محلی کوچک به یکدیگر متصل شده اند.محدوده ی IP مورد استفاده در ساب نت ۱۹۲،۱٦۸،۱.x انتخاب شده است.

نرم افزار

عملکرد اصلی سیستم کاملاً وابسته به منطقی است که در نرم افزار آن انجام می پذیرد. هسته ی نرم افزاری سیستم IVR مبتنی بر Asterisk است. تمامی منطق پردازش تماس برای گزینه های DTMF که بیمار وارد می کند توسط Asterisk انجام می پذیرد.رسانه ی IVR در محیط لینوکس برقرار می شود که از نسخه ی فدورا 11 استفاده شده است. رابط کاربری سیستم با استفاده از دلفی نوشته شده است.کنسول کاربری چندین گزینه را شامل می شود از جمله لیست عدم پایبندی دارویی،لیست پایبندی دارویی،تنظیم زمان خاص تماس با یک بیمار به ویژه در هنگام مصرف دارو.کاربر همچنین می تواند سابقه ی بیمار را به طور کامل در سیست ببیند و زمان هایی را که بیمار باید از طرف سیستم تماس دریافت کند را نیز می تواند مدیریت نماید.شکل 2-7 ساختار رابط کاربری سیستم پیاده سازی شده را نمایش می دهد:



شکل2 – 7 رابط کاربری مدیریت سیستم

این سیستم دارای مزایای بسیاری نسبت به سیستم های قدیمی استفاده شده برای ثبت اطلاعات بیمار است و از جمله ی آن ها این است که امکان اندازه گیری به صورت آنی را فراهم می کند.محدودیت اصلی این سیستم استفاده از درگاهGSM است که تنها یک تماس را می تواند در لحظه پشتیبانی کند. می توان برای توسعه ی سیستم مسأله ی تماس های همزمان را هم مدنظر قرار داد و برای آن راهکاری اندیشید.به عنوان مثال service provider می تواند از طریق خط E۱ امکان برقراری چندین تماس همزمان را فراهم نماید.بخش دیگری از سیستم که می تواند بهبود یابد موتور زبان آن است که می توان قابلیت پشتیبانی از چندین زبان را به آن اضافه نمود.[۲]

طراحی سیستم پیش بینی وضع آب و هوا با استفاده از IVR

امروزه تغییرات آب و هوا بیشتر در حوزه ی تغییرات الگوی آب و هوایی خود را نشان می دهد که موجب خشکسالی و یا سیل در کشورها می شود.این مسأله امنیت غذایی را به صورت کاهش زمین های قابل کشت و افزایش جمعیت با تهدید جدی مواجه می کند.موسسات تحقیقاتی کشاورزی در حال کار بر روی شیوه های

جدید کاشت گیاها ن و روش هایی هستند که در مقابل بلایای طبیعی مانند سیل مقاوم باشند.به هر حال در صورتی که سیستم مناسبی وجود نداشته باشد،این اطلاعات به موقع به کاربران واقعی آن که در اینجا کشاورزان هستند نمی رسد.

تغییرات اقلیمی به صورت تغییر در میزان میانگین وضعیت آب و هوا در طول یک دوره ی زمانی تعریف می شود.چنین تغییراتی به شدت بخش کشاورزی را تحت تأثیر قرار داده و نیاز به روالی برای جبران این تأثیرات را به وجود می آورد.موسسات تحقیقاتی کشاورزی در هند به تازگی گونه های را ابداع کرده اند که نسبت به گرمای بیش از حد و سیل مقاوم اند و برای مناطقی که در آن ها احتمال سیل و خشکسالی بیشتر است به کار می روند.برای انتقال این تکنولوژی های جدید از آزمایشگاه به زمین های کشاورزی نیازمند زیرساختی در شبکه ی ICT هستیم که بتوان از حوزه ی تحقیقات فراتر رفت و نتایج را به صورت عملی مشاهده نمود.

پلتفرم mKRISHI یک ساختار موبایلی مبتنی بر IVR است که بر اساس تکنولوژی وب خدمات مختلف را به کشاورزان و سرمایه داران آنها به زبان های محلی ارائه می نماید.از این پلتفرم در پروژه های مختلف استفاده شده است به عنوان مثال در یک پروژه متخصصان کشاورزی از دانشگاه ها و موسسات مختلف از این پلتفرم در راستای به اشتراک گذاری اطلاعات در حوزه ی گونه های مختلف گیاهی و مشخصات اختصاصی کشاورزی مربوط به هر منطقه استفاده کردند.

کشاورزان query های مختلفی را به زبان های مختلف توسط اپلیکیشن موبایلی و یا IVR به سیستم ارسال می کنند.متخصصان کشاورزی از سوی دیگر این query ها را در زمینه ی مشخصات خاک و پیش بینی آب و هوا برای یک هفته مورد بررسی و تحلیل قرار می دهند.این تحلیل باعث می شود که به هر کشاورز، توصیه های کشاورزی مختص خود او داده شود.در این فرآیند در حدود 9000 کشاورز در 360 روستای مختلف و 4 منطقه تحت پوشش قرار گرفتند.در جریان 18 ماه راه اندازی پایلوت پروژه ، در حدود 19000 query در سیستم جمع آوری شد.

در طول 50 سال گذشته فرکانس تکرار شرایط آب و هوایی نامساعد به شدت افزایش یافته است و دمای هوا در نقاط مختلف جهان رو به افزایش گذاشته است.تحقیقات کشاورزی در هند نشان داده است که میزان برداشت محصولاتی مانند برنج، گندم و جو به ازای هر 1 درجه ی سانتی گراد افزایش دما 10 درصد کاهش پیدا می کند.

بر اساس تهدیدهای آب و هوایی مربوط به هر منطقه، برای کاهش تلفات محصولات زیر کشت تدبیری اندیشیده شده است و دانشمندان در حال پژوهش بر روی گونه هایی هستند که کمترین آسیب پذیری را در مقابل چنین تهدیداتی از خود نشان دهند.

چالش اصلی در این امر این است ک چگونه در زمینه ی این نوع مداخلات به کشاورزان اطلاع رسانی شود و بتوان این تحقیقات را از آزمایشگاه به مزارع کشاورزی منتقل نمود.می توان از شبکه ی موبایلی به منظور ارائه ی خدمات مربوط به هر منطقه به صورت آنی و با هزینه ی کم استفاده نمود.در هند موسسات بسیاری در این زمنیه فعالیت می کنند اما اکثریت آن ها بر اساس ارسال پیامک به زبان انگلیسی خدمات خود را به کشاورزان ارائه می دهند.بنابراین نیاز است که سیستمی با زبان محلی بر اساس نیاز کشاورزان در هر منطقه طراحی شود که در هر زمانی قابل دسترسی باشد.پلتفرم mKRISHI این امکان را برای دانشمندان فراهم کرد که برای هر منطقه به طور خاص توصیه های مربوط به نحوه ی کاشت و برداشت محصولات مربوط به همان منطقه در این سیستم بارگزاری شده و در دسترس کشاورزان قرار بگیرد.کشاورزان می توانند از طریق موبایل خود که به شبکه ی GPRS متصل است در هر زمانی به این اطلاعات دسترسی داشته باشند.این فرآیند یک ارتباط آنی و مستقیم بین تولید کننده ی اطلاعت و مصرف کننده ی آن که کشاورزان باشند فراهم می کند.با استفاده از این اطلاعات فراهم شده در سیستم، کشاورزان توصیه های محققان در خصوص جایگزینی دانه ها و یا تغییرات در فرآیند آبیاری را به اجرا گذاشتند که این مسأله باعث کاهش هزینه ها و تلفات شد.

طراحی خدمات

با در نظر گرفتن انواع مختلف دستگاه های موبایلی که در هند مورد استفاده قرار می گیرند دو نسخه از سیستم mKRISHI طراحی گردید:

- Plain Vanilla offering - mKRISHI Lite
- Value Added Service – mKRISHI Regular

نسخه ی اول یک سیستم IVR مبتنی بر زبان محلی است.کشاورز یک شماره ی رایگان را می گیرد و سوال خود را در قالب یک query به زبان محلی به سیستم منتقل می کند.متخصص کشاورزی سوال پرسیده شده را تحلیل می کند و در پاسخ خود را در قالب یک پیام صوتی و با یک تماس به کشاورز مورد نظر منتقل می کند.

نسخه ی دوم یک سرویس مبتنی بر اپلیکیشن موبایل است که کشاورزانی که موبایل اندروید و یا جاوا داشته باشند می توانند از آن استفاده نمایند.از طریق این اپلیکیشن کشاورز می تواند query بفرستد که شامل اطلاعات تصویر، متن و صوت در خصوص زمین کشاورزی و منطقه ی مربوط به خودش است.این اپلیکیشن همچنین شامل اطلاعاتی همچون وضع آب و هوا، سوالات متداول و توصیه های کشاورزی می باشد.

کنسول متخصص این سیستم امکان مشاهده‌ی پروفایل مشخصات کشاورزان، سابقه‌ی کشت و پارامترهای لازم زمین کشاورزی را برای کارشناس فراهم می کند(شکل2-8)با استفاده از این اطلاعات، کارشناس کشاورزی می تواند سوالات کشاورز را تحلیل کند و پاسخ مناسب را به زبان محلی مورد نظر برای او ارسال نماید.

شکل 2 – 8 کنسول مدیریت سیستم mKRISHI

ساختار خدمات

در این سیستم دو منبع اصلی برای داده ها و اطلاعات وجود دارد:

- اطلاعات ارسال شده از سوی کشاورز
- اطلاعات مراکز تحقیقاتی کشاورزی

اطلاعات شخصی کشاورز و مشخصات زمین کشاورزی در جریان پروسه ی ثبت نام کشاورز در سیستم ذخیره می شوند.علاوه بر این، کشاورز اطلاعاتی همچون تنوع گونه ها، تاریخ بذرپاشی و سایر فرآیندهای زمین خود را وارد سیستم می نماید. متخصص کشاورزی پکیج گیاهی مختص هر منطقه را به زبان محلی همان منطقه آماده می کند. این اطلاعات به صورت متن، تصویر و صوت به سیستم منتقل می شوند.

1- ثبت نام کشاورز: در هر منطقه کشاورزان شناسایی شده و در سیستم توسط اپلیکیشن موبایلی یا IVR ذخیره می گردند.جزییات ثبت نام شامل مراحل زیر می شود:

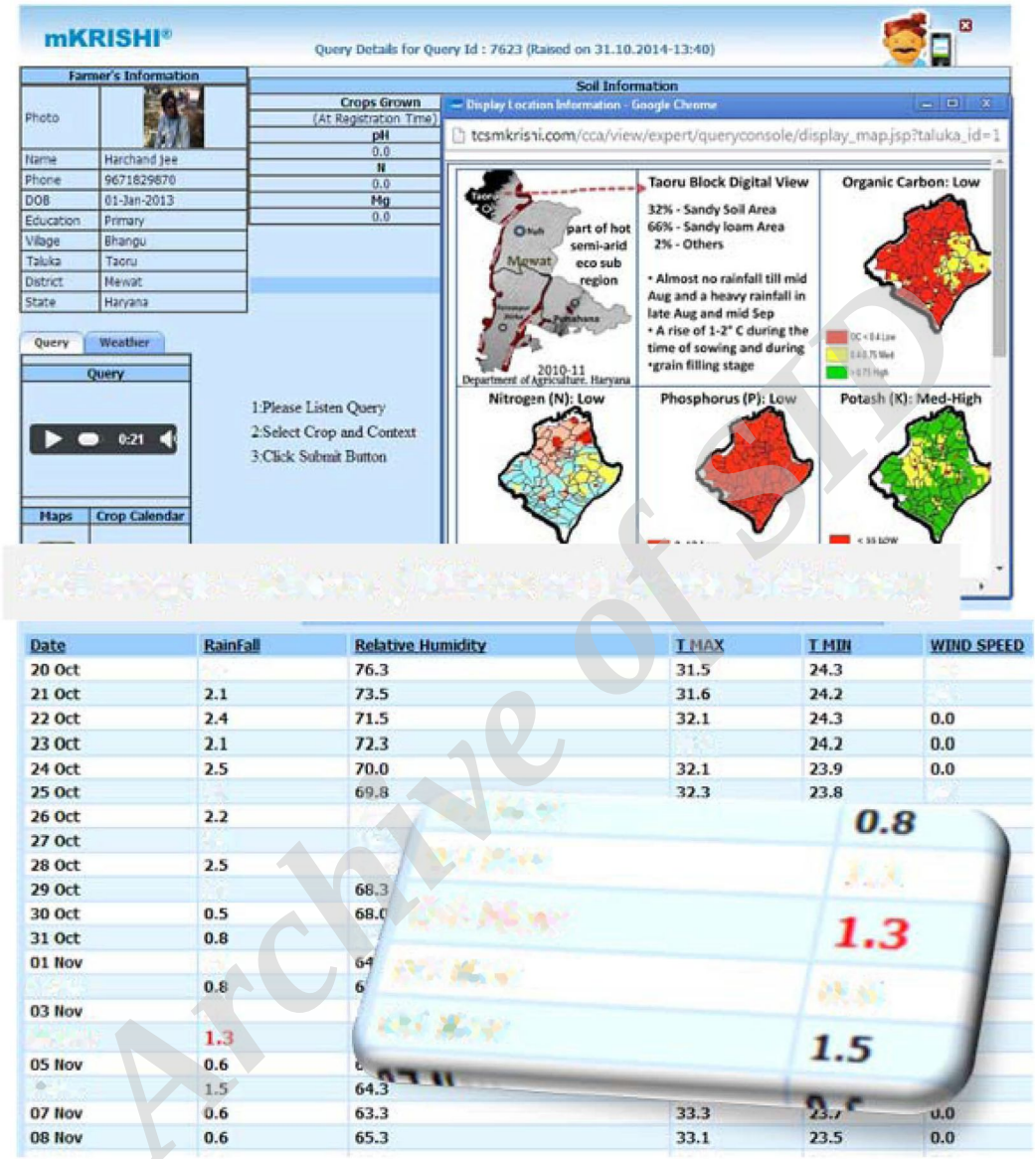
- اطلاعات شخصی کشاورز-نام، سن و منطقه
- اطلاعات زمین کشاورزی-داده های گیاهان، منبع آبیاری و اطلاعات عملیات کشاورزی انجام شده در زمین مورد نظر
- گزارش خاک منطقه

2- اطلاعات مراکز تحقیقاتی کشاورزی:اطلاعاتی که مراکز تحقیقاتی درباره ی زمین های کشاورزی مختلف و پارامترهای آن ها در دیتابیس خود دارند.

تمامی اطلاعات فوق در دیتابیس mKRISHI بارگزاری می شود.

3- نگاشت داده ها : سیستم به صورت هوشمندانه داده های مربوط به ثبت نام و داده های مراکز اطلاعاتی را در مرکز داده ی خود ذخیره می کند تا کارشناس کشاورزی از طریق آن بتواند اطلاعات مفیدی به کشاورزان ارائه دهد.کارشناس کشاورزی هم قبل از اینکه پاسخ خود را به سوال کشاورز مورد نظر اعلام کند، در داخل دیتابیس ابتدا به مشخصات زمین، منطق و گزارش خاک آن نگاه می کند و سپس بر اساس اطلاعات موجود بهترین راهکار را به او ارائه می نماید.از آنجایی که سیستم تمامی اطلاعات را از طریق یک کنسول ارسال و دریافت می

کند به راحتی می توان بخش سوالات متداول را نیز در این سیستم طراحی نمود و برای استفاده ی کشاورزان آن را در دسترس قرار داد.



شکل 2-9 نمایش اطلاعات مربوط به آب و هوا در کنسول مدیریت mKRISHI

4- اطلاعات مربوط به پیش بینی وضعیت آب و هوا:میانگین وضعیت آب و هوا برای مدت 50 سال اخیر به دیتابیس این کنسول اضافه شده است.داده ها به صورت یک هفته الی 15 روز بعد از اینکه سوال ارسال شده بود رسم شده اند.این کار باعث می شود تا بتوان نحوه ی تغییرات آب و هوا در روزهای آینده را نیز پیش بینی

نمود.علاوه بر این اطلاعات، داده های مربوط به پیش بینی بارش باران و میزان ابر موجود در هوا هم به سیستم اضافه شد.تمامی این اطلاعات به کارشناس کمک می کند که بتواند پاسخ دقیق تری به سوال های پرسیده شده از طریق IVR بدهد.بنابراین کشاورز نه تنها در مورد راهکار اطلاعات به دست می آورد بلکه در مورد زمان پیاده سازی آن هم مطلع می شود که همین امر بازخورد بسیار مناسبی در میان کشاورزان داشته است.

آموزش

سیستم پیاده سازی شد و بیش از 180 کمپ در 250 روستا برای آموزش و افزایش آگاهی کشاورزان طراحی گردید.اپلیکیشن موبایل بر روی موبایل کشاورزان نصب شد و نمونه ی سیستم IVR برای آن ها پیاده سازی گردید.بازدید کارشناسان از مزارع نشان داد که این طرح باعث افزایش اطمینان کشاورزان از محصولات و خدمات شان شده است.همچنین در طول زمان، از کشاورزان بازخوردهای فراوانی گرفته شد که باعث افزایش سادگی در طراحی و کاربرد سیستم گردید.[3]

3,2 نتایج تحلیلی و عملیاتی مقطع اول

در گزارش فاز اول، به مقایسه‌ی محصولات متن‌بازی مورد بررسی قرار گرفت، که در سه بخش مقایسه‌ی پروژه‌های متن‌باز مقیاس کوچک، مقایسه‌ی کارگزارهای SIP، مقایسه‌ی کارگزارهای رسانه انجام گرفت.

در بخش دوم مقایسه، به مقایسه‌ی کارگزارهای SIP پرداخته شد و بطورکلی نتایج آن را می توان در جدول زیر وزن دهی نمود و بعنوان معیاری تاثیر گذار در انتخاب و طراحی معماری محصولی منطبق با نیازها و اهداف پیشرو سود برد.

جدول 2-1. مقایسه کارگزارهای SIP

محصول مورد بررسی / معیار مقایسه	کامایلیو	اپن‌سیپس
وجود نسخه جدید در سال اخیر	✓	✓
استفاده از پروتکل SIP	✓	✓
معماری ماژولار	✓	✓
پشتیبانی از رمزنگاری	✓	✓
استفاده در پروژه‌های مقیاس‌پذیر دیگر	✓	•
سازگاری عملیاتی با کارگزارهای رسانه دیگر	✓	•
مجموع امتیازها	6/6	4/6

سپس به مقایسه راهکارهای کارگزار رسانه پرداخته شد که در جدول زیر نتایج آن بطور وزن دهی شده آورده شده است.

جدول 2-2 مقایسه کارگزارهای رسانه

محصول مورد بررسی / معیار مقایسه	Asterisk	Elastix	فری‌سوییچ	بیت	تریکس‌باکس
نسخه ارائه شده در سال اخیر	✓	✓	✓	✓	✓
تنوع پروتکل‌های مورد پشتیبانی	✓	✓	✓	✓	•
معماری	✓	✓	✓	•	•

تنوع زبان‌های مورد پشتیبانی	•	✓	✓	✓	✓
پشتیبانی از رمزنگاری	✓	✓	✓	✓	•
مجموع امتیاز (مرحله اول)	4/5	5/5	5/5	4/5	حذف از مقایسه
واسط گرافیکی کاربری	•	✓	✓	•	حذف‌شده از مقایسه
*	به دلیل یکی بودن هسته‌ی دو پروژه Elastix و Asterisk، و عدم پشتیبانی پروژه Asterisk از واسط گرافیکی، نرم‌افزار Elastix که هسته‌اش Asterisk است، در مقایسه‌های بعدی در نظر گرفته می‌شود.				
سازوکارهای پشتیبانی نظیر مستندات آموزشی	حذف‌شده از مقایسه	✓	✓	•	حذف‌شده از مقایسه
پشتیبانی توسط شرکت‌های ارتباطاتی در حوزه نرم‌افزاری و سخت‌افزاری	حذف‌شده از مقایسه	✓	✓	•	حذف‌شده از مقایسه
تنوع کدک‌های صوتی	حذف‌شده از مقایسه	✓	✓	•	حذف‌شده از مقایسه
تنوع کدک‌های تصویری		•	✓	•	
مجموع امتیاز (مرحله دوم)	حذف شده	4/5	5/5	حذف	حذف شده
ویژگی‌های عملکردی (پشتیبانی از چندمالکیتی)	حذف‌شده از مقایسه	•	✓	حذف‌شده از مقایسه	حذف‌شده از مقایسه

تطبیق‌پذیری بسیار بالا برای کاربردهای مختلف	حذف‌شده از مقایسه	•	✓	حذف‌شده از مقایسه	حذف‌شده از مقایسه
پایه‌ی توسعه‌ای[1]	حذف‌شده از مقایسه	✓	•	حذف‌شده از مقایسه	حذف‌شده از مقایسه
روش پیکربندی با امکان خودکارسازی ساده تر	حذف‌شده از مقایسه	•	✓	حذف‌شده از مقایسه	حذف‌شده از مقایسه
پایداری[2]	حذف‌شده از مقایسه	•	✓	حذف‌شده از مقایسه	حذف‌شده از مقایسه
خوشه‌بندی	حذف‌شده از مقایسه	•	✓	حذف‌شده از مقایسه	حذف‌شده از مقایسه
میزان نیازمندیهای سخت‌افزاری برای راه‌اندازی	حذف‌شده از مقایسه	•	✓	حذف‌شده از مقایسه	حذف‌شده از مقایسه
استفاده‌های کاربردی	حذف‌شده از مقایسه	✓	✓	حذف‌شده از مقایسه	حذف‌شده از مقایسه
مقیاس‌پذیری	حذف‌شده از مقایسه	•	✓	حذف‌شده از مقایسه	حذف‌شده از مقایسه
مجموع امتیاز (مرحله سوم)	حذف شده	2/9	8/9	حذف شده	حذف شده

سپس به بررسی عملکرد کارگزارهای رسانه‌ی Freeswitch و Asterisk که هسته‌ی Elastix است پرداخته شد. که بنا به مقایسه انجام شده، در عملکرد نیز پروژه‌ی Freeswitch نسبت به پروژه‌ی Elastix برتری دارد.

[1] development base
[2] stability

3.طراحی و انتخاب تکنولوژی‌های مورد استفاده

3,1 Freeswitch

فری‌سوییچ، یک نرم‌افزار ارتباطاتی رایگان و متن‌باز است که برای ایجاد محصولات صوتی و انتقال پیام از آن استفاده می‌شود. کتابخانه‌ی هسته‌ای آن که libfreeswitch نام دارد، این امکان را فراهم می‌آورد تا در دیگر پروژه‌ها تعبیه شود.

فری‌سوییچ یک پلتفرم مقیاس‌پذیر است که برای مسیردهی و اتصال پروتکل‌های ارتباطاتی با استفاده از صوت، تصویر، متن یا دیگر انواع رسانه‌ها طراحی شده است. این پروژه در سال 2006 به منظور پر کردن خلا به جای مانده از راه‌حل‌های تجاری ایجاد شد. این نرم‌افزار قادر است تا بستر پایداری را برای توسعه‌ی کاربردهای تلفنی دیگر چه به صورت فیزیکی و چه به صورت نرم افزاری مهیا نماید[4].

این نرم‌افزار از پروتکل‌های صوت روی اینترنت مختلفی پشتیبانی می‌نماید که برای نمونه می‌توان به پروتکل سیپ و یکس اشاره نمود. این نرم‌افزار توانایی ارتباط با دیگر نرم‌افزارهای تلفنی مانند Asterisk را فراهم می‌آورد. این نرم‌افزار از قابلیت‌های مختلفی مانند موارد زیر پشتیبانی می‌نماید:

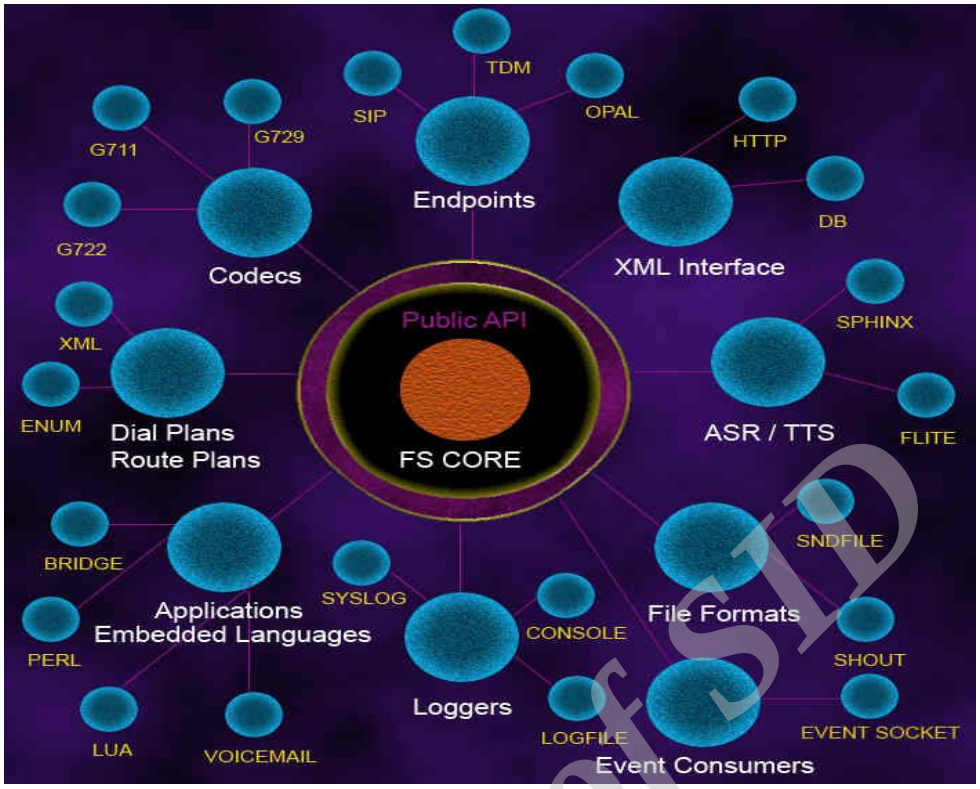
- پشتیبانی از تبدیل نوع کدگذاری[3] ویدیو
- دایرکتوری کاربر/ دامنه متمرکز
- ضبط تماس
- موتور چندریسمانی با عملکرد بالا
- مستقل از پروتکل[4]
- پشتیبانی از پروتکل ZRTP برای مبادله کلید و رمزنگاری مبتنی بر RTP
- تولید و کشف DTMF
- کنفرانس مبتنی بر نرم‌افزار (بدون نیاز سخت‌افزار)
- پشتیبانی از کارگزار اشتراک[5]

[۳] transcoding
[٤] Protocol Agnostic
[٥] Subscription server

- منشی خودکار[6]
- پشتیبانی از صف
- پارک تماس

این نرم‌افزار از سیستم‌عامل‌های مختلفی پشتیبانی می‌نماید که برای نمونه می‌توان به سیستم‌عامل‌های ویندوز، لینوکس، مک او.اس و بی.اس.دی اشاره کرد. فری‌سوییچ بر اساس زبان برنامه‌نویسی C توسعه یافته است. آخرین نسخه‌ی این نرم‌افزار در ماه می 2016 ارائه شده است. برای گسترش و کدنویسی روی بستر این نرم‌افزار می‌توان از زبان‌های برنامه‌نویسی جاوا، روبی، پایتون، پرل و لوا استفاده نمود. اهداف طراحی در این پروژه، پایداری[7]، مقیاس‌پذیری[8] و انتزاع[9] بوده است. طراحی این نرم‌افزار به صورت ماژولار است. این امر به این معنی است که بر حسب نیازمندی‌های پروژه‌های مختلف، امکان افزودن یا حذف ماژول‌ها در این سامانه مهیا است. علاوه بر این، به همین دلیل ماژولار بودن طراحی، خود مولفه‌های نرم‌افزار به یکدیگر وابسته نیستند که این امر، به واسطه‌ی وجود عنصر کلیدی انتزاع، میسر شده است.

[6] Automated Attendant
[7] stability
[8] scalability
[9] abstraction



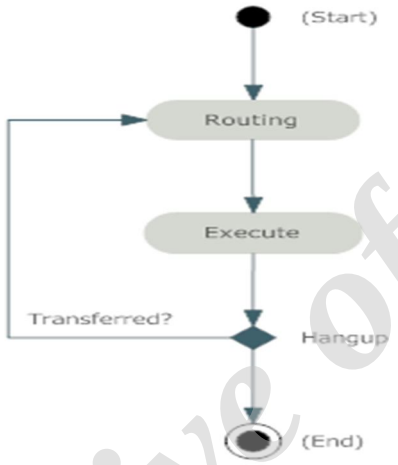
شکل 3-1: معماری نرم‌افزار فری‌سوییچ

به منظور کاهش پیچیدگی، فری‌سوییچ از کتابخانه‌های نرم‌افزاری متن‌باز استفاده نموده است که برخی از آنها عبارت‌اند از:

- کتابخانه APR[10]
- کتابخانه SQLite که یک پیاده‌سازی سبک از موتور SQL است.
- کتابخانه PCRE[11] به منظور پشتیبانی از عبارت‌های منظم
- کتابخانه Sofia-SIP که یک کتابخانه عامل کاربر SIP متن‌باز است.
- کتابخانه libspeex که یک کدک فشرده‌سازی گفتار متن‌باز است. البته کدک Opus جایگزین آن شده است.
- کتابخانه libSRTP که یک پیاده‌سازی متن‌باز از پروتکل انتقال بلادرنگ امن[12] است.

[10] Apache Portable Runtime
[11] Perl Compatible Regular Expressions
[12] Secure Real-time Transport Protocol (SRTP)

چرخه حیات تماس درنرم افزارمتن بازفری‌سوییچ در شکل زیر نمایش داده شده است. ابتدا تماس وارد حالت مسیریابی می‌شود. این حالت به دنبال ماژول «نقشه تماس[13]» میگردد و سپس، یک لیست از کارهایی که برای پردازش این تماس باید صورت بگیرد، تهیه می‌نماید. این لیست کارها شامل یک سری کلید مقدار است. درگام بعدی، تماس وارد حالت اجرا می‌شود که طی آن، کلید مقدارهای تهیه‌شده در گام قبل، مورد پردازش و اجرا قرار می‌گیرند. در قدم بعدی، تماس به شرط بررسی انتهای تماس وارد می‌شود که در آن ممکن است تماس خاتمه یابد و یا اینکه دوباره به حالت مسیریابی برگشت داده شود.



شکل 3-2: چرخه حیات تماس در فری‌سوییچ

این نرم‌افزار برای پشتیبانی از رمزنگاری، از پروتکل‌های امنیتی مانند TLS، SRTP و ZRTP پشتیبانی می‌نماید. این نرم‌افزار از کدکهای بسیار متنوعی پشتیبانی می‌نماید که در جدول زیر به آنها اشاره شده است.

جدول 3-1: کدک‌های مورد پشتیبانی فری‌سوییچ

کدک‌های صوتی	کدک‌های تصویری
PCMU – G.711 µ-law	H261
PCMA – G.711 A-law	H263
G.722	H263+ (H263-1998)
G.722,1	H263++ (H263-2000)

[13] dial plan

G.722,1c G.726 G.726 with AAL2 packing G.729 (passthrough) G.729 (licensed, 10/channel)[17] GSM CELT and Opus iLBC DVI4 (IMA ADPCM) BroadVoice SILK Speex Codec2 Siren LPC-10 G.723,1 (passthrough only) AMR (passthrough only) iSAC	H264 Theora MP4

ماژولهای این نرم‌افزار حوزه‌های مختف کاربردی صوت روی اینترنت را پوشش می‌دهد. توضیحات در مورد این ماژول‌ها و عملکردهای هر یک از آنها در پیوند زیر قابل دسترسی است:

https://wiki.freeswitch.org/wiki/Modules

برای ایجاد نقشه تماس‌های[14] دلخواه در این نرم‌افزار، از زبان XML استفاده می‌شود. یک فایل نقشه تماس دارای یک یا چند زمینه[15] است. هر کدام از زمینه‌ها می‌تواند شامل یک یا چند گسترش[16] باشد. هر گسترش نیز می‌تواند شامل یک یا چند شرط و هر شرط شامل چند اقدام[17] باشد.

نقشه تماس XML، نقشه تماس پیش‌فرضی است که توسط freeswitch استفاده می‌شود. زبان XML را می‌توان به راحتی و بدون نیاز به ابزار خاصی ویرایش نمود. در واقع، نقشه تماس برای مسیردهی یک ماس به یک نقطه‌ی نهایی است که می‌تواند یک گسترش سنتی، صندوق صوتی، سامانه پاسخ صوتی تعاملی و دیگر موارد این چنینی باشد. نقشه‌های تماس بسیار انعطاف‌پذیر هستند.

نقشه‌های تماس را می‌توان به چندین زمینه تقسیم نمود و به وسیله‌ی آن این امکان را برای تماس ها به وجود آورد که مسیرهای مختلف را دنبال نمایند. برای مثال می‌توان برای تماس‌های ورودی از PSTN، یک زمینه و برای تماسهای داخلی، زمینه‌ی دیگری را تعریف نمود. با این کار میتوان تماس‌های ورودی از PSTN را با دقت نظر بیشتری مورد نظارت قرار داد.

وقتی که یک تماس وارد سامانه freeswitch می‌شود، کارگزار Sofia به آن پاسخ می‌دهد. این کارگزار اطلاعاتی را در مورد تماس جمع‌آوری کرده و تصمیم می‌گیرد که کدام نقشه تماس را فراخوانی نماید. این کارگزار، اطلاعات در مورد تماس را در قالب یک سری متغیر کانال به نقشه تماس ارسال می‌کند. نقشه تماس با استفاده از این متغیرهای کانال می‌تواند در مورد آن تماس تصمیم‌گیری نماید. متغیرهای تماس شامل اطلاعاتی غنی در مورد تماس در حال پردازش هستند. برای مثال، مقدار متغیر کانال «شماره مقصد»، برابر شماره تماس گرفته شده است. دیگر متغیرها شامل اطلاعات شناسه تماس‌گیرنده[18]، آدرس IP منبع و غیره است.

یک فایل نقشه تماس XML، متشکل از یک سری تعریف گسترش است که freeswitch برای هر تماس، هر کدام از آنها را برای یافتن یک تطبیق طی می‌نماید. عمل تطبیق با بررسی تعاریف شرطی در هر کدام از گسترش‌ها صورت

---

[14] dialplan
[15] context
[16] extension
[17] action
[18] caller-ID

می‌پذیرد. وقتی که یک شرط برآورده شود، تعریف اقدام مربوط به آن اجرا می‌گردد. در ساده‌ترین حالت، یک اقدام می‌تواند برقراری تماس باشد. در زیر، یک نمونه نقشه تماس نمایش داده شده است:

```
<context name="example">
  <extension name="500">
    <condition field="destination_number" expression="^۵۰۰">
      <action application="bridge" data="user/500"/>
    </condition>
  </extension>

  <extension name="501">
    <condition field="destination_number" expression="^۵۰۱">
      <action application="bridge" data="user/501"/>
      <action application="answer"/>
      <action application="sleep" data="1000"/>
      <action application="bridge" data="loopback/app=voicemail:default ${domain_name}

${dialed_extension}"/>
    </condition>
  </extension>
</context>
```

برای ایجاد یک نقشه تماس کافی است تا در مسیر conf/dialplan، اقدام به ساخت یک فایل با پسوند xml شود. یکی از مهمترین اجزای یک نقشه تماس، بخش اقدامات است. در این بخش به صورت گذرا به بررسی این اقدام‌ها پرداخته می‌شود.

جدول 3-2: اقدام ها

ردیف	عنوان اقدام	توضیحات
1	log	با استفاده از این اقدام، امکان چاپ یک عبارت در خروجی وجود دارد. از این اقدام می‌توان برای عیب‌یابی استفاده کرد.
2	bridge	از این اقدام می‌توان برای ایجاد تماس با یک کاربر استفاده کرد.
3	answer	همیشه در ابتدای یک نشست نیاز است تا از این اقدام استفاده شود. این اقدام برای برقراری تماس نیاز است.
4	read	امکان خواندن تن‌های DTMF وارد شده توسط یک کاربر توسط کارگزار را فراهم می‌آورد.
5	hangup	یک تماس را قطع می‌نماید. یک نسخه‌ی دیگری از آن به نام sched_hangup وجود دارد که با استفاده از آن امکان قطع کردن یک تماس

		بعد از گذشت یک زمان مشخص وجود دارد.
6	set	با استفاده از این اقدام، امکان مقداردهی به متغیرها وجود دارد.
7	db	با استفاده از این اقدام، امکان ارتباط برقراری ارتباط با پایگاه‌داده وجود دارد.
8	execute_extension	با استفاده از این اقدام می‌توان به یک گسترش دیگر پرش کرد و آنرا اجرا نمود. عملکرد آن شبیه به عملکرد دستور goto در برنامه نویسی است.
9	echo	با استفاده از این اقدام، امکان پژواک صوت وجود دارد. از این اقدام می‌توان برای عیب‌یابی استفاده کرد.
10	delay_echo	این اقدام مانند اقدام echo است با این تفاوت که پژواک با تاخیر صورت می‌گیرد.
11	eavesdrop	با استفاده از این اقدام، امکان شنود تماس وجود دارد.
12	fifo	با استفاده از این اقدام، امکان ایجاد یک صف تماسی وجود دارد. این صف بر اساس سیاست موردی که ابتدا وارد صف شده است، زودتر خدمت می‌گیرد، عمل می‌نماید.
13	info	با استفاده از این اقدام، امکان مشاهده تمامی پارامترها و متغیرهای مربوط به یک کانال وجود دارد.
14	ivr	با استفاده از این اقدام، امکان راه‌اندازی یک سامانه پاسخگوی صوتی تعاملی وجود دارد.
15	transfer	برای انتقال تماس از این اقدام می‌توان استفاده نمود.
16	mkdir	با استفاده از این اقدام، می‌توان یک دایرکتوری را ایجاد نمود.
17	voicemail	با استفاده از این اقدام، امکان صندوق پستی را فراهم می‌آورد.
18	playback	از این اقدام می‌توان برای پخش یک صوت استفاده نمود.
19	record	برای ضبط یک صوت می‌توان از آن استفاده نمود.
20	record_session	با استفاده از این اقدام، امکان ضبط کل مکالمه وجود دارد.
21	stop_record_session	با استفاده از این اقدام، می‌توان ضبط صوت را خاتمه داد.
22	fax	با استفاده از این اقدام، امکان راه‌اندازی خدمت فکس برای دریافت و ارسال فکس وجود دارد.
23	say	برای خواندن یک عبارت می‌توان از این اقدام استفاده نمود.
24	sleep	برای ایجاد یک وقفه به مدت مشخص می‌توان از این اقدام استفاده نمود.
25	strftime	زمان محلی سامانه را باز می‌گرداند.
26	system	برای اجرای یک دستور در سیستم‌عامل می‌توان از این اقدام استفاده نمود.
27	lua	با استفاده از این اقدام، می‌توان اسکریپت‌های خاصی را به زبان lua اجرا نمود.

با استفاده از دستور fs_cli می‌توان به محیط خطفرمان نرم‌افزار freeswitch متصل شد. این دستور امکانات مختلفی را فراهم می‌آورد. این امکانات شامل مشاهده رویدادهای صورت گرفته در سامانه، مشاهده تماس‌های در حال انجام، نمایش کانال ها و موارد دیگر است. یکی از کاربردهای اصلی این دستور، بازنوسازی[19] freeswitch است.

در مسیر /usr/local/freeswitch/conf، مسیر فایلهای پیکربندی این نرم‌افزار است. پروفایلهای SIP، برای گوش دادن به درخواست های SIP هستند که به سمت کارگزار freeswitch می‌آیند. پورتی که کارگزار freeswitch به صورت پیش‌فرض به آن گوش می‌کند، پورت 5060 است. این پروفایلها شامل پروفایل Internal، External و نسخه‌های IPv6 آن است. نوع Internal برای تماس‌های داخلی و نوع External، برای تماس‌های خارجی است. در فایل SIPProfile، امکان تعیین پورت جهت دریافت بسته‌های پروتکل SIP، تعیین نوع کدکها و موارد مشابه وجود دارد.

برای ساخت دامنه کافی است تا در مسیر conf/directory مراجعه شود و سپس یک دایرکتوری و یک فایل xml با نام مورد نظر ایجاد گردد. سپس بایستی فایل xml باز شود و نام دامنه مورد نظر و دایرکتوری آن در تنظیمات آن مشخص گردد.

پس از ایجاد تغییرات، بایستی با استفاده از دستور fsctl shutdown restart، نرم‌افزار راه اندازی مجدد گردد. پس از ساختن دامنه، امکان تعریف داخلی ها وجود دارد. برای این منظور کافی است تا وارد دایرکتوری ایجاد شده برای دامنه شویم و یک فایل را به ازای هر داخلی ایجاد نماییم. در این فایل بایستی مقدار user-context را برابر نام دامنه قرار دهیم. برای اعمال این تغییرات بایستی وارد محیط fs_cli شویم و دستور reloadxml را اجرا نماییم. اکنون وارد سافت فون شده و مقدار داخلی و ID را برابر مقدار داخلی تعریف شده قرار می‌دهیم و مقدار نام دامنه را برابر مقدار تعریف شده قرار می‌دهیم. با اجرای این اقدامات، سافت فون متصل شده و در حالت on hook قرار می‌گیرد. در این حالت، سافت فون آماده دریافت تماس ها است.[5]

[19] refresh

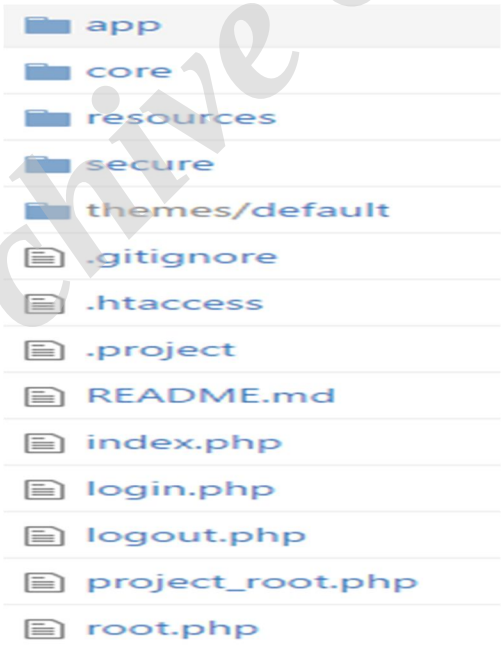
ACECR-PBX2,3

1,2,3 مقدمه

در این پروژه که یک واسط وبی سفارشی و انعطاف‌پذیر را برای سامانه سوییچ صوتی freeswitch طراحی نموده ایم. این نرم‌افزار را می‌توان روی سیستم‌عامل‌های مختلف اجرا نمود. با این وجود برای سیستم عامل Debian نسخه هشت، بهینه‌سازی شده است. این نرم‌افزار واسط گرافیکی را در اختیار می‌گذارد که به کمک آن امکان استفاده از قابلیت‌های مختلف سامانه freeswitch به شیوه‌ای آسان فراهم می‌شود.

2,2,3 ساختار پروژه

این پروژه به صورت عمده مبتنی بر زبان برنامه‌نویسی سمت کارگزار PHP، و زبان سمت کارخواه Javascript است. در شکل 1، ساختار کلی این پروژه نمایش داده شده است.



شکل 3-3: ساختار کلی پروژه ACECR-PBX

همانطور که در این شکل مشخص است، این پروژه شامل پوشه‌های app، core، resources، secure و theme است. پوشه‌ی app شامل کاربردهای مختلف است که در جدول 3- 3 به آنها اشاره شده است. پوشه‌ی core شامل قابلیت‌های اساسی سامانه مانند هویت‌سنجی، ارتباط با پایگاه داده، مدیریت کاربران، منوی نرم‌افزار و موارد دیگری از این دست است. پوشه resources دارای منابع مورد نیاز برای پروژه است که شامل فونت‌ها و کتابخانه‌ها می‌باشد. در ادامه به کتابخانه‌های مورد استفاده توسط این پروژه پرداخته شده است. لازم به ذکر است که در این پروژه از موتور تولید قالب[20] smarty استفاده شده است. یکی دیگر از پوشه‌های این پروژه، پوشه‌ی themes می‌باشد که تم‌های ظاهری مختلف برای وبسایت، در آن وجود دارد. به صورت پیش‌فرض، سامانه تنها دارای یک تم با نام default است.

جدول 3-3: کاربردهای موجود در پوشه app

کنترل دسترسی	پشتیبان‌گیری	گسترش‌ها[21]	رایانامه
فکس	دروازه‌ها	نمایش‌دهنده‌ی رویدادنگاشت‌ها[22]	صندوق صوتی
صف	نقشه تماس	کنفرانس	و موارد دیگر

در پیاده‌سازی این پروژه، از تکنولوژی‌های مختلفی در سمت کارگزار و نیز در سمت کارخواه استفاده شده است. برای مثال، چارچوب کاری Bootstrap، یک چارچوب کاری زبان CSS است که در این پروژه مورد استفاده قرار گرفته است. از طرف دیگر، jquery یکی از محبوب‌ترین کتابخانه‌های زبان جاوااسکریپت است که در این پروژه مورد استفاده قرار گرفته است. به عنوان یک نمونه‌ی دیگر، می‌توان به momentjs اشاره کرد که یک کتابخانه‌ی جاوااسکریپت برای تجزیه، اعتبارسنجی، دستکاری و فرمت‌دهی به تاریخ است.

در سمت کارگزار نیز کتابخانه‌های مختلفی برای تحقق اهداف پروژه به کار گرفته شده است. برای نمونه، از کتابخانه‌ی FPDI که یک کتابخانه‌ی زبان PHP می‌باشد، جهت خواندن صفحات موجود در اسناد PDF استفاده شده است. لازم به ذکر است برای تولید اسناد PDF، بدون نیاز به افزودن گسترش‌های خارجی، از کتابخانه‌ی دیگری استفاده شده است که

[20] templating engine
[21] extension
[22] log viewer

TCPDF نام دارد. این کتابخانه مبتنی بر Unicode است و از زبان‌های راست به چپ پشتیبانی می‌نماید. علاوه بر این، در این پروژه از کتابخانه‌ی PHPMailer جهت ارسال رایانامه بهره برداری شده است.

3,2,3 مزایا

- افزودن قابلیتهای بیشتر به پلتفرم صوت روی اینترنت freeswitch
- آسان کردن مدیریت freeswitch به دلیل ارائه‌ی یک واسط کاربری گرافیکی کاربرپسند
- جذب کاربران به دلیل طراحی یک واسط گرافیکی همه‌منظوره

4,2,3 قابلیت‌ها

در جدول زیر به قابلیت‌های اصلی نرم‌افزار ACECR-PBX پرداخته شده است.

جدول 3-4: قابلیت ها

مسدودسازی تماس	مخابره‌ی تماس[23]	جریان‌های تماس[24]	مرکز تماس[25]
رکوردهای جزییات تماس[26]	مرکز کنفرانس[27]	دفترچه تماس[28]	کارگزار فکس
تعقیب تماس[29]	Hot Desking	منوهای IVR	گروه‌های زنگ[30]
چنداستیجاری بودن	موسیقی انتظار[31]	صف	ضبط صوت
شروط زمانی[32]	WebRTC	صندوق صوتی[33]	و بسیاری موارد دیگر

3,3 PostgresSQL

[۲۳] Call Broadcast
[۲۴] Call Flows
[۲۵] Call Center
[۲۶] Call Detail Records (CDR)
[۲۷] Conference Center
[۲۸] Contacts
[۲۹] Follow-Me
[۳۰] Ring Group
[۳۱] Music on Hold
[۳۲] Time Conditions
[۳۳] voicemail

این پایگاه داده، یک سامانه پایگاه‌داده‌ای شیء-رابطه‌ای[34] متن‌باز است. به عنوان یک کارگزار پایگاه‌داده، عملکرد اصلی آن ذخیره‌سازی امن داده‌ها، و نیز بازیابی آنها در زمان درخواست است. این پایگاه‌داده توانایی مدیریت بارهای کاری کوچک تک‌ماشینه تا کاربردهای تحت اینترنت بزرگ را دارد. این پایگاه داده قادر است تا به درخواستهای تعداد زیادی کاربر همزمان پاسخ بدهد. این پایگاه‌داده، سازگار با خصوصیات ACID است. این پایگاه‌داده از مفاهیمی مانند دید[35]، تریگرها[36]، کلیدهای خارجی[37] و روال‌های ذخیره‌شده[38] پشتیبانی می‌نماید. این نرم‌افزار روی تمامی سیستم‌عامل‌های عمده قابل استفاده است و در آن می‌توان انواع رسانه‌ها مانند متن، تصویر، صوت و ویدیو را ذخیره نمود. این نرم‌افزار از واسطهای مختلفی در زبانهایی مانند C، C++، Java، Perl، Python و غیره پشتیبانی می‌نماید. برای مدیریت این سامانه پایگاه‌داده‌ای می‌توان از نرم‌افزارهای مختلفی مانند pgAdmin بهره جست.

در این نرم‌افزار، یک شما تمامی اشیاء را به استثنای نقش‌ها[39] و فضاهای جدولی[40] ذخیره می‌نماید. شماها به صورت کارآمدی مانند فضاهای نام عمل می‌کنند و این امکان را برای اشیای همنام فراهم می‌آورند تا در یک پایگاه‌داده واحد همزیستی کنند. به صورت پیش‌فرض، پایگاه‌داده‌های تازه ایجاد شده یک شما با نام «public» دارند، ولی هر شمای جدیدی را می‌توان به آن افزود. این پایگاه داده از نوع داده‌های مختلفی پشتیبانی می‌نماید. از این میان می‌توان به مواردی مانند نوع داده‌ی بولین، عددی، کاراکتری، باینری، زمان/تاریخ، پول، رشته‌های بیتی، مرکب، آرایه، آدرس‌های IPv4 و IPv6 اشاره نمود. علاوه بر این، این پایگاه‌داده از نوع داده‌های پیشرفته‌تری مانند XML و JSON پشتیبانی می‌نماید.

Nginx 4,3

مقدمه

کارگزار Nginx، یک کارگزار وب است که می‌توان از آن در کاربردهای دیگری مانند میانجی معکوس[41]، متوازن‌کننده‌ی بار و کَش پروتکل HTTP[42] استفاده نمود. این نرم‌افزار، یک نرم‌افزار متن‌باز است که جواز آن بر اساس

---

[34] object-relational database system
[35] view
[36] trigger
[37] foreign key
[38] stored procedure
[39] roles
[40] tablespace
[41] reverse proxy
[42] HTTP cache

جواز BSD ارائه شده است. این نرم‌افزار در ابتدا برای حد مسئله‌ی 10K مطرح شد که به مفهوم ارائه خدمت به 10 هزار اتصال همزمان است. این نرم‌افزار را می‌توان به عنوان یک کارگزار وب مستقل مورد استفاده قرار داد و یا اینکه از آن به عنوان میانجی معکوس در جلوی کارگزارهای وب دیگر استفاده کرد.

این نرم‌افزار از رویکرد غیرهمزمان و مبتنی بر رویداد برای مدیریت درخواست‌ها استفاده می‌نماید. معماری مبتنی بر رویداد و ماژولار آن می‌تواند کارایی پیش‌بینی‌پذیرتری را در بار بالا از خود به نمایش بگذارد.

4. امنیت

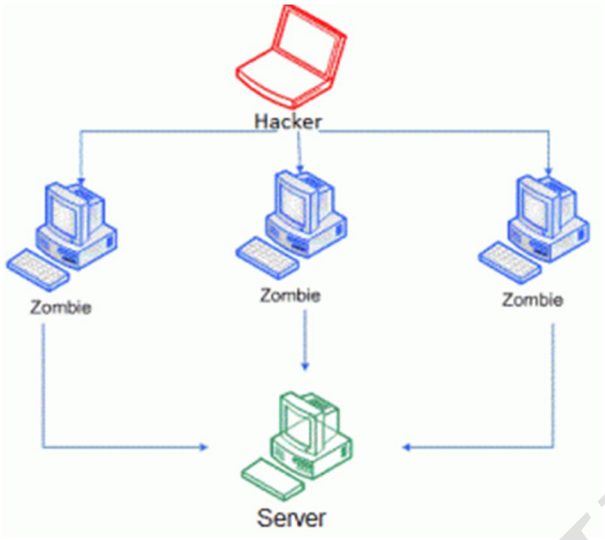
جهت برقراری امنیت، بایستی از گذرواژه‌های قوی، دیواره‌های آتش و دسترسی از طریق پوسته امن[43] استفاده نمود. علاوه بر این لازم است تا همواره از نسخه‌های به‌روز نرم‌افزارهای مختلف موردنیاز استفاده کرد. این مسئله شامل خود سیستم‌عامل، freeswitch و ACECR-PBXمی‌شود.

در این بخش تلاش می‌شود تا به معرفی حملاتی پرداخته شود که در یک سامانه صوت روی اینترنت ممکن است، رخ دهد. حملات ممکن است یک یا چند جنبه‌ی مثلث محرمانگی-جامعیت-دسترسی‌پذیری[44] را تحت‌الشعاع قرار دهند.

سیلابی کردن تماس‌ها[45]: در این حمله مهاجم، ترافیک سنگینی شامل بسته‌های سیگنال‌دهی و یا رسانه‌ای را به سامانه هدف که می‌توان کارگزارهای صوت روی اینترنت باشد، ارسال می‌نماید. این حمله می‌تواند منجر به شکست سامانه و یا کاهش کارایی آن باشد (6). این حمله در دسته‌بندی کلی‌تری به نام حملات منع خدمت جای می‌گیرد. نوع توزیع‌شده‌ی این حمله، حمله‌ی منع خدمت توزیع‌شده[46] نام دارد که در آن، مهاجم با آلوده کردن تعداد زیادی از رایانه‌های داخل یا خارج از شبکه، در یک زمان شروع به ارسال درخواست‌های انبوهی به سمت سامانه‌ی هدف می‌نماید. این امر در نهایت شکست سامانه‌ی هدف می‌گردد.

یک حمله‌ی سیلابی معمولاً از طریق دستور ping صورت می‌پذیرد. این دستور از پروتکل ICMP استفاده می‌نماید. علاوه بر این، مهاجم ممکن است از سیلابی کردن بسته‌ی SYN در پروتکل TCP برای این منظور استفاده نماید. از آنجایی که این حملات ممکن است از مکان‌های گسترده و متفاوتی نشات بگیرد، مقابله با آنها بسیار دشوار است (7).

[43] secure shell (SSH)
[44] Confidentiality – Integrity – Availability (CIA)
[45] call flooding
[46] Distributed Denial of Service (DDOS)



شکل 3-4: شمای حمله ی DDoS

پیام‌های بدشکل[47]: در این حمله، مهاجم ممکن است پیام‌های بدشکلی را به یک کارگزار هدف ایجاد و ارسال نماید. هدف وی از این اقدام می‌تواند قطع خدمت‌رسانی باشد. منظور از یک پیام بدشکل، یک پیام پروتکلی است که نحو[48] آن به درستی رعایت نشده است. کارگزاری که این نوع پیام را دریافت نماید، ممکن است واکنش‌های مختلفی را از خود نشان دهد که وابسته به نوع پیاده‌سازی است. برای مثال ممکن است وارد یک حلقه‌ی بینهایت شود یا امکان پردازش پیام‌های عادی دیگر را نداشته باشد و یا حتی، دچار شکست کامل شود (6).

پیام‌های جعلی[49]: در این حمله، مهاجم پیام‌های قلابی را در یک نشست صوت روی اینترنت خاص ارسال می‌نماید تا از این طریق بتواند خدمت را قطع نماید و یا اینکه نشست را سرقت نماید. یکی از نمونه‌های این حملات، حمله‌ی خاتمه دادن به تماس است که در آن مهاجم، یک پیام اتمام تماس (مانند بسته‌ی Bye در پروتکل SIP) را ایجاد و برای طرف مقابل ارسال می‌نماید. برای اجرای این حمله نیاز به سرقت اطلاعات نشست (مانند CallerID) وجود دارد (6).

سرقت تماس[50]: این حمله زمانی رخ می‌دهد که برخی تراکنش‌ها بین دو طرف تماس، توسط یک مهاجم دریافت شود. این تراکنش‌ها ممکن است یک درخواست ثبت‌نام[51]، راه‌اندازی تماس[52]، یک جریان رسانه‌ای[53] و موارد دیگری از این دست

---

[47] malformed message
[48] syntax
[49] Spoofed Message
[50] Call Hijacking

باشد. این سرقت ممکن است با مختل کردن ارتباط کاربران مجاز با سامانه صوت روی اینترنت، سبب قطعی خدمت شود. نمونه‌های متداولی از این حمله شامل سرقت ثبت‌نام و سرعت نشست رسانه‌ای می‌باشد (6).

شنود رسانه[54]: در این حمله، یک دسترسی غیرمجاز به بسته‌های رسانه ایجاد می‌شود. برای اجرای این حمله معمولاً دو روش وجود دارد. در روش اول، تلاش می‌شود به یک دستگاه سخت‌افزاری مانند یک سوییچ لایه دو دسترسی ایجاد شود و با استفاده از این دسترسی، بسته‌های رسانه رونوشت‌برداری شوند و برای مهاجم ارسال شود. در روش دوم، مهاجم مسیر اصلی ارسال رسانه را مورد شنود قرار می‌دهد که مانند روش‌های سنتی شنود در شبکه‌های PSTN است. برای مثال، مهاجم ممکن است به خط T1 دسترسی پیدا کند و بسته‌های رسانه را از این طریق مورد شنود قرار دهد (6).

رهگیری الگوی تماس[55]: در حمله، مهاجم بدون داشتن مجوزهای لازم، به تحلیل ترافیک صوت روی اینترنت می‌پردازد تا از این طریق یک دستگاه، اطلاعات دسترسی یک کارگزار خاص مانند آدرس IP و پورت آن، پروتکل‌های مورد استفاده یا آسیب‌پذیری خاصی از شبکه را بیابد (6).

بازمسیردهی تماس[56]: این حمله در واقع، تغییر بدون مجوز روی جهت تماس است که با دستکاری اطلاعات مسیردهی در پیامهای سیگنال‌دهی روی می‌دهد. حاصل این حمله، خارج شدن کاربران مجاز از مسیر سرویس‌دهی، و یا داخل شدن کاربران بدون مجوز به مسیر سرویس‌دهی است (6).

تزریق رسانه[57]: در این حمله، مهاجم بسته‌های جدید رسانه را به یک کانال فعال رسانه تزریق می‌نماید. پیامد این عمل این است که قربانی حمله ممکن است تبلیغات، نویز یا سکوت را در میانه‌ی مکالمه بشنود (6).

کاهش کیفیت رسانه[58]: حمله‌ای که در آن مهاجم تلاش می‌کند با دستکاری بسته‌های رسانه یا بسته‌های کنترل رسانه مربوط به یک نشست برقرارشده، کیفیت مکالمه را کاهش دهد. برای مثال مهاجم ممکن است شماره دنباله‌ی بسته‌های

---

[51] registration
[52] call setup
[53] media flow
[54] Media Eavesdropping
[55] Call Pattern Tracking
[56] Call Rerouting
[57] media injection
[58] media degrading

RTCP را در میانه‌ی مسیر دستکاری کند و با این کار، سبب شود تا دستگاه دریافت کننده، رسانه‌ی دریافتی را به ترتیب نادرستی پخش کند که این امر منجر به کاهش کیفیت مکالمه شود (6).

حملات BruteForce: در این حملات مهاجم تلاش می‌کند تا مقادیر مختلف نام کاربری و گذرواژه را برای هویت‌سنجی به سامانه بیازماید و یا اینکه تلاش می‌کند کلید رمزنگاری را با همین راهکار بدست آورد و با استفاده از آن، پیام‌های رمزشده را رمزگشایی نماید. برای مثال مهاجم ممکن است با استفاده از این روش به صفحه ورود Telnet حمله نماید و با دسترسی به سامانه از طریق پروتکل telnet، دستورات مخربی را روی سامانه اجرا نماید (7).

دسته‌ی دیگری از حملات، حملات مهندسی اجتماعی هستند. این حملات، مستقیماً اشخاص را هدف می‌گیرند. برای مثال، پیکربندی نادرست، عیب‌ها و یا راه‌اندازی نادرست یک پروتکل در سامانه‌ی صوت روی اینترنت، می‌تواند اجرای حملاتی را که در آنها هویت شخص به اشتباه ارائه شود، تسهیل نماید. در روش‌های مهندسی اجتماعی، از تکنیک‌های مختلفی برای فریب اشخاص و دسترسی به اطلاعات حساس استفاده می‌شود (10).

تهدید امنیتی دیگر، مربوط به ارسال اسپم روی شبکه‌ی سامانه‌های صوت روی اینترنت است که از آن با عنوان SPIT [59] یاد می‌شود. سامانه‌های صوت روی اینترنت، مانند کاربردهای اینترنتی نظیر رایانامه، در معرض ارسال اسپم هستند. در یک سامانه‌ی تلفنی، اسپم می‌تواند به شکل تماس‌های بی‌هدف باشد. البته این تماس‌ها ممکن است اهدافی مانند تبلیغات را دنبال کنند. در این حمله، مهاجم کارگزارهایی را که هر یک حاوی فهرستی از شماره‌های تماس است، راه‌اندازی می‌نماید. سپس این کارگزارها، شماره‌های موجود در فهرست را شماره‌گیری می‌نمایند و پیام‌هایی را منتقل می‌نمایند. این پیام‌ها ممکن است در خلال تماس پخش شوند و یا صندوق صوتی قربانی را پر کنند (9).

حملات فیزیکی نیز دسته‌ای دیگر از حملات هستند که در آنها، مهاجم دسترسی فیزیکی به تجهیزات مربوط به سامانه‌های صوت روی اینترنت دارد و می‌تواند انواع حملات را طراحی نماید (10).

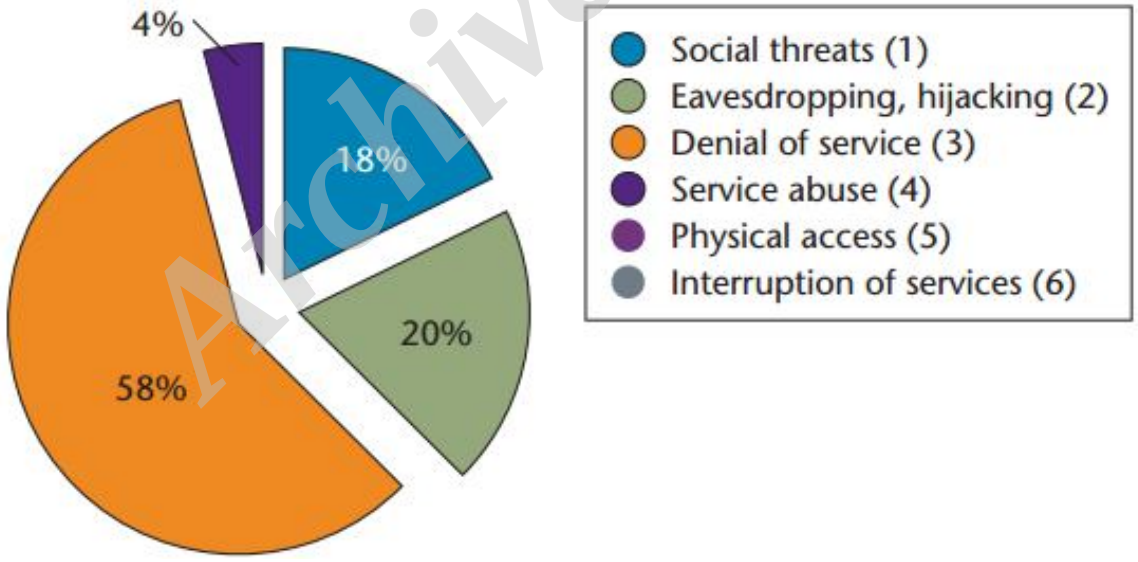
جدول 3-5 : جنبه های اثرگذاری حملات روی ابعاد CIA

جنبه‌ی تاثیر روی CIA / حمله	محرمانگی	جامعیت	دسترسی‌پذیری

[59] spam over Internet telephony

سیلابی کردن تماس‌ها			✓
پیام‌های بدشکل			✓
پیام‌های جعلی			✓
سرقت تماس			✓
شنود رسانه	✓		
رهگیری الگوی تماس	✓		
بازمسیردهی تماس		✓	
تزریق رسانه		✓	
کاهش کیفیت رسانه		✓	
حملات BruteForce	✓		
SPIT			✓

در شکل زیر، فراوانی حملات در زمینه‌ی صوت روی اینترنت نشان داده شده است. همانطور که مشخص است، تهدیدات مهندسی اجتماعی، سهم بیشتری را به خود اختصاص داده است (8).



شکل 3-5 : فراوانی حملات در زمینه ی صوت روی اینترنت

1,4 قابلیت‌های امنیتی پروتکل‌های صوت روی اینترنت

به منظور جلوگیری از حملات برشمرده شده در بالا، و کمک به استقرار سامانه‌های صوت روی اینترنت امن، پروتکل‌های صوت روی اینترنت مانند SIP و RTP، سازوکارهای امنیتی مشخصی را به عنوان بخشی از پروتکل خود ارائه می‌دهند و یا استفاده از یک راهکار ترکیبی را با کمک پروتکل‌های امنیتی مانند IPSec، SRTP و غیره پیشنهاد می‌دهند. در ادامه، قابلیت‌های امنیتی پروتکل‌های متداول صوت روی اینترنت مورد بررسی قرار می‌گیرد.

قابلیت‌های امنیتی پروتکل SIP

پروتکل SIP، چندین قابلیت امنیتی را توصیف می‌نماید. اصلی‌ترین قابلیت‌های امنیتی این پروتکل شامل موارد زیر است:

- هویت‌سنجی پیام: پروتکل SIP از هویت‌سنجی پیام‌های سیگنال‌دهی ثبت‌نام (پیام REGISTER)، دعوت (پیام INVITE) و پیام پایان مکالمه (پیام BYE) اطمینان حاصل می‌نماید. این امر جلوی حملاتی نظیر سرقت ثبت‌نام را می‌گیرد و امکانی را برای برقراری تماس غیرمجاز باقی نمی‌گذارد.
- رمزنگاری پیام: پروتکل SIP برای برآورده سازی این امکان، وابسته به پروتکل امنیتی S/MIME است تا به کمک آن، سرآیند پیام‌های سیگنال‌دهی را (به غیر از فیلدهای Via و Route) رمزنگاری نماید. با استفاده از این امکان، می‌توان محرمانگی، جامعیت و هویت‌سنجی را بین نقاط انتهایی تماس به وجود آورد.
- رمزنگاری رسانه: با استفاده از پروتکل SRTP، امکان رمزنگاری بسته‌های رسانه وجود دارد که به وسیله‌ی آن، محرمانگی و جامعیت رسانه‌ی مبادله‌شده فراهم می‌آید.
- امنیت لایه شبکه: پروتکل TLS، به منظور برآورده سازی امنیت لایه‌ی حمل پیام‌های SIP (درخواست‌ها و پاسخ‌ها) مورد استفاده قرار می‌گیرد. با استفاده از این پروتکل، کل درخواست‌ها و پاسخ‌های SIP رمزنگاری می‌شوند که به این دلیل، رمزنگاری و جامعیت پیام‌ها تضمین می‌گردد.

- امنیت لایه حمل: پروتکل SIP برای تحقق امنیت در لایه‌ی شبکه، به پروتکل IPSec وابسته است که امنیت ارتباطات شبکه‌های IP را با رمزنگاری و هویت‌سنجی ارتقا داده است. این پروتکل به منظور ایجاد یک کانال امن بین موجودیت‌های پروتکل SIP، به ویژه بین عامل‌های کاربری[60] و کارگزارهای میانجی قابل استفاده است.

تنها هویت‌سنجی پیام توسط پروتکل SIP در داخل این پروتکل صورت می‌پذیرد و دیگر قابلیت‌ها توسط دیگر پروتکل‌های امنیتی مانند S/MIME، SRTP، TLS و IPSEC قابل اجرا است.

قابلیت‌های امنیتی پروتکل RTP

پروتکل RTP امن (یا همان پروتکل SRTP)، یک پروفایل جدید را برای پروتکل RTP تعریف کرده است که هدفش، ارائه‌ی محرمانگی، جامعیت و هویت‌سنجی جریان‌های رسانه‌ای می‌باشد. این پروتکل علاوه بر محافظت از بسته‌های RTP، از جریان‌های داده‌ای پروتکل RTCP نیز پشتیبانی می‌نماید. طراحان پروتکل SRTP، روی توسعه‌ی پروتکلی تمرکز کرده‌اند که بتواند از یک سو، محافظت‌های لازم را برای جریان‌های رسانه‌ای برقرار نماید و از سوی دیگر، بتواند خصوصیات ضروری را برای پشتیبانی از شبکه‌های بی‌سیم و سیمی که ممکن است در آنها مسایلی مانند محدودیت پهنای باند وجود داشته باشد، حفظ نماید.

2,4 راهکارهای حفاظتی

تقسیم‌بندی شبکه[61]: در این راهکار، خدمات صوت و تصویر با استفاده از دو شبکه محلی مجازی[62] از یکدیگر جدا می‌شوند. با این کار می‌توان جلوی تاثیرات حملات روی هر کدام از این شبکه‌ها را مهار کرد و از نشر آن به شبکه‌ی دیگر جلوگیری نمود. برای مثال در صورتیکه یک حمله در شبکه‌ی داده‌ها صورت بگیرد، تاثیری روی ترافیک حیاتی صوت نخواهد گذاشت و برعکس (7). فناوری‌هایی مانند شبکه محلی مجازی، امکان تقسیم‌بندی لایه‌ی دو را به منظور جداسازی صوت از داده فراهم می‌آورند. در یک شبکه‌ی صوت روی اینترنت، دستگاه‌های پایانه‌ای مانند تلفن‌های IP، بایستی روی شبکه محلی مجازی‌ای قرار بگیرند که تنها خدمت‌های تلفنی بر مبنای IP را ارائه می‌دهد، و نه روی شبکه محلی مجازی‌ای که خدمت‌های داده‌ای را انجام می‌دهد (7).

---

[60] user agent (UA)
[61] network segmentation
[62] VLAN

تونل‌زنی[63] صوت روی اینترنت: الگوی تونل‌زنی صوت روی اینترنت، راهی را تضمین محرمانگی و جامعیت تماس‌ها ارائه می‌دهد. در این روش، داده‌های موجود در بسته‌های یک پروتکل، در جریان بسته‌های پروتکل دیگر لفافه‌سازی[64] می‌شود (2). تونل‌ها در حقیقت، اتصالات مجازی‌ای بین یک نقطه‌ی ورودی و یک نقطه‌ی خروجی هستند. در نقطه‌ی ورودی،داده‌ها با استفاده از یک روش رمزنگاری، رمز می‌شوند و در نقطه‌ی خروجی، دوباره به حالت اولیه باز می‌گردد. برای این منظور می‌توان از امکانات موجود در پروتکل‌هایی نظیر IPSec استفاده نمود (7).

رمزنگاری رسانه: محافظت از محتوای مکالمه‌ی صوتی از شنود، دغدغه‌ای بزرگ به حساب می‌آید. برای این منظور، می‌توان از گسترش امنیتی پروتکل RTP، به نام پروتکل SRTP استفاده نمود. با کمک این پروتکل، امکان رمزنگاری بسته‌های رسانه شامل صوت وجود دارد. این پروتکل علاوه بر محرمانگی، خدمت هویت‌سنجی را ارائه می‌دهد. پروتکل SRTP به گونه‌ای طراحی شده است که سربار کمی را به اندازه‌ی بسته تحمیل کند و تعداد زوج کلیدهایی که بایستی بین طرفین تماس به اشتراک گذارده شود، کمینه سازد (9).

تماس هویت‌سنجی‌شده‌ی امضا شده[65]: در این راهکار، دسترسی به خدمت‌های صوت روی اینترنت تنها زمانی اعطا می‌شود که هم هویت‌سنجی ابزار و هم هویت‌سنجی کاربر با موفقیت صورت گرفته باشد. امضای دیجیتالی، یک روش هویت‌سنجی است که در آن، مشترکان سامانه می‌توانند هویت تماس‌گیرنده را به تماس صورت گرفته از جانب وی گره بزنند. در این روش، ارسال‌کننده‌ی تماس صوتی امضاشده، هویت‌سنجی می‌شود و ارسال آن را نمی‌تواند انکار نماید (7).

غیر فعال کردن خدمت‌های غیرضروری: کارگزارهای صوت روی اینترنت، روی سیستم‌عامل‌هایی مانند لینوکس و ویندوز راه‌اندازی می‌شوند. معمولاً این سیستم‌عامل‌ها حاوی بسیاری از خدمت‌هایی می‌باشند که نیازی به آنها نیست. وجود این خدمت‌های بلااستفاده، تنها ریسک امنیتی را افزایش می‌دهد. بنابراین توصیه می‌شود تا این خدمت‌ها از روی سامانه غیرفعال شوند. برای مثال در سیستم‌عامل لینوکس، فایل /etc/inetd.conf حاوی فهرستی از خدمت‌هایی است که با هر بار اجرای سیستم‌عامل، شروع به کار می‌کنند. با بررسی این خدمت‌ها و حذف موارد غیرضروری، سطح امنیت سامانه ارتقا می‌یابد (11).

---

[63] tunneling
[64] encapsulation
[65] Signed Authenticated Call

غیر فعال کردن و یا تغییر در تنظیمات پیش فرض: یکی از اولین روش‌هایی که مهاجم برای دسترسی به سامانه از آن استفاده می‌نماید، استفاده از تنظیمات پیش‌فرض مانند گذرواژه‌های پیش‌فرض است. به همین دلیل، یکی از توصیه‌های مهم امنیتی این است که رمزهای عبور پیش‌فرض غیرفعال شوند و گذرواژه‌های مستحکم‌تری جایگزین آن شود. برای مثال، سامانه freeswitch یک گذرواژه پیش‌فرض برای ورود به صندوق پستی تمامی کاربران تعریف کرده است که در صورت عدم تغییر آن، مهاجم به سادگی می‌تواند به محتوای صندوق‌های پستی کاربران مختلف دسترسی داشته باشد (12).

رویدادنگاری[66]: در سامانه‌های لینوکس، می‌توان از خدمت syslog برای رویدادنگاری اتفاقات مختلف شامل اتفاقات امنیتی استفاده نمود. علاوه بر این، خود سامانه‌های صوت روی اینترنت نظیر freeswitch، امکانات مختلف رویدادنگاری را ارائه می‌دهند. در صورت وقوع یک حمله، با استفاده از این فایل‌های رویدادنوشت می‌توان به سرنخ‌هایی دست یافت و مولفه‌هایی که در برابر حمله دچار شکست شده‌اند، شناسایی نمود (11).

حذف برخی اطلاعات از بدنه پیام های ارسالی: بسته‌های پروتکل SIP در بدنه‌ی خود حاوی فیلدها و اطلاعاتی هستند که ممکن است توسط مهاجم مورد سوءاستفاده قرار بگیرد. . به همین دلیل، توصیه می‌گردد تا این اطلاعات با مقادیری جایگزین گردد که اطلاعاتی را در اختیار مهاجم قرار ندهد. به طور کلی، باید از انتشار هر گونه اطلاعاتی که ساختار و شبکه را برای مهاجم تا حدی مشخص می‌نماید، جلوگیری گردد که به آن اصطلاحا اختفای توپولوژی[67] گفته می‌شود. به عنوان مثال در بدنه پیام‌های پروتکل SIP، فیلدی به نام «Server» وجود دارد که در سامانه‌های تلفنی به صورت پیش‌فرض حاوی برند و مدل دستگاه و یا نرم افزار است.

تعاریف مشخص برای ترافیک های ورودی و خروجی: در سامانه‌های تلفنی باید به ازای تماس‌های ورودی و خروجی، قواعد مشخصی تعریف گردد و مسیر پیام‌های ورودی از مسیر پیام‌های خروجی به درستی جدا شود. یکی دیگر از سیاست‌های مهم برای ترافیک خروجی، جلوگیری از برقراری تماس‌های بین‌المللی است و در صورت نیاز تنها باید برای کاربران خاص فراهم گردد. برای مثال، در سامانه‌های freeswitch، می‌توان یک context به ازای هر کدام از تماس‌های داخلی و خارجی ایجاد نمود.

[٦٦] logging
[٦٧] Topology hiding

رد درخواست‌های دریافتی از موجودیت‌های ناشناس: یکی از روش‌های مهم به منظور محافظت از سامانه‌های تلفنی در برابر حملات پویش SIP[68]، عدم پذیرش درخواست‌های SIP از موجودیت‌های ناشناس است. برخی از بدافزارها با کشف سامانه صوت روی اینترنت، شروع به ارسال درخواست‌های SIP به آن کرده و سعی می‌کنند با بررسی الگوهای مختلف، راه نفوذ به این سامانه‌ها را بیابند. با رد این درخواست‌ها می‌توان از اینگونه حملات جلوگیری نمود. برای مثال، در سامانه‌ی freeswitch، می‌توان با پیکربندی مناسب فایل‌های مربوط به پروفایل SIP، درخواست‌های دریافتی از موجودیت‌های ناشناس را رد نمود.

محدود کردن دسترسی‌ها روی کارگزارهای صوت روی اینترنت: یکی از مشکلات امنیتی مهمی که در کارگزار صوت روی اینترنت بایستی مورد توجه قرار بگیرد، اعمال مجوزهای درست به کاربران و محدود کردن دسترسی آنها است. به عبارت دیگر، هر موجودیتی باید تنها به چیزی که نیاز دارد، دسترسی داشته باشد. برای مثال، دسترسی به خدمت SSH بایستی محدود شود (6). در همین راستا، نباید از دسترسی‌های کاربر ریشه برای اجرای freeswitch استفاده نمود. روش بهتر این است که یک کاربر جدید ایجاد شود و به عنوان مالک مسیر نصب freeswitch به سامانه معرفی شود. علاوه بر این، لازم است تا دسترسی‌های مناسبی را به بخش‌های مختلف نرم‌افزار اعطا نمود (12).

به‌روزرسانی مستمر: به‌روزرسانی مستمر برای هر نرم‌افزار می‌تواند سبب ارتقای امنیت سامانه شود. نرم‌افزار freeswitch نیز از این قاعده مستثنا نیست. بنابراین جهت اعمال آخرین وصله‌های امنیتی، همواره از آخرین نسخه‌ی ارائه شده برای نرم‌افزار استفاده شود (12).

محدود کردن آدرس های IP مجاز برای داخلی ها: یکی از روش‌های متداول برای ارتقای امنیت سامانه، ایجاد محدودیت برای آدرس‌های IP ای است که امکان دسترسی به سامانه را دارند. برای این منظور می‌توان از ابزار fail2ban استفاده نمود. این نرم‌افزار، ابزاری است که به منظور پایش فایل‌های رویدادنگاری و فعال‌سازی اقدامات مناسب در زمان کشف یک مورد مشکوک قابل استفاده است. این نرم‌افزار قادر است تا فایل‌های رویدادنگاری مربوط به برنامه‌های مختلف را به صورت همزمان پایش کند و انواع گوناگونی از واکنش‌ها را بر اساس آن فعال نماید (12).

[68] SIP scan

کنترل ترافیک ورودی و خروجی: با استفاده از دیواره‌آتش لینوکس که iptables نام دارد، می‌توان ترافیک ورودی و خروجی کارگزار را کنترل نمود. این امر سبب می‌شود تا تنها ترافیک مجاز، امکان گذر از دیواره‌آتش را داشته باشد و ترافیک‌های غیرمجاز از ورود به سامانه منع شوند.

3,4 ابزارهای امنیتی

iptables

یک دیواره‌آتش بسیار انعطاف‌پذیر است که برای سیستم‌عامل لینوکس طراحی شده است. این ابزار یک نرم‌افزار خطفرمان است که از زنجیره‌های سیاستی[69] برای اجازه یا مسدودسازی ترافیک استفاده می‌نماید. وقتی که از طرف یک کاربرد، تلاش برای ایجاد یک اتصال وجود داشته باشد، این نرم‌افزار به دنبال یک قاعده در فهرست خود جهت اجازه/مسدودسازی آن اتصال می‌گردد. در صورتیکه که قاعده‌ای در این فهرست باشد، نرم‌افزار آن را تطبیق می‌دهد و عمل متناسب (اجازه یا مسدودسازی) اتصال را می‌گیرد. در صورتیکه قاعده‌ی متناسبی وجود نداشته باشد، یک عمل پیش‌فرض انتخاب و اجرا می‌شود.

این نرم‌افزار از سه نوع زنجیره پشتیبانی می‌نماید: آ. ورودی، ب. انتقال، پ. خروجی.

- ورودی: از این زنجیره می‌توان برای کنترل رفتار اتصال‌های ورودی استفاده کرد. برای مثال، در صورتیکه یک کاربر تلاش به برقراری اتصال SSH به کارگزار داشته باشد، این نرم‌افزار با استفاده از این نوع زنجیره می‌تواند آدرس IP و پورت وی را با قواعد موجود در نرم‌افزار تطبیق دهد و عمل متناسب را اجرا نماید.
- انتقال: این زنجیره برای اتصال‌های ورودی‌ای استفاده می‌شود که مقصد پیام دریافتی، سامانه‌ی فعلی نمی‌باشد. برای مثال، یک مسیریاب شبکه را در نظر بگیرید که بسته‌های مختلف در شبکه را مسیریابی می‌نماید. مسلما بسته‌هایی که به یک مسیریاب می‌رسد، قرار نیست در همانجا بماند. در این شرایط لازم است تا از زنجیره انتقال استفاده شود.

[۶۹] policy chain

- خروجی: این زنجیره برای اتصال‌های خروجی مورد استفاده قرار می‌گیرد. برای مثال، وقتی با استفاده از یک مرورگر، وبسایتی مشاهده می‌شود، درخواست‌هایی تحت پروتکل HTTP روی پورت 80 ارسال می‌گردد. در صورتیکه یک زنجیره خروجی روی این پروتکل تعریف شده باشد، امکان اجازه یا مسدودسازی اتصال وجود خواهد داشت.

Fail۲ban

این نرم‌افزار، یک چارچوب کاری جلوگیری از نفوذ است که کارگزارهای رایانه‌ای را از حملات brute-force محافظت می‌نماید. این نرم‌افزار کار خود را با پایش فایل‌های رویدادنگاری اجرا می‌نماید. از این طریق، نرم‌افزار قادر است تا برای مثال آدرس‌های IP خاصی را که تعداد ورودهای ناموفق زیادی دارند، شناسایی کرده و دسترسی آنها به سامانه را مسدود نماید. مسدودسازی می‌تواند بر اساس دیگر اقدامات ناخواسته نیز تعریف و اعمال گردد. این تعریف در یک بازه‌ی زمانی مشخص صورت می‌پذیرد. علاوه بر این، Fail2ban این قابلیت را دارد تا میزبانهای مسدودشده را بازگشایی نماید و اجازه دسترسی دوباره‌ی آنها به سامانه را فراهم آورد، زیرا ممکن است یک اتصال قابل اعتماد تنها به دلیل عدم پیکربندی مناسب، مسدود شود.

زمانی که این نرم‌افزار به منظور پایش رویدادهای یک خدمت پیکربندی شده باشد، به دنبال فیلتری که برای آن خدمت پیکربندی شده است، می‌گردد. این فیلتر به منظور شناسایی شکست‌های هویت‌سنجی برای آن خدمت خاص طراحی می‌شود که بر پایه‌ی عبارتهای منظم است. خوشبختانه، این نرم‌افزار خود شامل فیلترهایی برای خدمت‌های متداول است. وقتی که یک خط از فایل رویدادنگاری یک خدمت با عبارت منظم تعریف شده برای آن تطبیق پیدا نماید، *اقدام* تعریف شده برای آن خدمت اجرا می‌گردد. اقدام مورد نظر می‌تواند، موارد مختلفی را شامل شود، ولی عمل پیش‌فرض، مسدودسازی آدرس IP میزبان است که از طریق ایجاد تغییراتی در قواعد دیواره‌آتش iptables صورت می‌پذیرد. این امکان وجود دارد که این اقدام به نحوی که شامل ارسال رایانامه به یک مدیر شبکه شود، گسترش یابد. لازم به ذکر است که امکان تغییر هدف اقدام[70]، به چیزی غیر از iptables (که هدف اقدام پیش‌فرض است)، وجود دارد.

۷۰ action target

به صورت پیش‌فرض در صورتیکه سه شکست در هویت‌سنجی در ده دقیقه شناسایی شود، یک اقدام صورت می‌پذیرد. همانطور که قبلاً گفته شد، این اقدام به صورت پیش‌فرض، مسدودسازی است که برای ده دقیقه به طول می‌انجامد.

برای پیکربندی Fail2ban، فایل‌های متنوعی که در مسیر /etc/fail2ban هستند، قابل استفاده می‌باشند. برای مثال، در فایل fail2ban.conf، برخی تنظیمات عملیاتی پایه مانند روش رویدادنگاری، سوکت و شناسه پردازه پیکربندی می‌گردد. فایل مهم دیگر که مسئول پیکربندی اقدامات لازم در صورت بروز عملیات بدخواهانه است، فایل jail.conf می‌باشد. از آنجایی که ممکن است این فایل در به‌روزرسانی‌ها، دستخوش تغییر شود، بهتر است برای اجرای تنظیمات یک رونوشت از آن تهیه گردد و پیکربندی در آن انجام شود. اولین بخش این نرم‌افزار، پیش‌فرض‌هایی را برای سیاست fail2ban تعریف می‌نماید. این گزینه‌ها را می‌توان برای هر خدمت خاص، به روش دلخواه تغییر داد. برای مثال، در شکل زیر بخشی از ساختار این فایل نمایش داده شده است.

```
[DEFAULT]

ignoreip = 127.0.0.1/8
bantime = 600
findtime = 600
maxretry = 3
backend = auto
usedns = warn
destemail = root@localhost
sendername = Fail2Ban
banaction = iptables-multiport
mta = sendmail
protocol = tcp
chain = INPUT
action_ = %(banaction)s[name=%(__name__)s, port="%(port)s",
protocol="%(protocol)s", chain="%(chain)s"]
action_mw = %(banaction)s[name=%(__name__)s, port="%(port)s",
protocol="%(protocol)s", chain="%(chain)s"]
          %(mta)s-whois[name=%(__name__)s, dest="%(destemail)s",
protocol="%(protocol)s", chain="%(chain)s", sendername="%(sendername)s"]
action_mwl = %(banaction)s[name=%(__name__)s, port="%(port)s",
protocol="%(protocol)s", chain="%(chain)s"]
```

```
            %(mta)s-whois-lines[name=%(__name__)s, dest="%(destemail)s",
logpath=%(logpath)s, chain="%(chain)s", sendername="%(sendername)s"]
action = %(action_)s
```

در ابتدای این فایل، از عبارت ignoreip، برای مستثنا کردن آدرس‌های IP که باید توسط سامانه fail2ban مورد چشم‌پوشی قرار بگیرند، استفاده می‌شود. پارامتر bantime در این فایل، طول مدت مسدودسازی را بر حسب ثانیه مشخص می‌نماید. مقدار پیش‌فرض برای این پارامتر، 600 ثانیه برابر ده دقیقه است. پارامتر findtime، پنجره‌ی زمانی را مشخص می‌کند که fail2ban در آن به دنبال تلاش‌های ناموفق جهت هویت‌سنجی است. مقدار این پارامتر برابر 600 ثانیه معادل ده دقیقه در نظر گرفته شده است. پارامتر maxretry، تعداد تلاش‌های شکست‌خورده قابل تحمل در بازه زمانی findtime را مشخص می‌نماید. پارامتر banaction اقدامی که باید در زمان رسیدن به حد آستانه انجام شود، مشخص می‌نماید. لازم به ذکر است که در این فایل، می‌توان تنظیم خاص‌منظوره‌ای را برای یک خدمت مشخص تعریف نمود. برای این منظور، نام خدمت را باید داخل کروشه ذکر کرد و پارامترها را به مقادیر دلخواه، مقداردهی نمود. برای نمونه، در شکل زیر، برای خدمت SSH، تنظیمات دلخواه صورت گرفته است.

```
[SSH]

enabled     = true
port        = ssh
filter      = sshd
logpath     = /var/log/auth.log
maxretry    = 6
```

4,4 پژوهشهای مرتبط

در مقاله (13) ، به موضوع حملات منع خدمت پرداخته شده باشد و دو نوع از آن، به نام حملات سیلابی و حملات هماهنگ برای کشف[71] مورد بررسی قرار گرفته است. حملات سیلابی کارگزارهای SIP از نوع بدون‌حالت و حالت‌مند را تحت تاثیر قرار می‌دهند، حال آنکه حملات هماهنگ برای کشف، تنها کارگزارهای حالتمند SIP را درگیر می‌سازند. در این

[71] coordinated attacks for detection

مقاله، عملیات SIP، به صورت یک سامانه رویداد گسسته[72] مدلسازی شده است و یک ماشین گذار حالت[73] جدید برای این منظور طراحی گردیده است. از این ماشین گذار حالت، برای توصیف رفتار عملکردهای مختلف پروتکل SIP استفاده شده است. در این مقاله، انواع مختلفی از ناهنجاری‌هایی که ممکن است در مدل DES رخ دهد، شناسایی شده است و حملات مختلف منع خدمت به یکی از انواع ناهنجاری در مدل DES نگاشت داده شده است.

با گسترش صوت روی اینترنت، تهدیدات امنیتی آن نیز نسبت به شبکه‌های سنتی تلفن، رو به فزونی گذارده است. استفاده از زیرساخت مبتنی بر IP، و نیز استفاده از پروتکل‌های سیگنال‌دهی مانند SIP، این فناوری را موضوع حملات متنوعی ساخته است. حمله‌ی منع خدمت، به دلیل سیلابی سازی انواع مختلفی از پیام‌های SIP، یکی از شناخته شده ترین این حملات است. در این مقاله، یک روش مبتنی بر ناهنجاری به منظور جلوگیری و کشف انواع مختلفی از حملات سیلابی ارائه شده است. برای تحقق این هدف، مشخصات SIP مدل‌سازی شده است. برای مقاصد جلوگیری از وقوع این دسته حملات، یک روش مبتنی بر فیلتر بر مبنای یک لیست سفید ارائه شده است. در این مقاله ادعا شده است که روش ارائه شده، حملات ذکر شده در بالا را با دقت بیشتری نسبت به روش‌های مشابه کشف می‌نماید.(14)

در مقاله (15)، یک شمای کشف ارائه شده است که رفتارهای نامنطبق را بر اساس تحلیل آماری و تست فرضیه[74]، در یک شبکه‌ی صوت روی اینترنت شناسایی می‌نماید. شبکه‌های صوت روی اینترنت، جایگزین‌های محبوب و کم‌هزینه‌ای نسبت به شبکه‌های تلفن سنتی هستند. علاوه بر این، شبکه‌های صوت روی اینترنت، خدمت‌هایی را ارائه می‌دهند که شبکه‌های تلفن سنتی را گسترش می‌دهد (مانند خدمت followme). در نتیجه، مسایل امنیتی مختلفی مانند تماس‌های کلاهبرداری در این شبکه‌ها ظهور می‌کنند. به همین خاطر، جلوگیری و کشف کاربرانی که رفتاری غیرمنطبق دارند، ضروری است. روش ارائه شده در این مقاله، یک شمای کنترل رفتار را برای کارخواه‌های صوت روی اینترنت ارائه می‌دهد. برای تطبیق رفتار کاربران، از تحلیل آماری استفاده می‌شود.

---

[72] discrete event system (DES)
[73] state transition machine
[74] hypothesis testing

یکی از کارآمدترین سازوکارهای دفاعی علیه تهدیدات، ایجاد سامانه‌ی هوش تهدید[75] و سامانه‌ی هشدار سریع، و نیز فهم رفتار، توانایی‌ها و قصد مهاجم است. سامانه‌های هوش تهدید و هشدار سریع، نیاز به همکاری فیمابین شرکت‌کنندگان قانونی‌ای دارد که راهکارها و خدمت‌های امنیت سایبری را ارائه کرده‌اند. خدمت‌های امنیت سایبری بخشی از مدیریت امنیت سایبری مبتنی بر اطلاعات است و در حقیقت، نتیجه‌ی به اشتراک‌گذاری اطلاعاتی است که از راهکارهای امنیت سایبری مانند دیواره‌آتش‌های نسل بعد،[76] و دیواره‌آتش‌های صوت روی اینترنت و وب به دست آمده است. یک خدمت امنیت سایبری، اطلاعات به موقع و دقیقی را در مورد منابع شناخته‌شده‌ی بدخواه[77] مانند یک کاربرد، آدرس وبی، یا یک فایل در اختیار می‌گذارد. در این مقاله، یک مدل مرکز اعتماد مبتنی بر اعتبار[78]، به عنوان یک سامانه‌ی هوش تهدید ارائه شده است که از خدمت‌های امنیت سایبری مبتنی بر VOIPبه منظور گزارش منابع بدخواه استفاده می‌نماید. این مدل، ساختاری بازدارنده دارد که مبتنی بر روش‌های ساده‌ی ریاضی می‌باشد.(16)

با افزایش محبوبیت خدمت‌های صوت روی اینترنت، انواع مختلف حملات بر ضد آنها نیز در حال افزایش است. پروتکل اصلی مورد استفاده در فناوری صوت روی اینترنت، پروتکل SIP است. این پروتکل، موضوع حملات متنوعی است که از جمله‌ی آنها می‌توان به حمله‌ی منع خدمت اشاره نمود. این مقاله، گزارشی از آزمایش‌های صورت گرفته روی محیط شبیه‌سازی‌شده‌ی صوت روی اینترنت با استفاده از ابزارها و فناوری‌های متن‌باز این حوزه را ارائه داده است. این سامانه‌ی صوت روی اینترنت شبیه‌سازی‌شده به منظور نمایش یک ارتباط معمولی صوت روی اینترنت، اجرای حملات سیلابی منع خدمت علیه پروتکل SIP، و پیاده‌سازی یک سامانه‌ی کشف نفوذ[79] مبتنی بر Snort مورد استفاده قرار گرفته است. این سامانه توانایی گرفتن پیام‌های SIP مشکوک را دارد. علاوه بر این، در این مقاله یک معماری صوت روی اینترنت جدید ارائه شده است که مبتنی بر بافر کردن تمامی پیام‌های ورودی ارسالی از سمت کارخواهان است و هدفش، پردازش پیام‌ها داخل بافر، و قبل از ارسال آنها به مقصد می‌باشد.(17)

پروتکل SIP، یک پروتکل سیگنال‌دهی محبوب است که به منظور مدیریت ارتباطات بین عامل‌های کاربری مختلف ارتباطات صوت روی اینترنت مورد استفاده قرار می‌گیرد. این پروتکل، یک پروتکل متنی است. به همین دلیل نسبت به

---

[۷۵] threat intelligence
[۷۶] Next-Generation Firewall (NGFW)
[۷۷] malicious
[۷۸] reputation
[۷۹] Intrusion Detection System (IDS)

حملات سیلابی آسیب‌پذیر است. این حمله می‌تواند با درگیر کردن منابع مانند پردازنده و حافظه اصلی، سامانه‌ی صوت روی اینترنت را عملاً از کار بیاندازد. بنابراین، بایستی اقدامات لازم برای کشف این حملات انجام شود. در این مقاله، یک ابزار به نام VoIPFD ارائه شده است که یک کشف‌کننده‌ی ناهنجاری[80] به منظور کشف حملات سیلابی ضد پروتکل SIP به حساب می‌آید. مانند هر کشف‌کننده‌ی ناهنجاری دیگر، این ابزار پروفایل نرمال SIP را به صورت یک توزیع احتمالی مدل می‌نماید. توزیع استفاده شده برای این منظور، توزیع احتمالی پواسون است. پیام‌هایی که نسبت به این مدل احتمالی انحراف داشته باشند، به عنوان پیام‌های مشکوک SIP شناسایی می‌شوند.(18)

صوت روی اینترنت، فناوری‌ای است که ارتباطات صوتی بلادرنگ را روی بستر شبکه‌های سوییچ بسته با استفاده از پشته‌ی پروتکلی TCP/IP فراهم می‌آورد. این فناوری به سرعت در حال گسترش است و توسعه‌ی آن پیچیده می‌باشد. از آنجایی که سامانه‌های صوت روی اینترنت در محیط‌های باز استقرار می‌یابند، در معرض همان تهدیداتی هستند که سامانه‌های دیگر مستقر در اینترنت با آن مواجهند. یکی از مهترین این تهدیدات، حملات منع خدمت است که در شبکه‌های اینترنتی به وفور اتفاق می‌افتد. در این مقاله، هدف تحلیل و ارزیابی راهکارهای مقابله با این حملات است. در این مقاله، روش‌های مختلف جلوگیری و کشف حملات منع خدمت مورد ارزیابی قرار گرفته است و یک حمله‌ی سیلابی مبتنی بر SIP علیه یک کارگزار SIP شبیه‌سازی شده است. سپس نتایج آزمایش به منظور ارائه‌ی یک روش مقابله‌ای جدید مورد استفاده قرار گرفته شده است. این روش شامل پیاده‌سازی نرم‌افزار Snort در حالت درخط[81] به عنوان سامانه محافظت از نفوذ[82] است. علاوه بر این نرم‌افزار، از ابزار iptables به منظور برقراری امنیت کارگزار SIP مورد استفاده قرار گرفته است.(19)

5. پارامترهای مقیاس پذیری

1. تعداد نامحدود دامنه

از پارامترهای مهم در ارزیابی مقیاس پذیری امکان ایجاد دامنه های مختلف می باشد. در این راستا در Freeswitch امکان ایجاد دامنه های مختلف مدنظر قرار گرفته است. بدین ترتیب می توان داخلی های مختلف

[80] anomaly detector
[81] inline mode
[82] Intrusion Protection System (IPS)

را ثبت نمود. بدین ترتیب مدیریت هدفمند داخلی ها و افزایش آن ها را بدنبال دارد. بنابراین این ویژگی بعنوان یکی از راهکارهای اساسی در پاسخگویی به تنوع و تعدد سرویس های مبتنی بر VOIP مدنظر کارشناسان می باشد.

2. سرویس های نامحدود

پارامتر دیگر در ارزیابی مقیاس پذیری یک سیستم، امکان سرویس های نامحدود می باشد. وجود سرویس های متنوع و یکپارچه سازی آنها در ارائه از چالش های این حوزه می باشد. بنابراین سیستمی که بتواند مدیریت جامعی روی این سرویس های متنوع داشته باشد از در اولویت بکارگیری در این حوزه می باشد. برای مثال، می‌توان تعداد نامحدود داخلی را در یک دامنه‌ی مشخص تعریف نمود.

3. SIP profiles

با وجود SIP profile های مختلف، امکان مجزاسازی فراهم می گردد. بنابراین با مدیریت پورت های مختلف روبرو می باشیم که این خود نقش بسزائی در افزایش کنترل و امنیت سیستم ایفاء می نماید.

مقایسه Asterisk و Freeswitch از منظر مقیاس پذیری

در بخش قبل پارامترهای اساسی ارزیابی مقیاس پذیری لیست شد و در مورد آن بررسی انجام شد. حال به بررسی دو سیستم برتر در این حوزه می پردازیم. همانطور که در گزارش مقطع اول بیان شد. پس از مطالعات میدانی بنا به مقالات، متون و تجربیات متخصصین در این حوزه، به تعریف معیارهای ارزیابی پرداخته شد. سپس سیستم های متن باز مختلف مورد ارزیابی قرار گرفت. در این میان تست های عملیاتی نیز بر روی آنها انجام شد. در هر مرحله متن باز ها که حائز شرایط بودند انتخاب و در وارد ارزیابی مرحله بعد می شدند. این فرآیند ادامه پیدا کرد تا اینکه دو سیستم متن باز باقی ماندند. در آخر ارزیابی تنها بر روی این دو انجام شد. حال در این بخش، بعد دیگری از ارزیابی بنام مقیاس پذیری را مدنظر قرار می دهیم.

در ابتدا باید معماری کلی دو سیستم را مدنظر قرار داد. معماری Asterisk شامل یک هسته‌ی بزرگ است، حال آنکه freeswitch شامل یک هسته‌ی کوچک به همراه مولفه‌های اقماری است. این معماری freeswitch، بستر مناسب‌تری را جهت مقیاس‌پذیری در اختیار می‌گذارد.

در مورد پارامتر اول باید گفت که Asterisk قابلیت دامنه مختلف را ندارد و به عبارت دیگر دارای proxy server نمی باشد. پس بتنهایی Asterisk این ویژگی را ندارد. اما freeswitch این قابلیت را دارد که این خود از علل فراگیری استفاده از آن می باشد.

در ساختار freeswitch، Proxy سیستم قابلیت ترجمه Domain های مختلف دارد بنابراین این ویژگی خود سبب بهره برداری از دامنه های مختلف را فراهم می سازد. همچنین با وجود SIP profile های مختلف می توان قابلیت مقیاس پذیری آن را افزایش داد.

پس به طورکلی Asterisk دارای محدودیت مقیاس پذیری می باشد اما freeswitch دارای قابلیت مقیاس پذیری بسیار بالاتری می باشد و بعنوان یک راهکار در این حوزه قابل تعریف است.

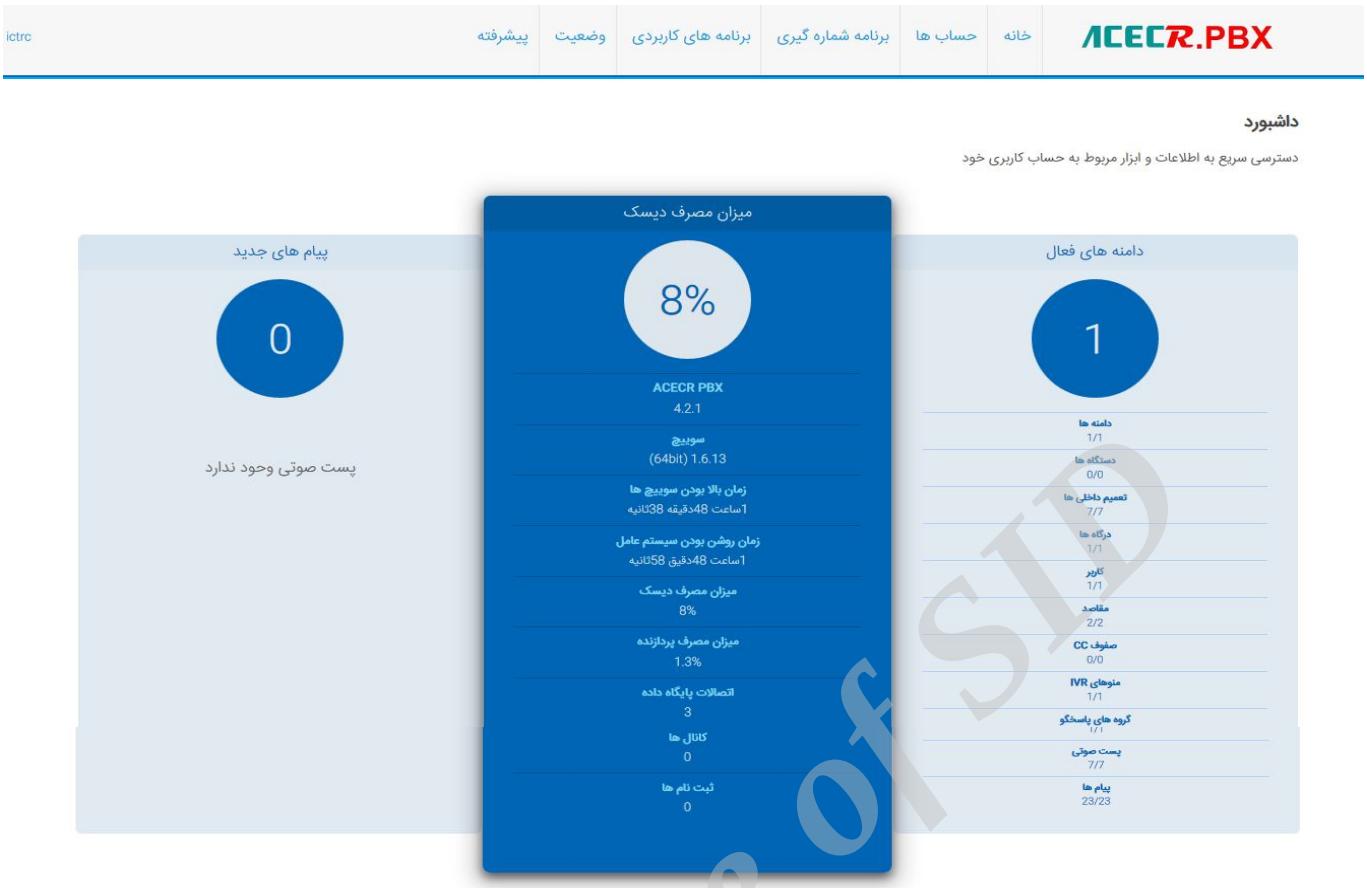
6 . ساختار سیستم

1,6 ساختار محصول بومی سازی شده

نرم‌افزار ارائه شده دارای امکانات و قابلیت‌های مختلفی است. در این بخش تلاش می‌شود تا به بررسی امکانات محصول که در قالب صفحات و منوهای مختلف نرم‌افزار ارائه گردیده است، پرداخته می‌شود.

1,1,6صفحه داشبورد

شکل 5-1 نشان دهنده صفحه داشبورد سامانه است. این صفحه، به صورت اجمالی گزارش کاملی از وضعیت سامانه را به مدیر نرم‌افزار ارائه می‌دهد. این اطلاعات شامل وضعیت سیستم، شمارش سیستم و پیامگیر صوتی است و همانطور که در شکل مشخص است در هر گروه اطلاعات جامعی فهرست شده است. برای مثال در بخش وضعیت سیستم، فهرستی از میزان منابع مصرفی سامانه در اختیار مدیر سامانه قرار می‌دهد. علاوه بر این، طول مدت اجرای سامانه را مشخص می‌نماید. به عنوان مثال دیگر در بخش شمارش سیستم، تعداد دامنه‌ها، درگاه‌ها، داخلی‌ها، کاربران و غیره به مدیر سامانه نمایش داده شده است. این گزارش‌ها، مدیر سامانه را در مورد وضعیت کلی سامانه از ابعاد مختلف مطلع می‌سازد. لازم به ذکر است که مدیر سامانه با کلیک بر روی هر یک از گزینه‌های موجود در بخش «شمارش سیستم» به بخش مربوطه هدایت می شود و قادر خواهد بود تا اطلاعات کامل‌تری را کسب نماید.



شکل 6-1: صفحه ی داشبورد سامانه

2,1,6 صفحه فهرست داخلی‌ها

در این صفحه، فهرستی از داخلی‌های تعریف‌شده در سامانه قابل مشاهده است. در این صفحه امکاناتی مانند جستجوی داخلی، انتخاب داخلی جهت ویرایش یا حذف وجود دارد.

شکل 6-2 : نمای منوی داخلی ها

3,1,6 صفحه ایجاد/ویرایش داخلی

با کلیک روی یکی از داخلی‌های فهرست شده در صفحه‌ی «فهرست داخلی‌ها»، امکان مشاهده و ویرایش داخلی مورد نظر وجود دارد. در این صفحه ویژگی‌های مختلف یک داخلی قابل دسترس است و امکان ویرایش هر کدام از آنها وجود دارد. برای مثال با مراجعه به این صفحه، می‌توان گذرواژه‌ی داخلی را تغییر داد.

شکل 6-3 : ایجاد و ویرایش داخلی ها

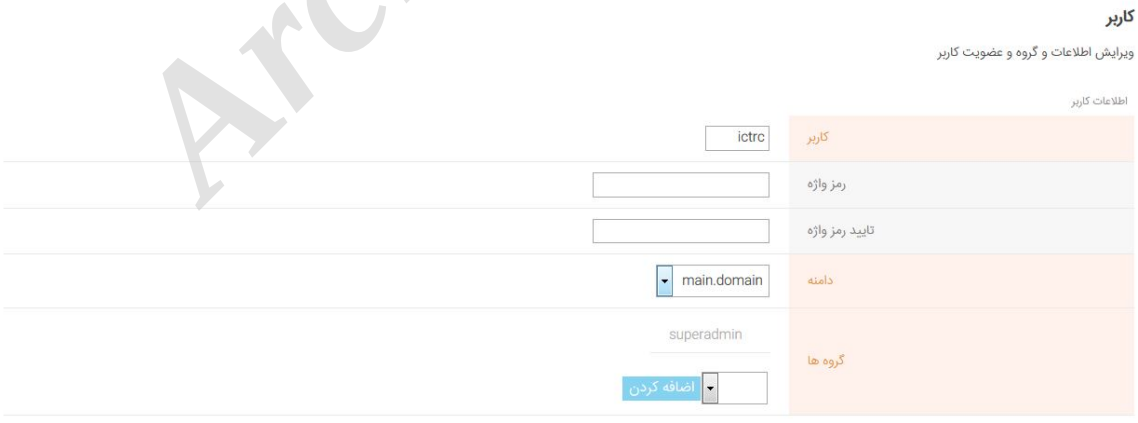
4,1,6 صفحه فهرست کاربران

در این صفحه، فهرستی از کاربران تعریف شده در سامانه قابل مشاهده است. عملیات مختلفی در این صفحه قابل اجرا است. برای مثال، امکان جستجوی یک کاربر، ویرایش اطلاعات کاربر یا حذف کلی آن وجود دارد.

شکل 6-4: فهرست کاربران

5,1,6 صفحه ایجاد/ویرایش کاربر

با کلیک روی یکی از موارد موجود در فهرست کاربران، امکان مشاهده و ویرایش هر کدام از آنها وجود دارد. در این صفحه خصوصیات متنوعی در مورد کاربرد قابل دسترس است و امکان ویرایش هر کدام از آنها وجود دارد. برای مثال امکان تغییر نام کاربری، گذرواژه و دامنه کاربر از طریق این صفحه وجود دارد.



شکل 6-5 : ایجاد و ویرایش کاربر

6,1,6 صفحه فهرست درگاه

در صفحه‌ی فهرست درگاه، امکان مشاهده‌ی تمامی درگاه‌های تعریف‌شده در سامانه وجود دارد. مدیر سامانه با یک نگاه گذرا به این صفحه می‌تواند اطلاعاتی را در مورد فعال بودن درگاه و موارد مشابه دیگر کسب نماید. علاوه بر این، مدیر سامانه امکان اضافه کردن یک درگاه جدید، حذف آن یا ویرایش اطلاعات یک درگاه موجود را دارد.

شکل 6-6: فهرست درگاه

7,1,6 صفحه مدیر برنامه شماره گیری

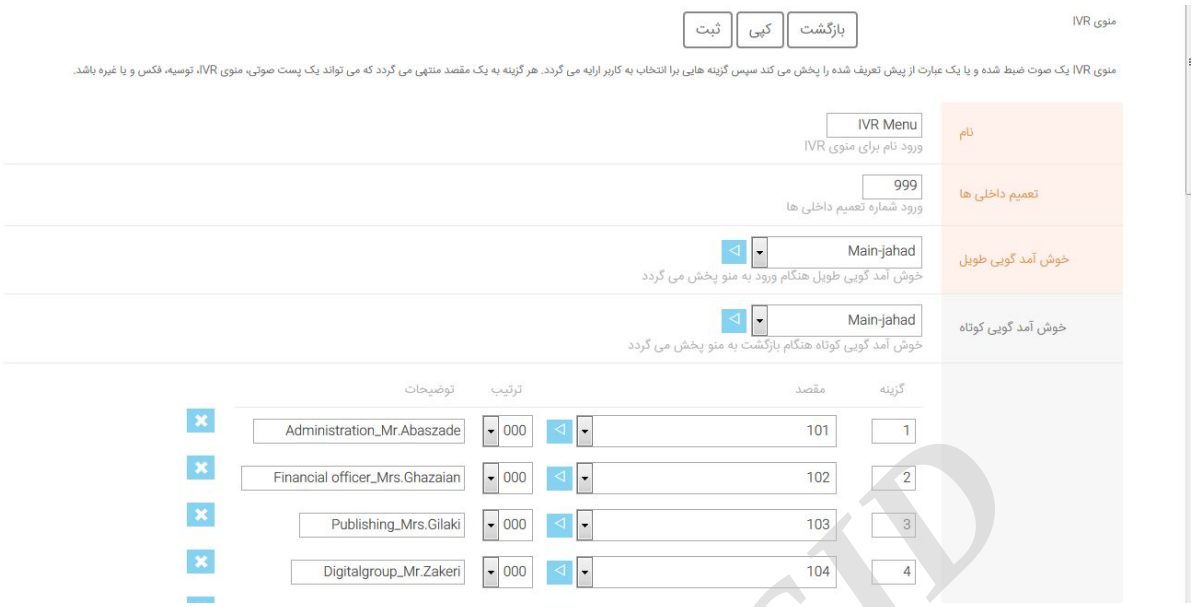
در این صفحه، امکان تعریف گسترش‌های[83] مختلف برای نقشه‌ی تماس[84] وجود دارد. هر گسترش می‌تواند مشتمل بر یک سری شرط[85] و اقدام[86] باشد. با استفاده از امکانات موجود در این صفحه، امکان هدایت یک تماس از لحظه‌ی ایجاد تا لحظه‌ی خاتمه وجود خواهد داشت. برای مثال با امکانات ارائه شده در این صفحه، امکان هدایت یک تماس ورودی به یک داخلی خاص و یا یک سامانه IVR وجود دارد. در این صفحه، امکانات دیگری علاوه بر تعریف یک گسترش جدید وجود دارد که عبارت‌اند از: جستجوی یک گسترش، حذف یک گسترش و یا ویرایش اطلاعات آن.

[۸۳] extension
[۸٤] dialplan
[۸۵] condition
[۸٦] action

شکل 6-7 : صفحه ی مدیر برنامه شماره گیری

8,1,6 صفحه طراحی IVR

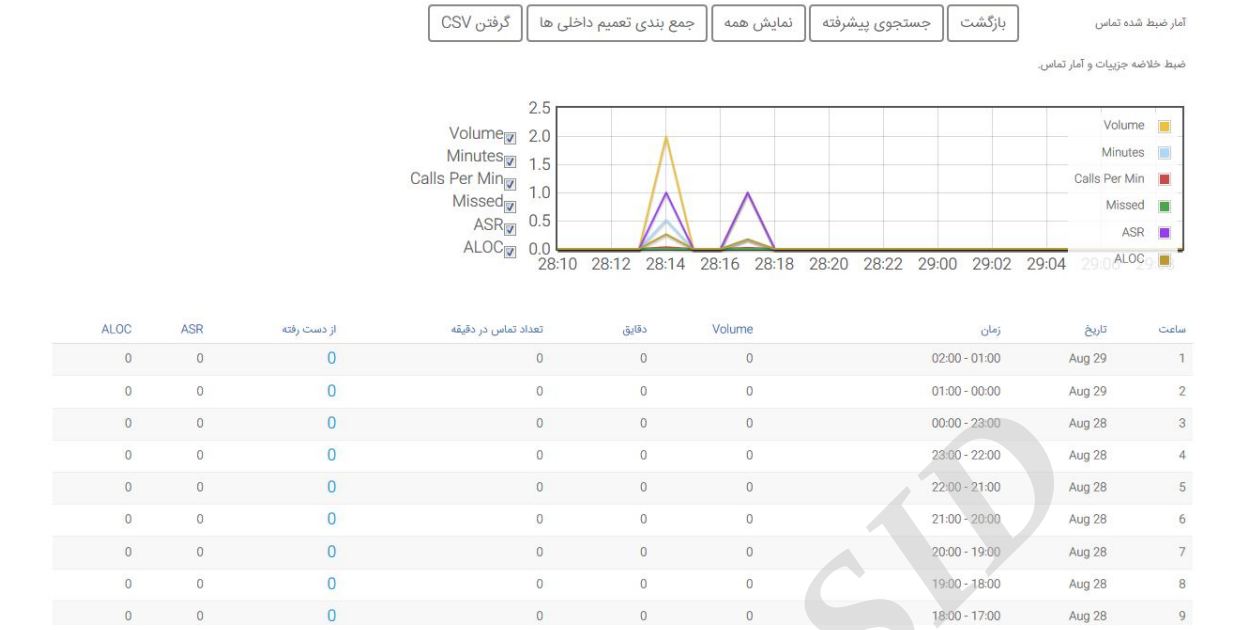
این صفحه یکی از کاربردی‌ترین صفحات نرم‌افزار است که امکان تعریف یک IVR را می‌دهد. با استفاده از این صفحه، کاربر می‌تواند یک IVR را به صورت کامل ایجاد نماید. برای تعریف یک IVR، بایستی صوت‌های لازم برای خوشامدگویی و منوها از قبل روی سامانه بارگذاری شود و در این صفحه برای استفاده مشخص گردد. سپس در بخش گزینه‌های این صفحه مشخص گردد که کاربر با وارد کردن هر شماره، به چه مقصدی هدایت می‌شود. لازم به ذکر است که برای سامانه IVR باید یک نام مناسب به همراه داخلی مربوط به آن تعریف شود که در شکل زیر، این موارد مشخص شده است.



شکل 6-8 : منوی طراحی IVR

9,1,6 صفحه جزییات تماس

این صفحه حاوی یک گزارش از تمامی تماس‌هایی است که در سامانه روی داده است. مدیر سامانه با استفاده از این صفحه می‌تواند اطلاعاتی را در مورد تماس‌های مختلف و زمان هر کدام از آنها کسب نماید. علاوه بر این با استفاده از نمودار موجود در این صفحه، اطلاعاتی را در مورد فراوانی تماس‌ها در زمان‌های مختلف بدست آورد. در این صفحه امکانات مختلفی در نظر گرفته شده است. برای مثال، امکان جستجو روی این اطلاعات وجود دارد. علاوه بر این می‌توان رکوردهای آن را در قالب یک فایل CSV، خروجی گرفت.



ساعت	تاریخ	زمان	Volume	دقایق	تعداد تماس در دقیقه	از دست رفته	ASR	ALOC
1	Aug 29	02:00 - 01:00	0	0	0	0	0	0
2	Aug 29	01:00 - 00:00	0	0	0	0	0	0
3	Aug 28	00:00 - 23:00	0	0	0	0	0	0
4	Aug 28	23:00 - 22:00	0	0	0	0	0	0
5	Aug 28	22:00 - 21:00	0	0	0	0	0	0
6	Aug 28	21:00 - 20:00	0	0	0	0	0	0
7	Aug 28	20:00 - 19:00	0	0	0	0	0	0
8	Aug 28	19:00 - 18:00	0	0	0	0	0	0
9	Aug 28	18:00 - 17:00	0	0	0	0	0	0

شکل 6-9 : صفحه ی جزییات تماس

10,1,6 صفحه تماس‌های فعال

این صفحه، تماس‌های فعال موجود در ساماره را نشان می‌دهد. منظور از تماس فعال تماسی است که در حال حاضر، یک نشست برای آن در سامانه وجود دارد. کاربر با استفاده از این صفحه می‌تواند اطلاعاتی را از جمله شماره، نام کالرآیدی، شماره کالرآیدی و غیره کسب نماید.

شکل 6-10: صفحه ی تماس های فعال

11,1,6 منوی حساب‌ها

این منو حاوی چهار زیربخش است: آ. داخلی‌ها، برای ایجاد، حذف و ویرایش داخلی‌ها، ب. دستگاه‌ها، برای تعریف، حذف و ویرایش دستگاه‌ها، پ. کاربران، برای ایجاد، حذف و ویرایش کاربران و، ت. درگاه‌ها، برای ایجاد، حذف و ویرایش درگاه‌ها. لازم به ذکر است که در بخش مربوط به صفحات توضیحات در مورد امکانات هر کدام از این زیربخش‌ها ارائه شده است.

شکل 6-11 : منوی حساب ها

12,1,6 برنامه شماره گیری

این منو حاوی امکاناتی برای ایجاد گسترش‌های مختلف در نقشه‌ی تماس است. این منو حاوی مواردی از جمله برنامه شماره گیری (مدیریت Dialplan)، جهت تعریف، حذف و ویرایش گسترش‌ها در نقشه‌ی تماس، مسیر تماس‌های ورودی و خروجی، برای تعریف مسیر تماس‌هایی است که به سامانه وارد می‌شوند یا از آن خارج می‌گردند.

شکل 6-12: **برنامه شماره گیری**

13,1,6 منوی برنامه‌ها

این منو، کاربردی‌ترین منوی نرم‌افزار است و تمامی برنامه‌ها و کاربردهایی که نیاز به راه‌اندازی آن وجود داشته باشد، از طریق این منو قابل دسترسی است. برای مثال با استفاده از این منو و انتخاب گزینه‌ی «منوی منشی دیجیتال»، امکان ایجاد یک سامانه IVR وجود دارد. به عنوان مثال دیگر، با انتخاب گزینه‌ی «مکالمات ضبط‌شده»، امکان مشاهده و بررسی تمامی مکالماتی است که در سامانه ضبط شده است.

شکل 6-13: منوی برنامه ها

14,1,6 منوی وضعیت

این منو امکان دسترسی به انواع گزارشات از سامانه را فراهم می‌آورد. برای مثال با استفاده از مورد «تماس‌های فعال»، امکان دسترسی و مشاهده‌ی تماس‌های فعال در سامانه وجود دارد. به عنوان مثالی دیگر، با استفاده از مورد «مشاهده‌کننده لاگ»، امکان بررسی رویدادنگاشت‌های مختلف سامانه برای اهداف مختلفی از جمله عیب‌یابی وجود دارد. علاوه بر این با استفاده از مورد «آمار جزییات تماس»، می‌توان اطلاعات مشروحی را در زمینه‌ی تماس‌ها بدست آورد.

شکل 6-14: منوی وضعیت

15,1,6 منوی پیشرفته

این منو حاوی امکانات و اطلاعاتی است که باید توسط مسئول فنی سامانه مورد استفاده قرار بگیرد. برای مثال، در این منو امکان دسترسی به پروفایل‌های SIP و پیکربندی آنها وجود دارد. علاوه بر این در این بخش، امکان پیکربندی تنظیمات مربوط به پایگاه‌داده وجود دارد. همچنین با استفاده از این منو، امکان مشاهده‌ی ماژول‌هایی که در سامانه فعال شده است، وجود دارد.

شکل 6-15: منوی پیشرفته

7. ویژگیهای سیستم

در این بخش به بیان ویژگیهای سامانه پرداخته می‌شود.

- برقراری امنیت بر روی سیستم تلفنی با راه اندازی فایروال های لینوکسی و بستن پورت های سیستم برای IP هایی که نباید به سیستم تلفنی دسترسی داشته باشند.
- امنیت بیشتر تماس نسبت به سیستم های تلفنی سنتی به دلیل پیاده سازی بر روی بستر شبکه
- پشتیبانی از تماس‌های همزمان با نرخ بالا
- امکان تعریف دامنه‌های کاملاً مجزا با قابلیت‌های مختلف

- پشتیبانی از کدکهای HD
- کاربرپسندی واسط گرافیکی کاربر
- ثبت تماس ها ورخدادهای انجام گرفته
- تعریف دامنه به تعداد نامحدود به منظور جداسازی سرویس‌ها
- تعریف داخلی ها بر روی بستر شبکه به تعداد نامحدود
- تعریف چندین منوی منشی دیجیتال بر روی سیستم تلفنی که قابلیت درختواره بودن منوی ورودی را در اختیار کاربر قرار می دهند
- هویت سنجی
- ایجاد گروه های زمانی مختلف برای بخش مختلف که زمان های کاری متفاوت دارند
- امکان گزارش گیری بسیار دقیق با تقویم شمسی از تماس های سیستم
- امکان ضبط مکالمات برای هر داخلی
- قابلیت پایش برخط از تماس های سیستم و وضعیت داخلی ها
- امکان محدود کردن تماس داخلی های مختلف هم از لحاظ شماره ای و هم از لحاظ زمانی
- مدیریت تماس های تلفنی : نگهداشتن تماس (Hold) ،انتقال تماس (Transfer) ، مسدودکردن تماس های ورودی ((Do Not Disturb، Directe Pickup , Call Parking.
- منوی منشی دیجیتال (IVR) : این بخش از سیستم این امکان را به ما می دهد که با پخش یک متن صوتی فرد تماس گیرنده قادر به وارد نمودن یک عدد جهت اتصال مکان یا برنامه تعیین شده باشد و یا به صورت مستقیم داخلی مورد نظر خود را شماره گیری نماید. در اکثر سیستم های تلفنی از منوی منشی دیجیتال جهت مدیریت

ورودی سیستم و راهنمایی مشتریان جهت اتصال هر چه سریعتر و آسانتر به بخش مورد نظرشان استفاده می گردد.

- صندوق صوتی : هر کاربر در سیستم می تواند با داشتن صندوق صوتی مخصوص خود پیام های صوتی تماس گیرندگان را ذخیره نموده و یا می تواند اصل پیام ها و یا هشدار دریافت پیام ها را در ایمیل خود دریافت نماید.
- گروه های زمانی و شرایط زمانی : می توان برای هر قسمت از سازمان یک زمان کاری مشخص گردد که در ساعات کاری تماس گیرنده به یک مسیر خاص هدایت گردد و در خارج از زمان کار به مسیرهای تعیین شده دیگر فرستاده شود.
- امکان تعریف سفارشی نقشه‌ی تماس[87] مشتمل بر شرط‌ها و اقدام‌های مختلف
- گزارش گیری از سامانه شامل گزارش جزییات تماس، تماس‌های فعال، میزان مصرف منابع و غیره.

8 . ویژگی های محیط تست

1,8 مودم

برای انجام و پیاده سازی محیط تست، از یک خط SIP Trunk استفاده نموده ایم. که در اصل جایگزینی برای ارتباطات PRA و E1 در شبکه های TDM است. قابلیت ارائه سرویس های متنوع VOIP دارد. با پیگیری های انجام شده، خط SIP Trunk با مالکیت پژوهشکده فناوری اطلاعات و ارتباطات (ICT) به سر شماره" 43416" تهیه گردید. این خط دارای ویژگی های از جمله

- امکان ارتقاء در گستره متنوعی از کانال های همزمان و نامبرینگ به طور مثال: تعداد 10 ، 20 ، 150 و یا 1000 کانال

[87] dialplan

- قابل استفاده بر روی کابل مسی و فیبر نوری
- عدم نیاز به افزایش تعداد تجهیزات سمت متقاضی با افزایش تعدادشماره (مثلا 120 شماره تلفن با فقط یک مودم قابل سرویس دهی است)
- عدم وجود محدودیت جغرافیایی برای ارائه سرویس
- امکان مدیریت ترافیک صوتی ارسالی بر روی لینک به دلیل استفاده از بسته های IP

بدنبال بهره برداری از این خط یک مودم G.SHDSL مبتنی برنیاز های پروژه و سازگار با پروتکل های مدنظر مخابرات منطقه تهیه گردید. مودم تهیه شده با مشخصات زیر می باشد.

مشخصات فنی مودم GNTU764 TAINET ، انتقال پرسرعت اترنت روی یک زوج – دو زوج یا چهار زوج سیم مسی با تکنولوژی EFM G.Shdsl.bis با سرعت:

- 5,7 (GNTU764/102)مگابیت بر ثانیه در Normal mode و 51 مگابیت بر ثانیه در Extended mode
- پشتیبانی از کدینگ های TC-PAM 16/32/64/128 bits بر اساس استاندارد ITU-T G.991,2
- قابلیت انتخاب وضعیتهای CO و CPE و امکان مدیریت دستگاه Remote توسط دستگاه -Local
- برقراری اتوماتیک ارتباط با حداکثر سرعت ممکن در صورت فعال بودن بررسی مسیر مسی توسط دستگاه
- دارای LED های لازم به منظور مشاهده سریع وضعیت

-مدیریت توسط CLI ، Web و -TAINET UNMS

- پشتیبانی از TR069
- دارای دکمه TST به منظور بررسی سریع مسیر مسی با BERT
- امکان Loopback و مشاهده پارامترهای کارآیی G.Shdsl.bis
- قابلیت افزونگی مسیر به منظور افزایش سطح اطمینان انتقال دیتا
- دارای یک پورت اترنت VLAN وQoS

- امکان کنترل سرعت پورت اترنت به صورت Nx64 Kbps (N=1~1600)
- حافظه لازم به منظور یادگیری 2000 آدرس MAC
- امکان انتقال فریمهای اترنت با حداکثر سایز 1664 بایت
- دو ورودی پاور مستقل با امکان AC+AC ، AC+DC و DC+DC
- قابلیت آپگرید دستگاه توسط File Upload یا TFTP
- امکان استفاده به عنوان دستگاه مستقل دسکتاپ یا لاین کارت در شاسی iEAC-16-
- قابلیت اتصال به دستگاههای Comet ، دستگاهها و لاین کارتهای SNTU ، GNTU روی شاسی iEAC-16و پورتهای EFM G.Shdsl.bis روی تمامی DSLAM ها

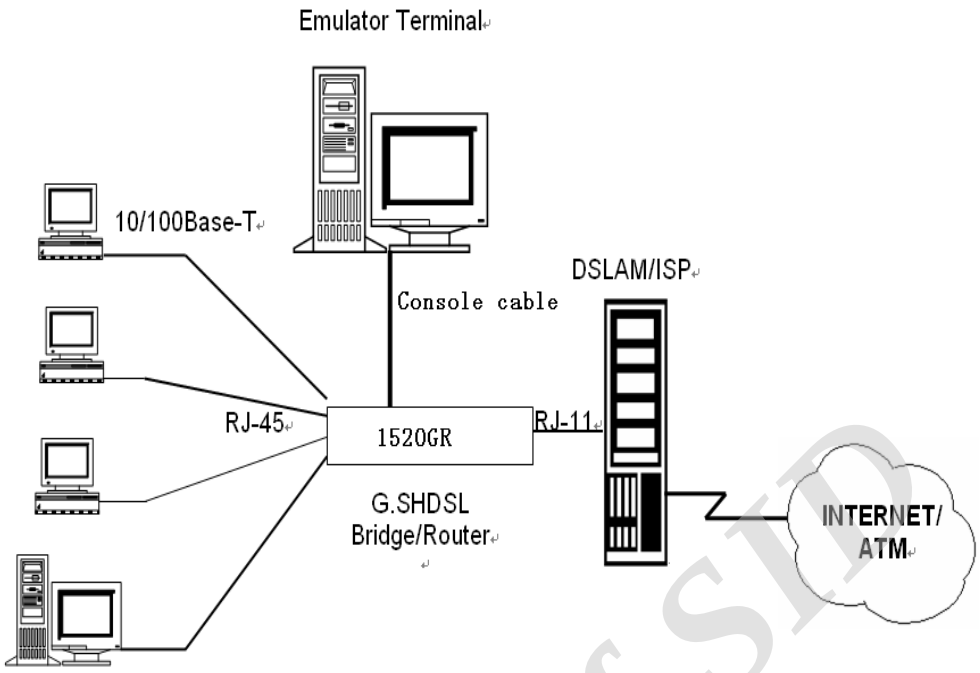
شکل 8-1: مودم مورد استفاده در پروژه

خط SIP Trunk در حقیقت، ارائه دهنده سرویس های آنی مخابراتی توسط سرویس اینترنت تلفنی می باشد که تماس های همزمان شرکت های بزرگ، توسط ساختار مبتنی بر IP یک ارائه دهنده سرویس اینترنت (ISP[88]) ، ایجاد می شود[22]. مزایای به کارگیری این سرویس را می توان به سه دسته تقسیم نمود:

- حذف سیم کشی های متعدد برای خط تلفنی معمولی
- امکان برقرای تماس های مقیاس پذیر در شبکه ها و پروژهای ارتباطی بزرگ
- صرفه جویی اقتصادی قابل حصول در شرکت ها و پروژه های بزرگ
- بازگشت پذیری سریع سرمایه در گذار به سیستم های مبتنی برIP
- کاهش هزینه های بکارگیری PRI[89] و BRI[90]
- بهینه سازی مصرف پهنای باند جهت بکارگیری در انتقال صوت و داده
- قابلیت انعطاف پذیری در تعداد کاربران (برخلاف خطوط E1 و T1 که ظرفیت بسیار محدودتری داشتند)

به طور کلی اتصال این مودم به تجهیزات و سیستم های جانبی به صورت ساختار پیشنهادی (توسط کارخانه سازنده) می باشد (شکل 6-2).

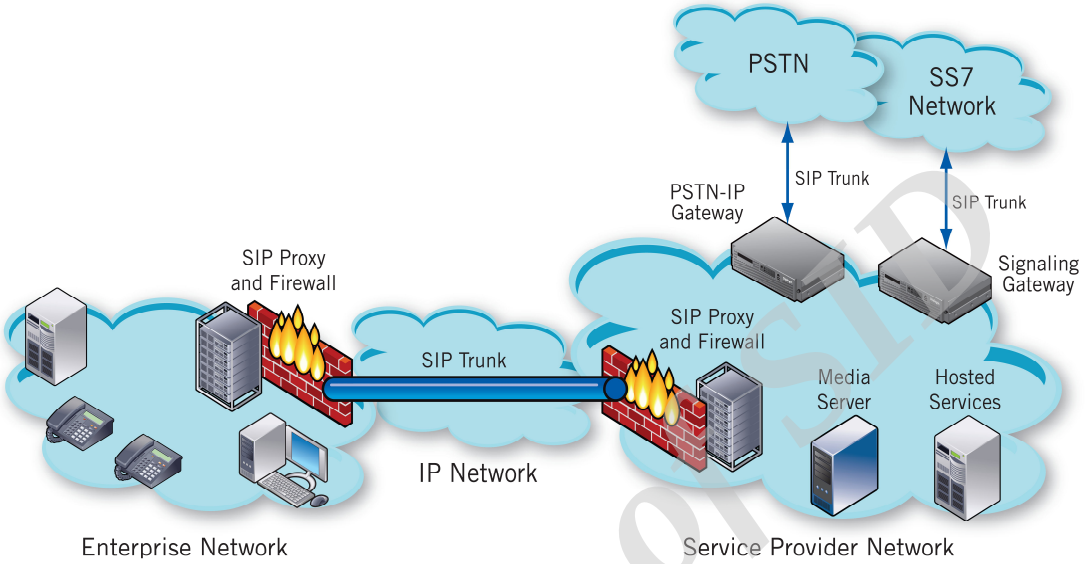
[88] Internet Service Provider
[89] Primary Rate Interfaces
[90] Basic Rate Interfaces



شکل 8-2: نحوه اتصال کلی مودم

9. معماری سیستم SIP Trunking

شکل زیر(8-1) معماری سیستم مبتنی بر خط SIP Trunking در یک محیط VOIP را نشان می دهد. در این معماری، بهره برداری از سیستم مبتنی بر IP به شبکه تلفنی PSTN و شبکه SS7 مهیا شده است[23].



شکل 9-1: نحوه اتصال کلی مودم

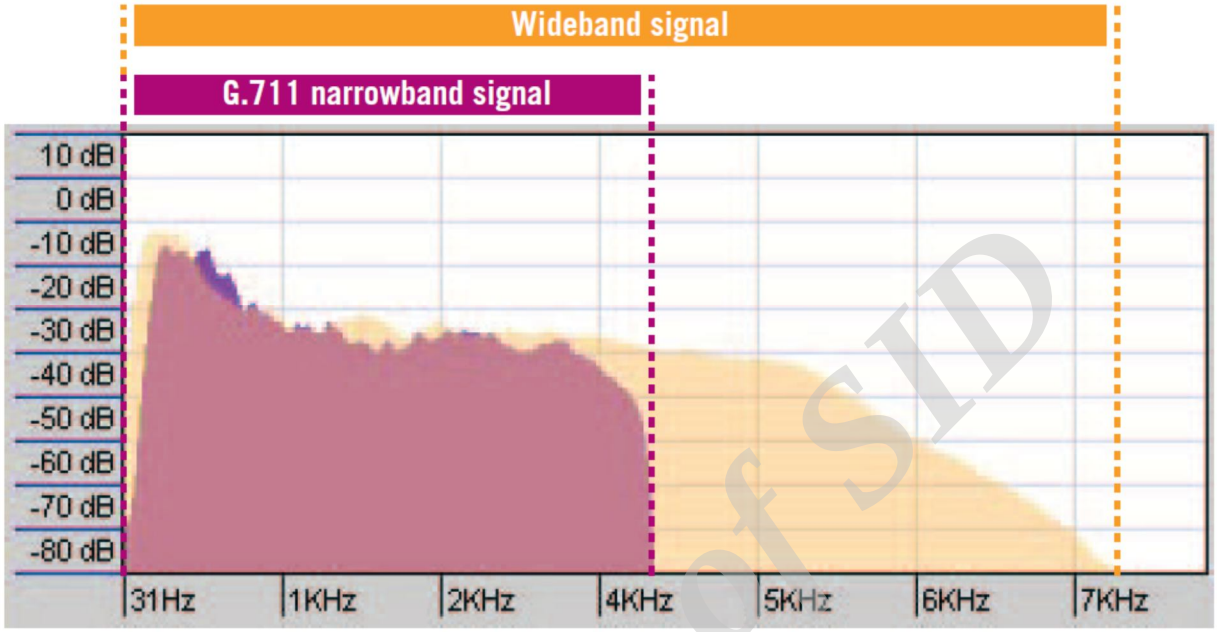
صوت پهن باند[91]

صوت پهن باند در حقیقت به سیگنال صوتی گفته می شود که دارای رنج گسترده فرکانسی بین 50 تا 7000 هرتز می باشد. این نوع سیگنال صوتی جهت انتقال صوت با کیفتی بالاتر از حد معمول (300 تا 3400 هرتز) مورد استفاده قرار می گیرد. این رنج گسترده قابلیت های موثری به کاربران در شبکه تلفنی می دهد که از آن جمله می توان به

- تسهیل در شناسایی صوت
- تسهیل در تشخیص اصوات حروف مشابه در تشخیص گفتار به متن
- حذف و یا کاهش نویز و صداهای اضافی محیط
- ارائه صدای مکالمه طبیعی تر

[91] wideband

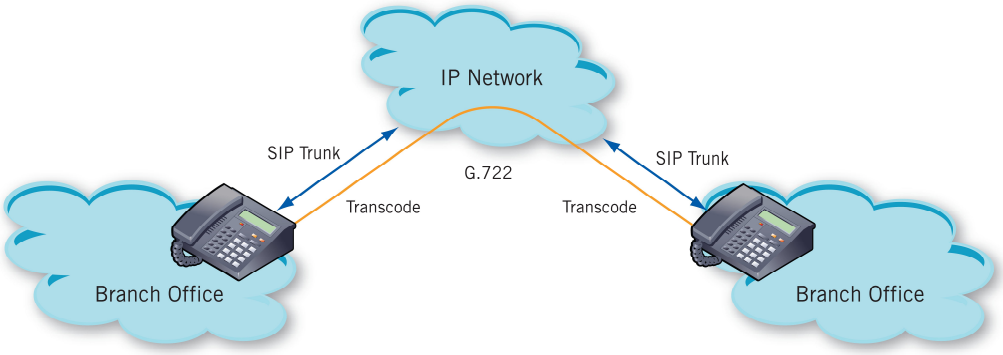
اشاره نمود. در شکل زیر (8-2) دامنه سیگنال صوتی در نمونه زمانی 30 ثانیه نشان داده شده است. به طور محسوسی گستردگی بین دو سیگنال معمولی (باند باریک[92]) و پهن باند نشان داده شده است [24].



شکل 9-2: بررسی دامنه سیگنال نمونه

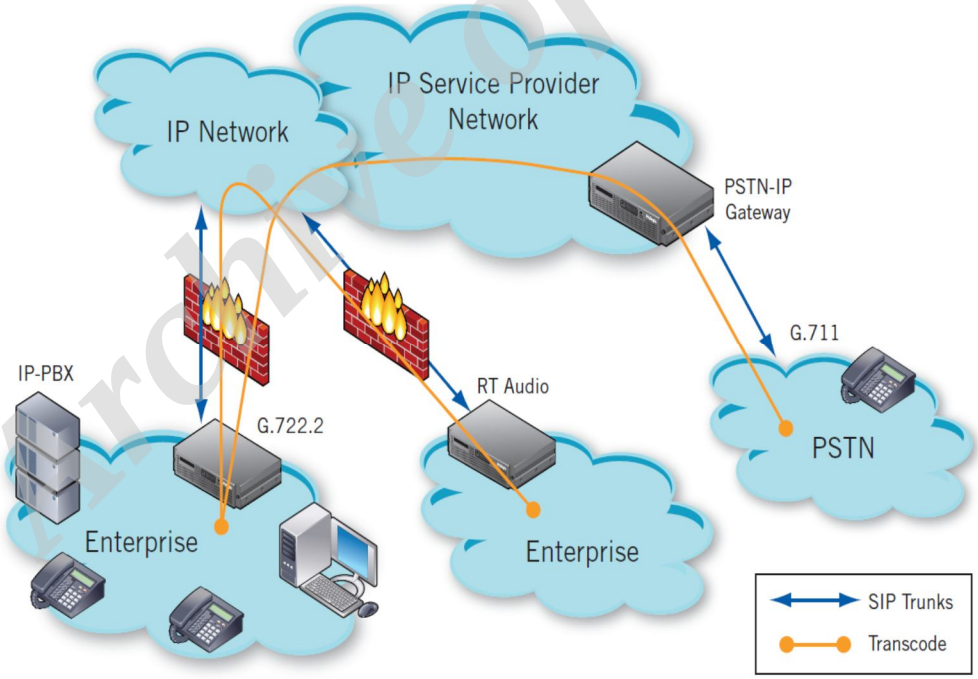
از طرفی سیستم مبتنی بر SIP Trunk قابلیت اتصال ارتباطات داخلی به شبکه ارتباطی بسیار بزرگ را دارد. این نوع ارتباط داخلی می‌تواند داخل یک شعبه یا بین شعبه های اداره از طریق شبکه بزرگ ارتباطی با استفاده از سرویس هایی مانند Skype مهیا می شود. این ساختار شبکه با اتصالات مختلف، از کدگذاری مشترک جهت ارتباط بین مشترکین استفاده می نماید. شکل زیر (شکل 8-3) نمونه ای از این شبکه را نشان می‌دهد.

[92] Narrow band



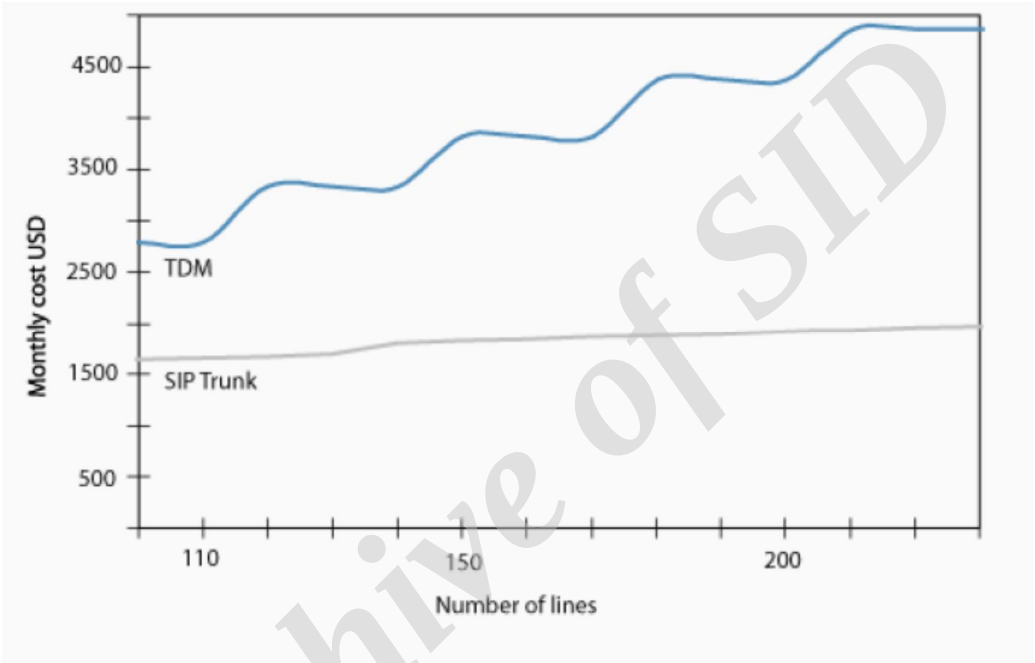
شکل 9-3: شبکه بین شعبه های اداره

حال در مقیاس جامع تر می توان این معماری را بصورت شکل (8-4) در نظر گرفت. همانطور که مشخص است اگر ارتباط بین شبکه های بزرگ از طریق یک سرویس بین شبکه ای IP ایجاد شود. در نتیجه شبکه از سیگنال پهن باند (صوت HD) یکپارچه انتها - انتها شبکه پشتیبانی می نماید. در این شکل سیستم های شبکه صوتی پهن باند با کدهای مختلف با هم مرتبط شده اند. [۲۵]



شکل9-4: شبکه جامع

در حقیقت هزینه اضافه نمودن تعداد کاربران و خطوط در سیستم ارتباطی میتنی بر SIP Trunk بصورت نسبتا خطی می باشد. در شکل زیر نمودار مقایسه هزینه نسبت به خطوط بر حسب تخصیص زمانی TDM ترسیم شده است (شکل 8-5).



شکل 9-5: مقایسه هزینه ها

10. تست ، ارزیابی و تحلیل سیستم

1,10 مقدمه

در این بخش به تست و ارزیابی محصول منتخب خود ACECR PBX و رقیب نزدیک به آن (از لحاظ عملکرد) Elastix می پردازیم. همانطور در قبل اشاره شد Elastix، یک نرم‌افزار متن‌باز برای راه‌اندازی یک سامانه ارتباطی یکپارچه است. تلاش این پروژه روی تجمیع تمامی گزینه‌های ارتباطاتی در قالب یک راهکار واحد بوده است. عملکردهای ارائه شده در این پروژه مبتنی بر پروژه‌های متن‌باز دیگر است. لازم به ذکر است که سیستم‌عامل‌های قابل استفاده برای این نرم‌افزار، linux centos می‌باشد. زبان توسعه‌ی این نرم‌افزار زبان برنامه‌نویسی C می‌باشد. زمان آخرین ورژن ارائه شده برای این نرم‌افزار فوریه 2016 میلادی می‌باشد. برای برنامه‌نویسی و گسترش عملکرد این نرم‌افزار می‌توان از زبان C و یا واسط دروازه Asterix استفاده نمود. طراحی این نرم‌افراز از Asterisk الهام گرفته است و مبتنی بر مجموعه‌ای از ماژول‌ها است که در کنار هم، نیازمندی‌های کاربر را برآورده می‌نمایند. به همین خاطر، نرم‌افزار متشکل از یک هسته‌ی اصلی و مجموعه‌ی متنوعی از ماژول‌ها است که بر حسب نیاز ممکن است بارگذاری شوند یا نشوند. کنترل ماژول‌های بارگذاری شده از طریق یک فایل پیکربندی مرکزی صورت می‌پذیرد.
این نرم‌افزار از کدکهای مختلفی پشتیبانی می‌نماید که مهترین آنها عبارتند از:

- ADPCM
- G.711 (A-Law & μ-Law)
- G.722
- G.723,1
- G.726
- G.728
- G.729
- GSM
- iLBC

از آنجایی که این پروژه از Asterisk منشعب شده است، ماژول‌های آن بسیار شبیه به ماژول‌های Asterisk است. این نرم‌افزار برای پشتیبانی از رمزنگاری، از پروتکل‌های امنیتی TLS و SRTP پشتیبانی می‌نماید.

تماس در هر ثانیه (CPS[۹۳])

[۹۳] Calls per Second

تماس در هر ثانیه نماینگر قابلیت سیستم در ایجاد و قطع تعداد تماس در هر ثانیه می باشد. که در حقیقت پارامتر محدود کننده در فرآیند پیام SIP می باشد. همچنین بسته به نوع ترافیک تماس که سیستم دارد این پارامتر می تواند تاثیرگذار باشد و خود نشئت گرفته از پارامترهای دیگری است. در کتابخانه freeswitch برخی از آنها آورده شده است.

تماس های همزمان

با بکارگیری تجهیزات سخت افزاری جدید، دیگر محدویت محسوسی در رابطه با تماس های همزمان SIP (صرفنظر از RTP) وجود ندارد. از منظر مباحث تئوری، با برقراری تماس از طریق پورت اترنت گیگا بیت ما قادر خواهیم بود، که تماس های همزمانی در حدود ۱۰،۵۰۰ را بدون RTCP ایجاد نماییم (با فرض G.711 codec) . اما در واقعیت محدودیت های دیگری نیز وجود دارد از جمله آن، پارامترهای محدودکننده لایه های شبکه که ناشی از بسته های هر ثانیه جریان مدیای RTP است را می توان نام برد.

شرح سناریوی تست

در این تست با استفاده از ابزار SIPp، تعدادی تماس شبیه‌سازی گردید و یک تماس دستی برای ارزیابی کیفیت صوتی برقرار گردید.

برای تست عملکرد این دو برنامه، دو سناریو تعریف شده است.پارامترهای دستورات مورد استفاده در SIPp به صورت زیر می باشد:

- d- : برای نمایش تاخیر توقف بر حسب میلی ثانیه
- s-: برای نمایش نام سرویس(داخلی مورد نظر)
- r- : برای نمایش نرخ تماس به صورت تعداد تماس در ثانیه
- l-: برای نمایش ماکزیمم تعداد تماس همزمان.وقتی تعداد تماس ها از این مرز بگذرد ،ترافیک تا زمانی که تعداد تماس های فعال کم شود کاهش می یابد.

2,10 تست پلتفرم ACECR-PBX

پس از تنظیمات در ACECR-PBX , Elastix به صورتی که دارای شرایط یکسان از لحاظ منابع باشند با دستور زیر در محیط SIPp به تست آنها می پردازیم. در ابتدا برای حالت بدون تماس فعال ارزیابی را انجام می دهیم. این تست اولیه بسیار حائز اهمیت خواهد بود از آنجایی که مشخص کننده شرایط اولیه و میزان مصرف هر یک از منابع در حالت اولیه می باشد. به عبارت دیگر پلتفرم مربوطه به خودی خود چه میزان منابع مصرف می نماید.

```
>> Command:   sipp -snuac -d ١٠٠٠٠٠٠٠٠ -s ٩٨٧٦٥ ١٩٢,١٦٨,١,١٠١:٥٠٦٠ -l
١٠٠٠ -r ٤
```

TEST ١: ٠ concurrent call

```
----------------------Memory RAM -------------------------
   totalused   free    shared   buffers   cached
Mem:          ٢٠١٠        ٢٦١       ١٧٤٨    ٢٣          ٩        ١٤٧
+/-buffers/cache:        ١٠٤       ١٩٠٦
Swap:            ٠          ٠
           -------------------------Processor Parameters-----------------
%Cpu(s):  ٠,٣ us,  ٠,٣sy,  ٠,٠ ni, ٩٩,٣ id,  ٠,٠ wa,  ٠,٠ hi,  ٠,٠ si,  ٠,٠ st
KiBMem:   ٢٠٥٨٦٢٠ total,     ٢٧٣٦٠٠ used,  ١٧٨٥٠٢٠ free,        ٩٩٣٦ buffers
KiB Swap: ٠ total,        ٠ used,        ٠ free.   ١٥٦٧٦٨ cached Mem

PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+COMMAND
  ٥٧٤ www-data  -٢ -١٠  ٨٨١٤٩٦  ٥٣٧٧٢  ٢٢٣٨٨ S  ١,٠  ٢,٦   ٠:٠١,٩٣ freeswitch
  ٧ root      ٢٠   ٠       ٠      ٠      ٠ S  ٠,٣  ٠,٠   ٠:٠٠,٠٩ rcu_sched
  ٨٤ root       ٠ -٢٠       ٠      ٠      ٠ S  ٠,٣  ٠,٠   ٠:٠٠,٠٤ kworker/٠:
```

TEST ٢: ١٠٠ concurrent call

```
----------------------Memory RAM-------------------------
```

```
total       used       free     shared    buffers     cached
Mem:          ٢٠١٠        ٣٧٠       ١٦٣٩         ٢٤          ٩        ١٨٠
 +/-buffers/cache:        ١٨٠       ١٨٣٠
Swap:           ٠          ٠          ٠
          ------------------------Processor Parameters-----------------
top - ٠٧:٥٣:١٣ up ٤ min,  ٢ users,  load average: ١,٨٦, ٠,٦٥, ٠,٢٧
Tasks:  ٨٦ total,   ١ running,  ٨٥ sleeping,   ٠ stopped,   ٠ zombie
%Cpu(s): ٦٥,٨ us, ٣٣,٢ sy,  ٠,٠ ni,  ٠,٠ id,  ٠,٠ wa,  ٠,٠ hi,  ١,٠ si,  ٠,٠ st
KiBMem:   ٢٠٥٨٦٢٠ total,   ٣٥٧٨٣٢ used,  ١٧٠٠٧٨٨ free,    ١٠٠٥٦ buffers
KiB Swap:        ٠ total,        ٠ used,        ٠ free.   ١٨٢٢٥٦ cached Mem

PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 ٤٦١ root      ٢٠   ٠  ٧٢٤٧٨٤  ١٤٠٤٠   ٥٩٣٢ S ٥١,٥  ٠,٧   ٠:٣٠,٥٣ fail٢ban-se+
 ٥٧٣ www-data  -٢ -١٠  ٩٠٧١٦٠  ٩٥٨٩٦  ٢٢٧٥٦ S ٤٧,٢  ٤,٧   ٠:١٠,١٧ freeswitch
 ٩٢٨ postgres  ٢٠   ٠  ٢٢٧٨٠٤  ١٣٢٧٢  ١٠٩٦٤ S  ٠,٧  ٠,٦   ٠:٠٠,١٥ postgres
 ٣٩٥ memcache  ٢٠   ٠  ٣٣١٥١٦   ٦٨٤٤   ٢٢١٢ S  ٠,٣  ٠,٣   ٠:٠٠,٠٨ memcached
   ١ root      ٢٠   ٠   ٢٨٧١٦   ٤٨٠٨   ٣٠٨٨ S  ٠,٠  ٠,٢   ٠:٠٠,٥٧ systemd
```

TEST ٣: ٢٠٠ concurrent call

```
          ----------------------Memory RAM-------------------------
total       used       free     shared    buffers     cached
Mem:          ٢٠١٠        ٤٣٦       ١٥٧٤         ٢٤          ٩        ١٨٨
 +/-buffers/cache:        ٢٣٧       ١٧٧٢
Swap:           ٠          ٠          ٠
          ------------------------Processor Parameters-----------------
top - ٠٧:٥٣:٣٧ up ٥ min,  ٢ users,  load average: ١١,٨٧, ٣,٠٠, ١,٠٥
Tasks:  ٨٥ total,   ٤ running,  ٨١ sleeping,   ٠ stopped,   ٠ zombie
%Cpu(s): ١٩,٩ us, ٨٠,١ sy,  ٠,٠ ni,  ٠,٠ id,  ٠,٠ wa,  ٠,٠ hi,  ٠,٠ si,  ٠,٠ st
KiBMem:   ٢٠٥٨٦٢٠ total,   ٤٢١٦٢٠ used,  ١٦٣٧٠٠٠ free,    ١٠٠٩٦ buffers
```

```
KiB Swap:        ۰ total,        ۰ used,        ۰ free.   ۱۹۰۵٤۸ cached Mem

PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 ٥۷۳ www-data  -۲ -۱۰  ۹۳٤۳۹٦ ۱۳۹۱۷۲ ۲۲۷٥٦ S ۸۷,۲  ٦,۸   ۰:۲۷,٦۳ freeswitch
 ٤٦۱ root      ۲۰   ۰  ۷۲٤۷۸٤ ۱٤۰٤۰   ٥۹۳۲ S ۹,۸  ۰,۷   ۰:۳٦,۹۰ fail۲ban-se+
 ۹۲۸ postgres  ۲۰   ۰  ۲۲۷۸۰٤ ۱۳۲۷۲  ۱۰۹٦٤ R ۱,۰  ۰,٦   ۰:۰۰,۳۲ postgres
 ۳۹٥ memcache  ۲۰   ۰  ۳۳۱٥۱٦  ٦۸٤٤  ۲۲۱۲ S ۰,۳  ۰,۳   ۰:۰۰,۱٦ memcached
 ۱   root      ۲۰   ۰   ۲۸۷۱٦  ٤۸۰۸  ۳۰۸۸ S ۰,۰  ۰,۲   ۰:۰۰,٥۷ systemd
```

TEST ٤: ۳۰۰ concurrent call

```
-----------------------Memory RAM-------------------------
total       used       free     shared    buffers     cached
Mem:          ۲۰۱۰        ٥۳۳       ۱٤۷٦         ۲٤          ۹        ۱۹٥
 +/-buffers/cache:        ۳۲۸       ۱٦۸۲
Swap:            ۰          ۰          ۰
-------------------------Processor Parameters-----------------
top - ۰۷:٥٤:۰۳ up ٥ min,  ۲ users,  load average: ۸۲,٤۹, ۱۹,۹۲, ٦,٦۸
Tasks: ۱۰۸ total,   ۱ running, ۱۰۷ sleeping,   ۰ stopped,   ۰ zombie
%Cpu(s): ۱۷,٤ us, ۸۲,٤ sy,  ۰,۰ ni,  ۰,۰ id,  ۰,۰ wa,  ۰,۰ hi,  ۰,۳ si,  ۰,۰ st
KiBMem:   ۲۰٥۸٦۲۰ total,   ٥۱۹٦۷۲ used,  ۱٥۳۸۹٤۸ free,    ۱۰۱٤۰ buffers
KiB Swap:        ۰ total,        ۰ used,        ۰ free.   ۱۹۷٦۹٦ cached Mem

PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 ٥۷۳ www-data  -۲ -۱۰  ۹٦۲۰٦۰ ۱۸٥۷۲۰ ۲۲۷۸۰ S ۹٥,۹  ۹,۰   ۰:٥۱,۷۲ freeswitch
 ٤٦۱ root      ۲۰   ۰  ۷۲٤۷۸٤ ۱٤۰٤۰   ٥۹۳۲ S ۳,۳  ۰,۷   ۰:۳۷,۷۳ fail۲ban-se+
 ۸٦٦ root      ۲۰   ۰   ۸۲۷۲۸  ٦۱۱٦  ٥۲٥۲ S ۰,۳  ۰,۳   ۰:۰۰,۰۷ sshd
 ۱   root      ۲۰   ۰   ۲۸۷۱٦  ٤۸۰۸  ۳۰۸۸ S ۰,۰  ۰,۲   ۰:۰۰,٥۷ systemd
```

TEST ٥: ٤٠٠ concurrent call

```
-----------------------Memory RAM-------------------------

total       used       free     shared    buffers     cached
Mem:          ٢٠١٠        ٦١١       ١٣٩٨         ٢٤         ١٠        ٢٠١
 +/-buffers/cache:        ٣٩٩       ١٦١٠
Swap:            ٠          ٠          ٠

-------------------------Processor Parameters-----------------


top - ٠٣:٢٩:٢٤ up ١٠ min,  ٢ users,  load average: ٣٧٧,٨٩, ١٥٨,٩٥, ٥٩,٨٤
Tasks:  ٧٩ total,   ٩ running,  ٧٠ sleeping,   ٠ stopped,   ٠ zombie
%Cpu(s):  ٦,٣ us, ٩٣,٢ sy,  ٠,٠ni,  ٠,٠ id,  ٠,٠ wa,  ٠,٠ hi,  ٠,٥ si,  ٠,٠ s
KiBMem:   ٢٠٥٨٦٢٠ total,   ٦١٥٢٠٨ used,  ١٤٤٣٤١٢ free,    ١١٨٤٠ buffers
KiB Swap:        ٠ total,        ٠ used,        ٠ free.   ٢٤٨٨٤٠ cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
  ٥٧٤ www-data  -٢ -١٠ ١٠٦٠٠٧٦ ٢٣٩٥٢٤ ٢٢٥٦٠ S ٩٦,١ ١١,٦   ٣:٠٤,٨٧ freeswitch
  ٤٦١ root      ٢٠   ٠  ٧٢٤٧٨٤  ١٤١٦٠   ٦٠١٦ S  ٤,٠  ٠,٧   ٠:٣١,١٤ fail٢ban-s+
  ٨٧٩ root      ٢٠   ٠   ٢٣٥٢٠   ٢٨٤٤   ٢٤٢٤ R  ٠,٣  ٠,١   ٠:٠٠,٤٧ top
```

TEST ٦: ٥٠٠ concurrent call

```
-----------------------Memory RAM----------------------------

Mem:          ٢٠١٠        ٨٤٨       ١١٦١         ٢٨         ١٦        ٣٩٩
-/+ buffers/cache:        ٤٣٢       ١٥٧٧
Swap:            ٠          ٠          ٠


top - ٠٤:٥٨:٢٤ up  ١:٣٩,  ٢ users,  load average: ٥١٠,٨٠, ٣٠٧,٥٢, ١٣١,٢٩
Tasks:  ٨٠ total,   ٢ running,  ٧٨ sleeping,   ٠ stopped,   ٠ zombie
```

```
%Cpu(s):  ٦,١ us, ٩٣,٤ sy,  ٠,٠ni,  ٠,٠ id,  ٠,٠ wa,  ٠,٠ hi,  ٠,٥ si,  ٠,٠ s
KiBMem:   ٢٠٥٨٦٢٠ total,   ٨٧٤٦٢٠ used,   ١١٨٤٠٠٠ free,    ١٦٩٨٨ buffers
KiB Swap:        ٠ total,        ٠ used,        ٠ free.   ٤٠٩٤٩٢ cached Mem
          ------------------------Processor Parameters----------------


  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
  ٥٧٤ www-data  -٢ -١٠ ١٠٩٣١٦٤ ٣٢١٦٣٢  ٢٣٠١٦ S ٩٦,١  ١٥,٦  ١٤:٠٥,٧٠ freeswitch
  ٤٦١ root      ٢٠   ٠  ٧٢٤٧٨٤  ١٤١٨٤   ٦٠١٦ S  ٣,٨  ٠,٧   ١:٤٣,٤١ fail٢ban-s+
```

TEST ٧: ٨٠٠ concurrent call

```
          ------------------------Memory RAM-----------------------------
total       used       free     shared    buffers     cached
Mem:          ٢٠١٠        ٨٣٤       ١١٧٥         ٢٤         ١٠
٢١٣
-/+ buffers/cache:        ٦١٠       ١٣٩٩
Swap:             ٠          ٠          ٠
          ------------------------Processor Parameters----------------
top - ٠٥:٢٩:١٢ up ٧ min,  ٢ users,  load average: ٧٧٨,٣٣, ٣٨٩,١٧, ١٥٥,٣٠
Tasks:  ٧٩ total,  ١٠ running,  ٦٩ sleeping,   ٠ stopped,   ٠ zombie
%Cpu(s):  ٦,٦ us, ٩٣,٤ sy,  ٠,٠ni,  ٠,٠ id,  ٠,٠ wa,  ٠,٠ hi,  ٠,٠ si,  ٠,٠ st
KiBMem:   ٢٠٥٨٦٢٠ total,   ٧٩٣٠٤٨ used,   ١٢٦٥٥٧٢ free,    ١٠٣٨٤ buffers
KiB Swap:        ٠ total,        ٠ used,        ٠ free.   ٢٠٩٩٣٦ cached Mem


  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
  ٥٧٥ www-data  -٢ -١٠ ١٢٣٧٩٦٠ ٤٠٥٠٩٢  ٢٢٨٤٤ S ٩٦,١ ١٩,٧   ٤:٣١,٣٤ freeswitch
  ٤٤٩ root      ٢٠   ٠  ٧٢٤٧٨٤  ١٤٠٤٨   ٦٠٠٠ S  ٣,٨  ٠,٧   ١:١٨,٨١ fail٢ban-se+
    ١ root      ٢٠   ٠   ٢٨٧١٦   ٤٨١٢   ٣٠٩٦ S  ٠,٠  ٠,٢   ٠:٠٠,٥٦ systemd
    ٢ root      ٢٠   ٠       ٠      ٠      ٠ S  ٠,٠  ٠,٠   ٠:٠٠,٠٠ kthreadd
```

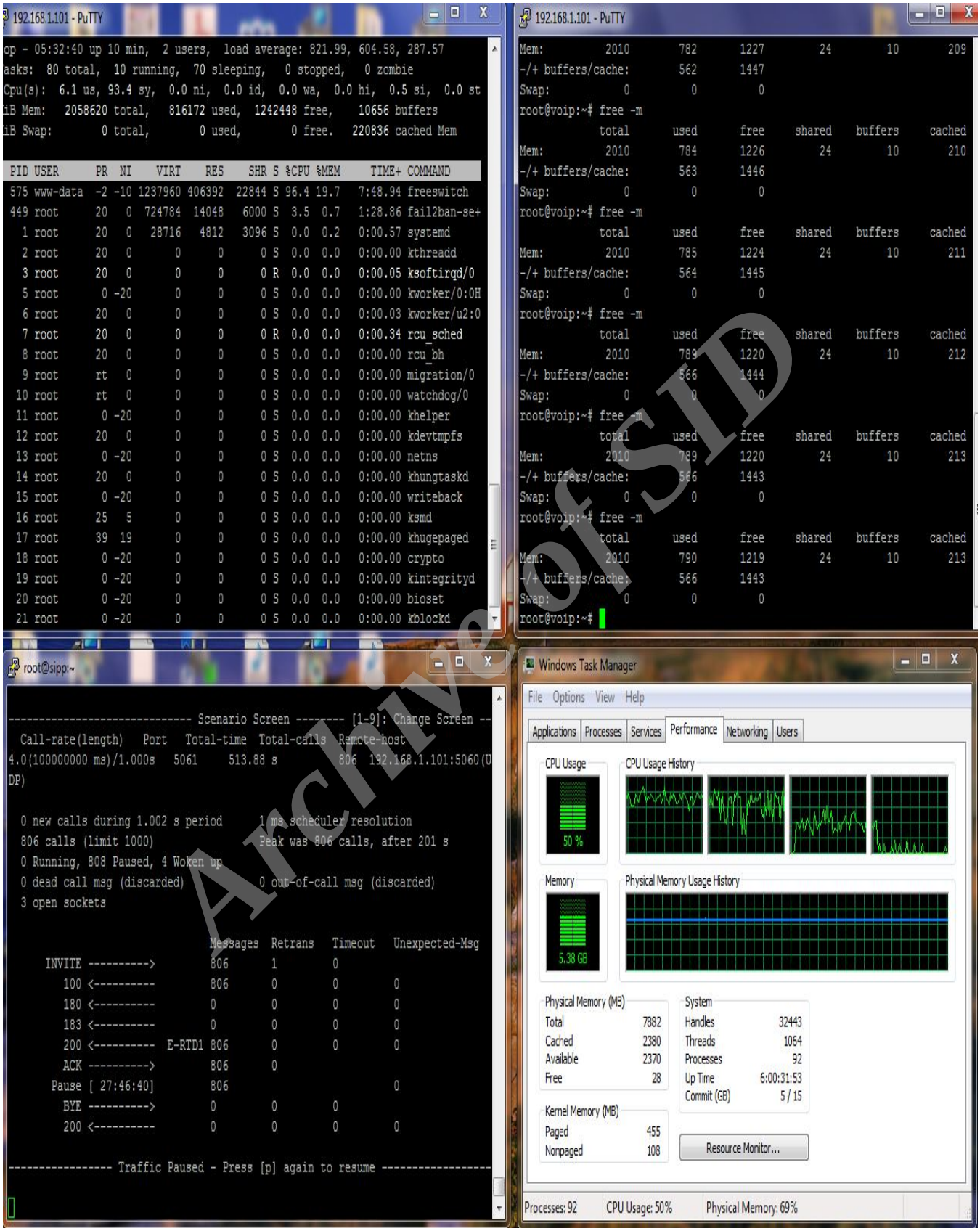
TEST ۸: ۹۰۰ concurrent call

```
------------------------Memory RAM-----------------------------
total       used       free     shared    buffers     cached
Mem:          ۲۰۱۰        ۹۰٤        ۱۱۰٦          ۲٤          ۱۰        ۲۱۹
-/+ buffers/cache:        ٦۷٤       ۱۳۳٦
Swap:            ۰          ۰          ۰
-------------------------Processor Parameters-----------------
top - ۰۵:۵۸:٤۸ up ۸ min,  ۲ users,  load average: ۸۲۷,٤۹, ۳۷۸,۰۳, ۱٤۷,۵۳
Tasks: ۱۰۹ total,  ۱۰ running,  ۹۹ sleeping,   ۰ stopped,   ۰ zombie
%Cpu(s): ۱۱,٤ us, ۸۸,٤ sy,  ۰,۰ni,  ۰,۰ id,  ۰,۰ wa,  ۰,۰ hi,  ۰,۳ si,  ۰,۰ st
KiBMem:   ۲۰۵۸٦۲۰ total,   ۹۳۱۷۲۰ used,  ۱۱۲٦۹۰۰ free,    ۱۰٤٦۰ buffers
KiB Swap:        ۰ total,        ۰ used,        ۰ free.   ۲۲۵۵۰۰ cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
  ۵۷۷ www-data  -۲ -۱۰ ۱۲۸۱٦۸٤ ٤٦۵۸۱۲  ۲۲۸۷۲ S ۹٦,۱ ۲۲,٦   ٤:۱۲,۲۸ freeswitch
  ٤۵۵ root      ۲۰   ۰  ۷۲٤۷۸٤  ۱٤۲۸۰   ٦۱۹۲ S  ۳,۵  ۰,۷   ۰:۵۳,۲٤ fail۲ban-se+
 ۱۲۷٤ postgres  ۲۰   ۰  ۲۲۷۷٤۸  ۱۲٦۸۰  ۱۰۵۲۰ S  ۰,۳  ۰,٦   ۰:۰۰,۰۳ postgres
    ۱ root      ۲۰   ۰   ۲۸۷۱۲   ٤۸۲٤   ۳۱۰۰ S  ۰,۰  ۰.۲   ۰:۰۰,۵۸ systemd
    ۲ root      ۲۰   ۰      ۰      ۰      ۰ S  ۰,۰  ۰,۰   ۰:۰۰,۰۰ kthreadd
```

TEST ۹: ۱۰۰۰ concurrent call

```
------------------------Memory RAM-----------------------------
total       used       free     shared    buffers     cached
Mem:          ۲۰۱۰        ۹۲۵        ۱۰۸٤          ۲٤          ۱۰        ۲۲٤
-/+ buffers/cache:        ٦۹۰       ۱۳۱۹
Swap:            ۰          ۰          ۰
-------------------------Processor Parameters-----------------
%Cpu(s):  ٦,۳ us, ۹۳,۲ sy,  ۰,۰ni,  ۰,۰ id,  ۰,۰ wa,  ۰,۰ hi,  ۰,۵ si,  ۰,۰ st
```

```
KiBMem:   ٢٠٥٨٦٢٠ total,   ٩٣٢١٥٢ used,  ١١٢٦٤٦٨ free,    ١٠٥٨٨ buffers
KiB Swap:        ٠ total,        ٠ used,        ٠ free.   ٢٣٠٧٤٠ cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
  ٥٧٧ www-data  -٢ -١٠ ١٢٩١٧٨٤ ٤٧٨٢٠٤  ٢٢٨٧٢ S ٩٦,١ ٢٣,٢   ٥:٣٨,٧٣ freeswitch
  ٤٥٥ root      ٢٠   ٠  ٧٢٤٧٨٤  ١٤٢٨٤   ٦١٩٢ S  ٣,٨  ٠,٧   ٠:٥٧,٥٤ fail٢ban-se+
    ١ root      ٢٠   ٠   ٢٨٧١٢   ٤٨٢٤   ٣١٠٠ S  ٠,٠  ٠,٢   ٠:٠٠,٥٨ systemd
    ٢ root      ٢٠   ٠       ٠      ٠      ٠ S  ٠,٠  ٠,٠   ٠:٠٠,٠٠ kthreadd
```



شکل 10-1 نتایج تست

3,10 تست پلتفرم Elastix

اکنون تست های بالا را برای Elastix نیز انجام می دهیم. مانند قبل ابتدا شرایط بدون تماس فعال را بررسی می نماییم و میزان مصرفی منابع را بدست می آوریم. سپس برای تماس 100، 200 و 300 تماس همزمان و بیشتر تست را انجام می‌دهیم.

TEST ۱: ۰ concurrent call

```
             total       used       free     shared    buffers     cached
Mem:          ۱۸٤۰        ٥٤۷       ۱۲۹۳          ۸          ۰        ۲۲۰
-/+ buffers/cache:        ۳۲٦       ۱٥۱٤
Swap:         ۱٥۳٥          ۰       ۱٥۳٥
top - ۱۱:٤٥:۰۳ up ۱۳ min,  ۳ users,  load average: ۰,۱۷, ۰,۱۲, ۰,۱۲
Tasks: ۱٤۲ total,   ۲ running, ۱٤۰ sleeping,   ۰ stopped,   ۰ zombie
%Cpu(s):  ۲,٥ us,  ۲,۱ sy,  ۰,۰ ni, ۹٥,۱ id,  ۰,۰ wa,  ۰,۰ hi,  ۰,٤ si,  ۰,۰ st
KiB Mem:   ۱۸۸٤۸۰۸ total,   ٥٦۱۲۳٦ used,  ۱۳۲۳٥۷۲ free,      ٤۰۰ buffers
KiB Swap:  ۱٥۷۲۸٦۰ total,        ۰ used,  ۱٥۷۲۸٦۰ free.   ۲۲٦۲۱٦ cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 ۲۰٦٤ asterisk   ۰ -۲۰ ۱۳۰۱٤٦٤  ۳۹٦٦٤  ۱۳۹٦۰ S  ۲,۰  ۲,۱   ۰:۱٤,۳۹ asterisk
 ۱۳٤۰ mysql     ۲۰   ۰ ۱۱۱۰۲٤۸  ۹٥۲۸٤   ۹۰٤۰ S  ۰,۷  ٥,۱   ۰:۰۱.۱٦ mysqld
  ۲۷۸ root      ۰ -۲۰       ۰      ۰      ۰ S  ۰,۳  ۰,۰   ۰:۰۰,۲۳ kworker/۰:۱H
  ٥۷٥ root      ۲۰   ۰  ۳۷۷۹۹٦   ۸٦٤٤   ٦۸۹٦ S  ۰,۳  ۰,٥   ۰:۰۰,٤۳ NetworkMana+
    ۱ root      ۲۰   ۰   ٤۷۸۱٦   ۳۹۸۸   ۲۲۸۰ S  ۰,۰  ۰,۲   ۰:۰۰,۸۱ systemd
```

TEST ۲: ۱۰۰ concurrent call

```
             total       used       free     shared    buffers     cached
Mem:          ۱۸٤۰        ٥٤۲       ۱۲۹۷          ۸          ۰        ۲۱٦
```

```
-/+ buffers/cache:        ۳۲۵        ۱۵۱۴
Swap:         ۱۵۳۵           ۰        ۱۵۳۵
top - ۱۱:۴۷:۳۳ up ۱۵ min,  ۳ users,  load average: ۰,۴۰, ۰,۱۷, ۰,۱۴
Tasks: ۱۴۱ total,   ۳ running, ۱۳۸ sleeping,   ۰ stopped,   ۰ zombie
%Cpu(s):  ۷,۳ us, ۵۸,۶ sy,  ۰,۰ ni, ۳۳,۷ id,  ۰,۰ wa,  ۰,۰ hi,  ۰,۴ si,  ۰,۰ st
KiB Mem:   ۱۸۸۴۸۰۸ total,   ۵۸۶۲۷۲ used,  ۱۲۹۸۵۳۶ free,      ۴۰۰ buffers
KiB Swap:  ۱۵۷۲۸۶۰ total,        ۰ used,  ۱۵۷۲۸۶۰ free.   ۲۲۶۳۰۸ cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 ۲۰۶۴ asterisk   ۰ -۲۰ ۱۳۶۰۱۰۰  ۵۴۳۳۶  ۱۴۳۱۲ S ۵۸,۸  ۲,۹   ۰:۲۸,۴۳ asterisk
 ۲۲۱۰ asterisk  ۲۰   ۰  ۱۵۵۴۴۸  ۱۵۴۱۲   ۲۳۸۸ R  ۵,۶  ۰,۸   ۰:۰۲,۸۳ op_server.pl
    ۱ root      ۲۰   ۰   ۴۷۸۱۶   ۳۹۹۲   ۲۲۸۴ S  ۰,۰  ۰,۲   ۰:۰۰,۸۲ systemd
    ۲ root      ۲۰   ۰       ۰      ۰      ۰ S  ۰,۰  ۰,۰   ۰:۰۰,۰۰ kthreadd
```

TEST ۳: ۲۰۰ concurrent call

```
              total       used       free     shared    buffers     cached
Mem:          ۱۸۴۰        ۵۹۳       ۱۲۴۷          ۸          ۰        ۲۲۱
-/+ buffers/cache:        ۳۷۱       ۱۴۶۸
Swap:         ۱۵۳۵           ۰       ۱۵۳۵

top - ۱۱:۴۸:۲۲ up ۱۶ min,  ۳ users,  load average: ۲,۰۴, ۰,۷۵, ۰,۳۴
Tasks: ۱۴۲ total,   ۲ running, ۱۴۰ sleeping,   ۰ stopped,   ۰ zombie
%Cpu(s): ۱۳,۶ us, ۸۶,۱ sy,  ۰,۰ ni,  ۰,۰ id,  ۰,۰ wa,  ۰,۰ hi,  ۰,۳ si,  ۰,۰ st
KiB Mem:   ۱۸۸۴۸۰۸ total,   ۶۰۶۱۵۲ used,  ۱۲۷۸۶۵۶ free,      ۴۰۰ buffers
KiB Swap:  ۱۵۷۲۸۶۰ total,        ۰ used,  ۱۵۷۲۸۶۰ free.   ۲۲۶۳۱۲ cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 ۲۰۶۴ asterisk   ۰ -۲۰ ۱۴۰۳۱۲۴  ۷۰۴۶۴  ۱۴۳۱۲ S ۹۳,۹  ۳,۷   ۱:۰۱,۷۸ asterisk
 ۲۲۱۰ asterisk  ۲۰   ۰  ۱۵۵۷۰۸  ۱۵۷۲۸   ۲۳۸۸ R ۱۰,۲  ۰,۸   ۰:۰۴,۰۹ op_server.pl
```

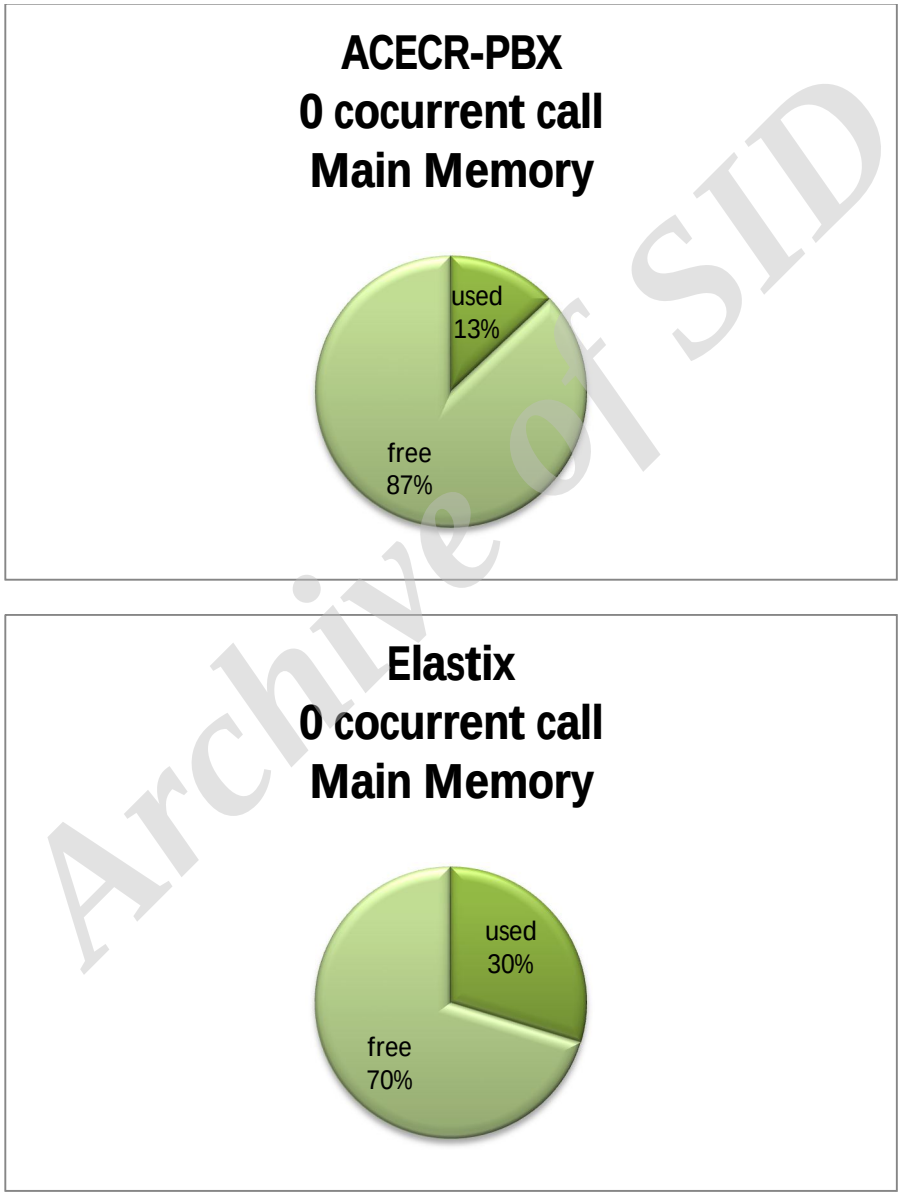
```
  ٢٣٤٢ root      ٢٠   ٠  ١٢٣٦٢٨   ١٦١٦   ١١٥٦ R  ٠,٣  ٠,١   ٠:٠٠,٩٤ top
  ٢٣٧٤ root      ٢٠   ٠        ٠      ٠      ٠ S  ٠,٣  ٠,٠   ٠:٠٠,١٥ kworker/٠:٠
```

TEST ٤: ٣١٣ concurrent call

```
KiB Mem:   ١٠١٧٤٨٠ total,   ٦٢٧٩٥٦ used,   ٣٨٩٥٢٤ free,      ٤٠٠ buffers
KiB Swap:  ١٥٧٢٨٦٠ total,        ٠ used,  ١٥٧٢٨٦٠ free.   ٢٢٣٣٨٨ cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
  ٢٠٨٥ asterisk   ٠ -٢٠ ١٤٥٩٣٠٤  ٩٢٦٣٢  ١٤٣٢٨ S ٩٩,٩  ٩,١   ٢:٣١,٩٩ asterisk
  ٢٥٦١ root      ٢٠   ٠        ٠      ٠      ٠ R  ٠,٣  ٠,٠   ٠:٠٠,٠١ kworker/٠:٢
     ١ root      ٢٠   ٠   ٤٧٨١٦   ٣٩٨٤   ٢٢٨٠ S  ٠,٠  ٠,٤   ٠:٠٠,٧٨ systemd
```

4,10 تحلیل نتایج تست

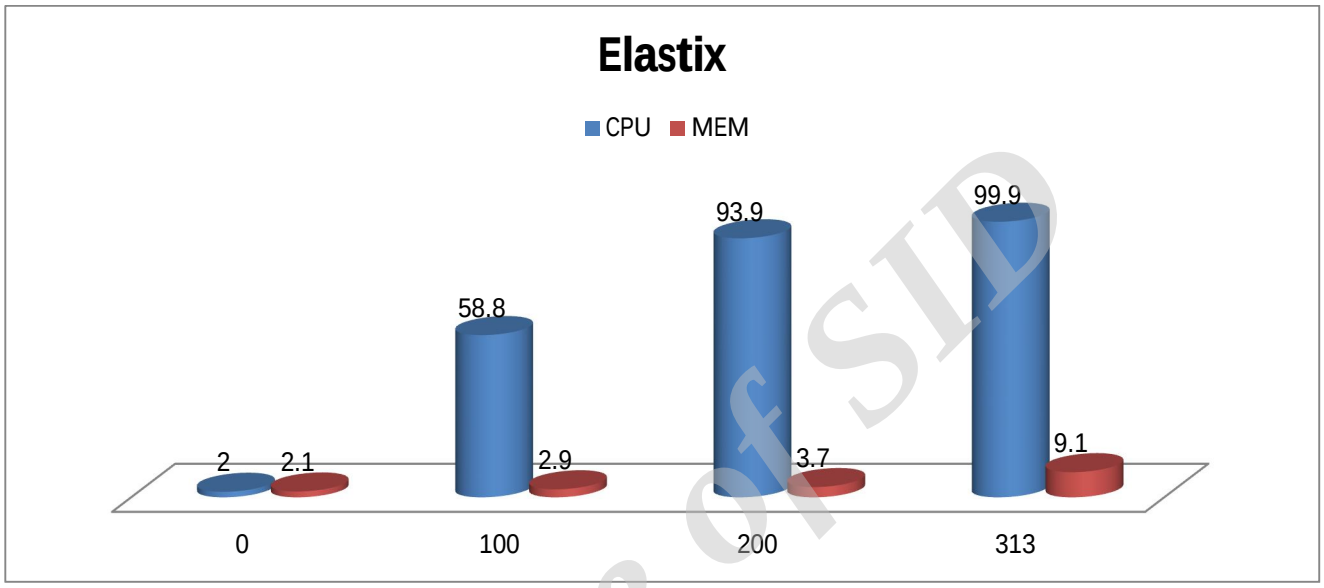
در این بخش به ترسیم نتایج حاصل از تست و تحلیل آن می پردازیم. شکل 8-2 نشان دهنده مصرف memory کلی از ماشین مجازی می باشد. با دقت در این نتایج در می یابیم که محصول منتخب به میزان منابع مصرفی کمتری نیاز دارد و این خود نقطه قوت در سیستم مبتنی برVOIP می باشد.



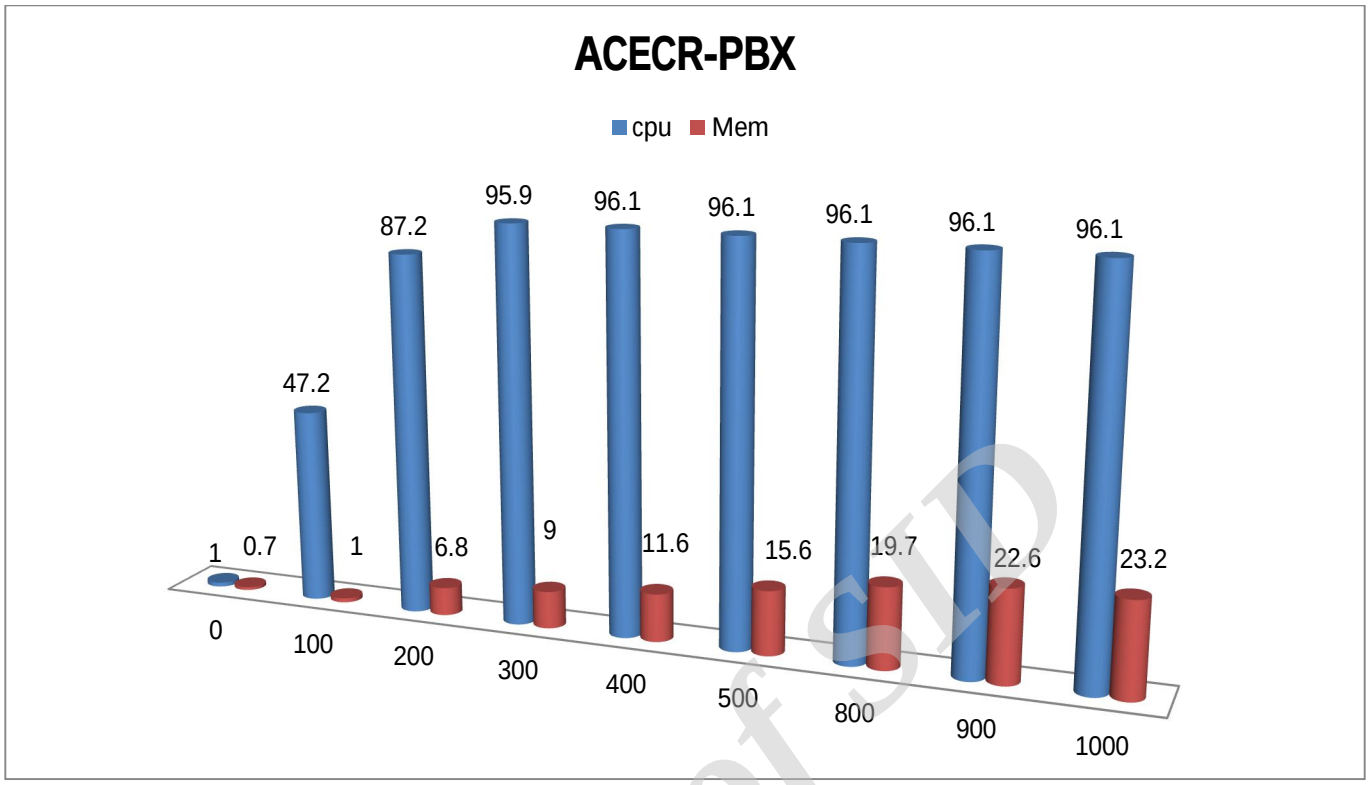
شکل 10-2 مقایسه ی میزان حافظه مصرفی راهکار پیشنهادی و Elastix

حال نتایج حاصل تماس های همزمان که در هر قسمت به صورت جدول لیست شده بود را در نمودار میله ای ترسیم می‌نماییم (شکل 9-3) و به تحلیل آن می پردازیم.

همانطور که از شکل مشخص است از منظر مصرف CPU و حافظه محصول منتخب دارای ویژگی های قابل تاملی می باشد و برای شبکه های که نیاز به امکان برقرای بار ترافیک بالایی دارند بسیار مناسب می باشد.



شکل 3-10 میزان CPU و حافظه ی مصرفی Elastix



شکل 10-4 میزان CPU و حافظه ی مصرفی راهکار پیشنهادی

11. جمع بندی

در این گزارش ابتدا مرور کوتاهی بر نتایج تحقیقات مقطع نخست پروژه داشتیم و کاربردهای عملیاتی سیستم های مبتنی بر IVR را مورد بررسی قرار دادیم. سپس به معرفی پلتفرم انتخاب شده جهت طراحی سیستم پیشنهادی و بیان مشخصات و شیوه ی عملکرد آن پرداختیم. در این مرحله از میان راهکارهای موجود و پس از انجام مقایسه ی دقیق در مقطع نخست، ساختار freeswitch برای انجام این پروژه مناسب تشخیص داده شد. به منظور فراهم کردن دسترسی ساده تر به منوها و گزینه های داخلی freeswitch یک رابط کاربری مبتنی بر وب برای سامانه طراحی گردید.

امنیت در VoIP ، موضوعی است که با گسترش روزافزون استفاده از سیستم های تلفنی تحت شبکه از اهمیت بیشتری برخوردار شده است freeswitch هم به عنوان یکی از نرم افزارهای مدیریت تماس متن باز از روش ها و تکنولوژی های مختلفی برای برقراری امنیت استفاده می کند. برای برقراری امنیت در freeswitch از دو دسته روش های پیشگیرانه (proactive) و تدافعی (defensive) استفاده شده است .در روش های پیشگیرانه از انواع مختلف روش های رمزنگاری برای غیرقابل مشاهده و شنودکردن ارتباطات SIP و RTP استفاده شده است و در روش های تدافعی،freeswitch با استفاده همزمان از ابزارهای متن باز دیگری مانند Fail۲Ban، می تواند ترافیک های مشکوک از منابع ناشناس را شناسایی و مسدود کند.یکی از ماژول هایی که.در این سامانه به منظور برقرای امنیت مورد استفاده قرار گرفته Fail۲Ban است. Fail۲Ban یک نرم افزار جانبی است که در پس زمینه اجرا می شود و لاگ ها را کنترل می کند.به محض اینکه رفتار مشکوکی را تشخیص دهد یکی از کارهای از پیش تعیین شده را انجام می دهد.

در هر سیستم تلفنی به منظور ذخیره و دسته بندی اطلاعات تماس کاربران، ذخیره ی فایل ها و داده های مورد نیاز به یک پایگاه داده نیازمندیم که در این سامانه همان طور که در بخش های پیش گفته شد از پلتفرم PostgresSQL استفاده شده است.

با در نظر گرفتن شرایط فوق و بر اساس پلتفرم انتخاب شده سامانه ای طراحی شد که دارای قابلیت های زیر است:

- پشتیبانی از تماس های همزمان با نرخ بالا
- مقیاس پذیری در حوزه ی تعریف دامنه های مجزا با قابلیت های فراوان
- پشتیبانی از انواع کدک ها
- رابط کاربری مناسب و کارا
- قابلیت ثبت تمامی رخدادها

در سامانه ی طراحی شده به سبب استفاده از فایروال های لینوکسی امنیت سیستم بالا رفته و تحقق ساختار بر روی شبکه موجب کاهش درصد احتمال نفوذ به سیستم شده است. همچنین در این ساختار می توان

به تعداد دلخواه داخلی تعریف نمود. از مهم ترین مزایای سیستم امکان گزارش گیری آنی از تمامی رخدادها و نیز برقراری صف در راستای پاسخگویی صحیح به تمامی تماس ها می باشد. در چند سازمان که ارتباطات تلفنی زیادی با یکدیگر دارند و هزینه های بالای مخابرات را پرداخت می کنند می توان با ارتباط دادن این مراکز بر روی بستر شبکه ی اینترنت و یا اینترانت هزینه های تلفنی را بسیار کاهش داد. همچنین با استفاده از ساختار منوی منشی دیجیتال می توان با پخش یک عبارت و وارد کردن اطلاعات توسط کاربر، امکان اتصال مستقیم به داخلی مورد نظر، ارسال پیام صوتی و یا ضبط آن را برای کاربران فراهم نمود.

در این مقطع از پروژه جهت پیاده سازی سخت افزاری سیستم از یک خط SIP Trunk استفاده شد و تمامی سرویس ها بر روی این زیرساخت بالا آمده است. مزایای استفاده از چنین زیرساختی عبارت است از:

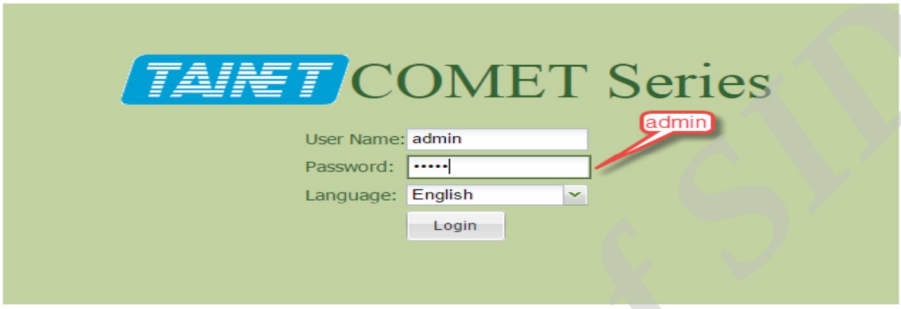
- امکان ایجاد مقیاس پذیری در ساختار تماس ها و به کارگیری در پروژه های عظیم
- عدم نیاز به سیم کشی های مجدد مانند خطوط تلفن عادی
- صرفه ی اقتصادی برای شرکت ها با توجه برقراری خدمات بر بستر اینترنت
- استفاده ی بهینه از پهنای باند
- افزایش تعداد کاربران هر خط در مقایسه با خطوط E۱ و T۱

به منظور تست مشخصات سیستم طراحی شده، با استفاده از ابزار SIPp تعداد دلخواه تماس شبیه سازی شد و از طریق شبکه ی LAN به سمت سرور ارسال گردید و همچنین یک تماس هم به صورت دستی برقرار گردید.مقایسه ی میزان منابع مصرفی از جمله CPU و حافظه در راهکار پیشنهادی و پلتفرم Elastix حاکی از آن است که در حالتی که هیچ تماسی بر روی سرور ارسال نشده است میزان حافظه ی اشغال شده توسط Elastix در حدود دو برابر راهکار پیشنهادی می باشد.هم چنین به ازای ارسال ترافیک یکسان بر روی هر دو پلتفرم، مشاهده شد که مقدار CPU مصرفی در ساختار ACECR-PBX کمتر است.نکته ی بسیار مهم و قابل توجه در نتایج تست این است که با توجه به سخت افزار یکسان مورد استفاده در تمامی تست ها، بیشینه ی تعداد تماس همزمانی که در Elastix می توان به آن رسید در حدود 300 تماس است در حالی که در ساختار پیشنهادی می توان تا تعداد 1000 تماس همزمان هم کارایی مناسبی از سیستم داشت و کیفیت تماس ها قابل قبول خواهد بود.

12.ضمیمه

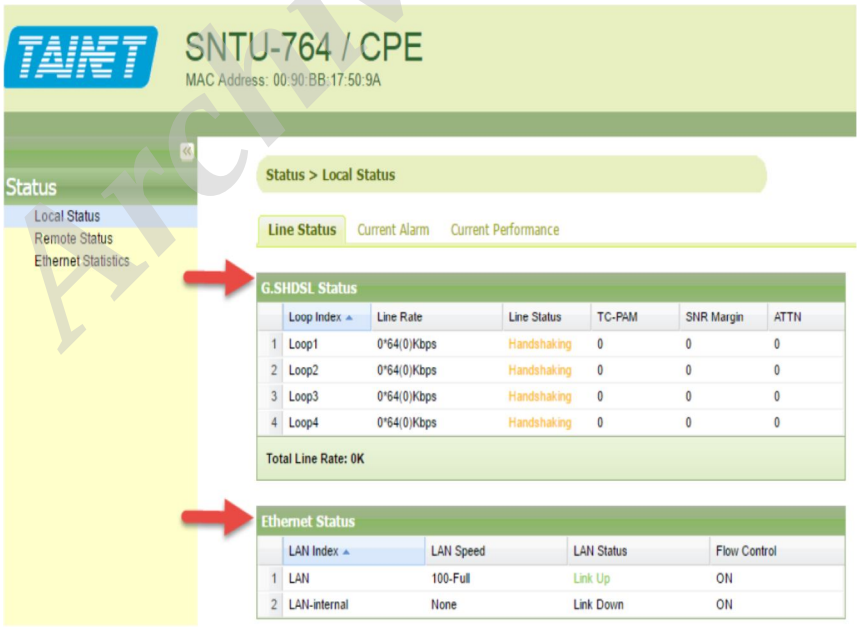
1,12 تنظیمات دستگاه GNTU764

ابتدا به IP دستگاه که 192,168,0,1 میباشد از طریق(browser ترجیحا Google Chrome) متصل شده و به دستگاه login کنید (شکل 11-1) .



شکل 11-1 : صفحه ورودی

در قسمت status >line status میتوانید مشخصات مربوط به پورت های G.shdsl و Ethernet را مشاهده فرمایید.



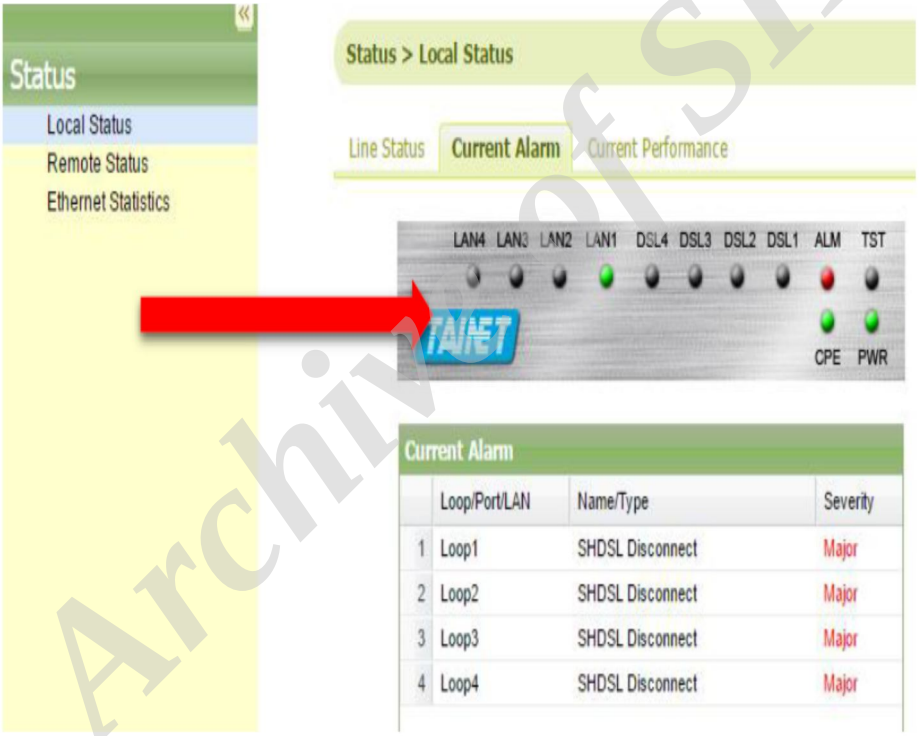
شکل 11-2 : صفحه وضعیت

در قسمت G.Shdsl >line rate میتوانید سرعت هر زوج را مشاهده فرمایید

در قسمت line status وضعیت ارتباط هر لینک قابل مشاهده میباشد.

توجه : این نکته قابل ذکر میباشد که (line rate سرعت هرخط(با SNR مسیر ارتباط معکوس داشته و بستگی به طول مسیر و کیفیت مسیر دارد.

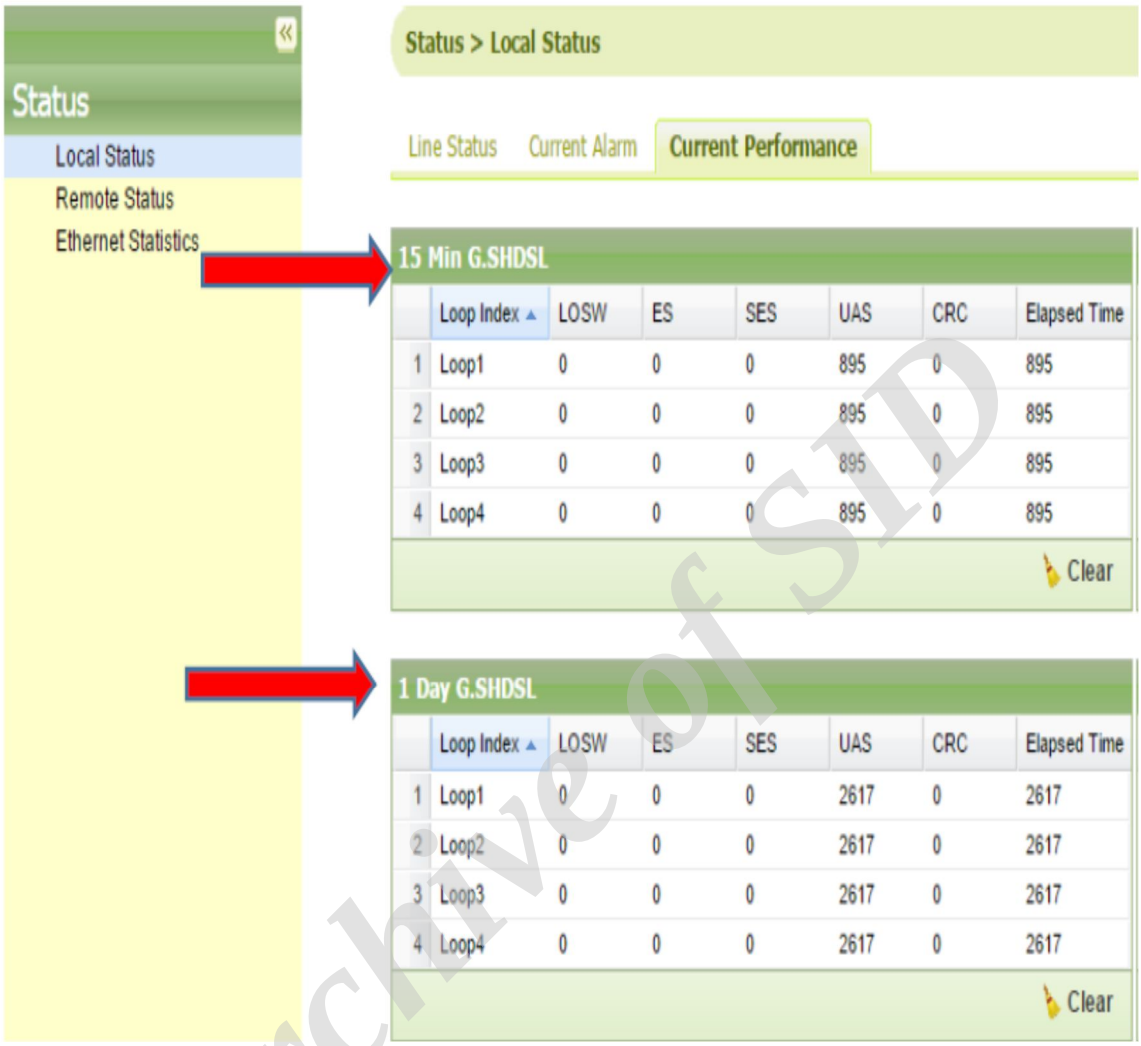
Current Alarm2,12



شکل 3-11 : Current Alarm

Current performance3,12

در قسمت Current performance میتوانید در منوی اول وضعیت هر لینک در 15 دقیقه قبل و در منوی بعدی وضعیت هر لینک در یک روز را کامل را به طور دقیق مشاهده فرمایید.



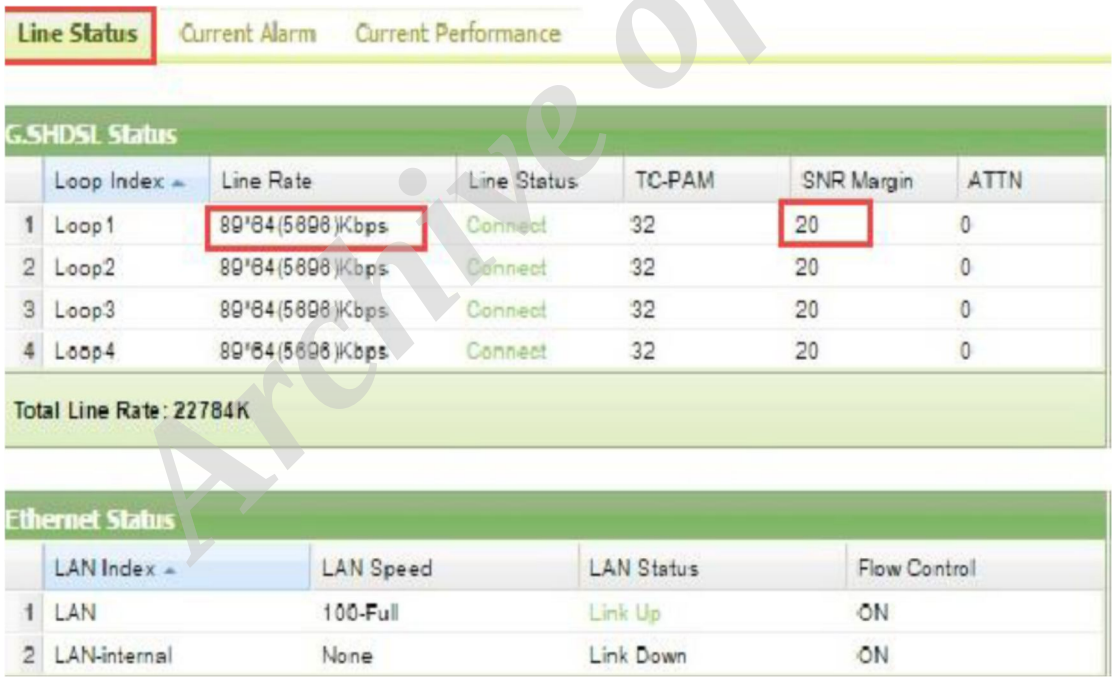
شکل 4-11 : Current performance

استاندارد صنعتی SHDSL در توصیه نامه ی ITU G.991,2 تعریف می شود. در ابتدا، این استاندارد در فوریه 2001 انتشار یافت.

آپدیت های اصلی G.991,2 در دسامبر 2003 مطرح گردید. تجهیزات منطبق با نسخه ی 2003 استاندارد G.991,2 اغلب به استانداردهای G.SHDSL یا SHDSL.bis ارجاع داده می شود . توصیه نامه ی G.991,2 روش انتقال داده

برای شبکه های دسترسی را تعریف می کند، اغلب G.SHDSL نامیده می شود. این توصیه نامه به صورت رسمی در سال 2003 انتشار یافت و در سال 2005 مواردی به آن اضافه شد. به عبارت دیگر، SHDSL یک توصیه نامه ی بسیار استاندارد است . کریرهای امروزی علاقه مند به اتصال مشتریان تجاری به شبکه های مترو هستند . تکنولوژی G.SHDSL.bis EFMبهترین راهکار برای شرکت ها با حجم تقاضای معینی در پهنای باند متقارن است. این تکنولوژی مزیت حداکثر کردن عملکرد سیم مسی با سرعت بیشتر و مسافت طولانی تر را دارد. به علاوه، با ارائه ی پکیج های مختلف پهنای باند با استفاده از تکنولوژی باندینگ G.SHDSL.bis ، این تکنولوژی بهترین راهکار برای کریرها است تا ارائه ی سرویس خود را گسترش دهند.

* همانطور که در تصویر زیر مشاهده می کنید در Normal Mode حد اکثر سرعت هر زوج 5,7 مگابیت بر ثانیه میباشد.



شکل 11-5 : وضعیت خط

Extended mode 4,12

یکی از مهم ترین نکات مثبت و مورد توجه این دستگاه است که توسط شرکت Tainet به صورت اختصاصی برنامه ریزی شده است و انتقال پرسرعت اترنت تا 60 مگابیت بر ثانیه روی چهار زوج مسی را مقدور می سازد.

در صورتی که از Extended mode استفاده می شود در هر دو سمت CO و CPE لینک، گزینه proprietary برای Mode ، TC-PAM-128 برای Options و عدد 239 برای Extended Rate انتخاب گردد.

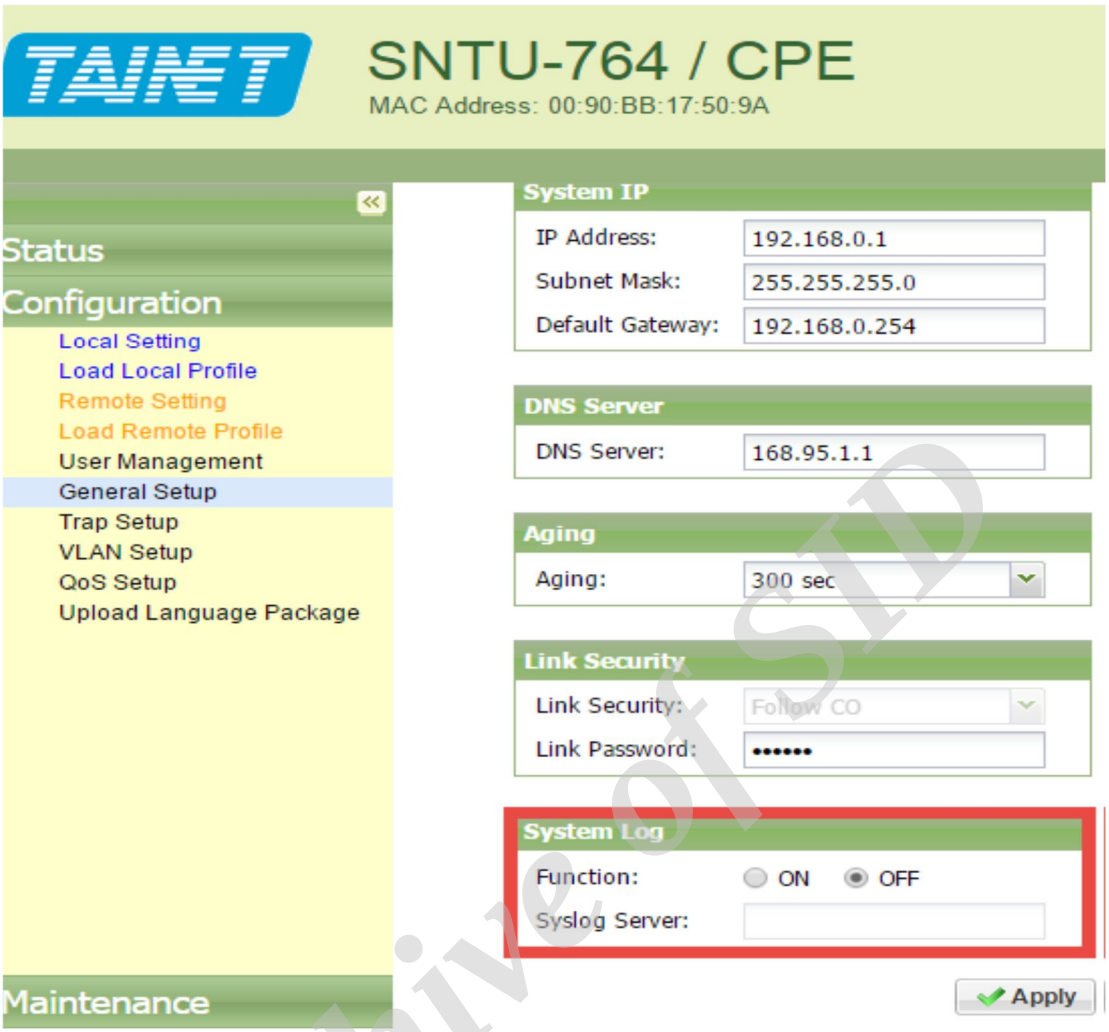
توجه داشته باشید که Extended mode برای فواصل زیر 2 کیلومتر قابل راه اندازی میباشد و اصولا موقعی مورد استفاده خواهد بود که در حالت G.991,2 خطوط با عرض باند 195 مگابیت بر ثانیه و با SNR بالای 10 برقرار گردند.(در پایان apply کرده و تنظیمات را save نمایید.

system log 5,12

پروتکلی است که به دستگاه اجازه ارسال log ها ی خود به سرور را میدهد . در مواقعی که رویدادی در شبکه رخ می دهد تجهیزات شبکه این توانایی را دارند که رویداد را در قالب یک پیغام به سرور یا مدیر شبکه اطلاع دهند.

زمانی log فرستاده میشود که یک error اتفاق افتاده باشد و یا برای مثال یک رویداد معمولی ولی مهم مانند login کردن کاربران اتفاق می افتد این پیغام به صورت Notification به syslog server ارسال میگردد.

شما قادر هستید با تخصیص مشخصات مورد نظر syslog server در این سیستم آن را فعال نمایید.



شکل 11-6 : آدرس ها

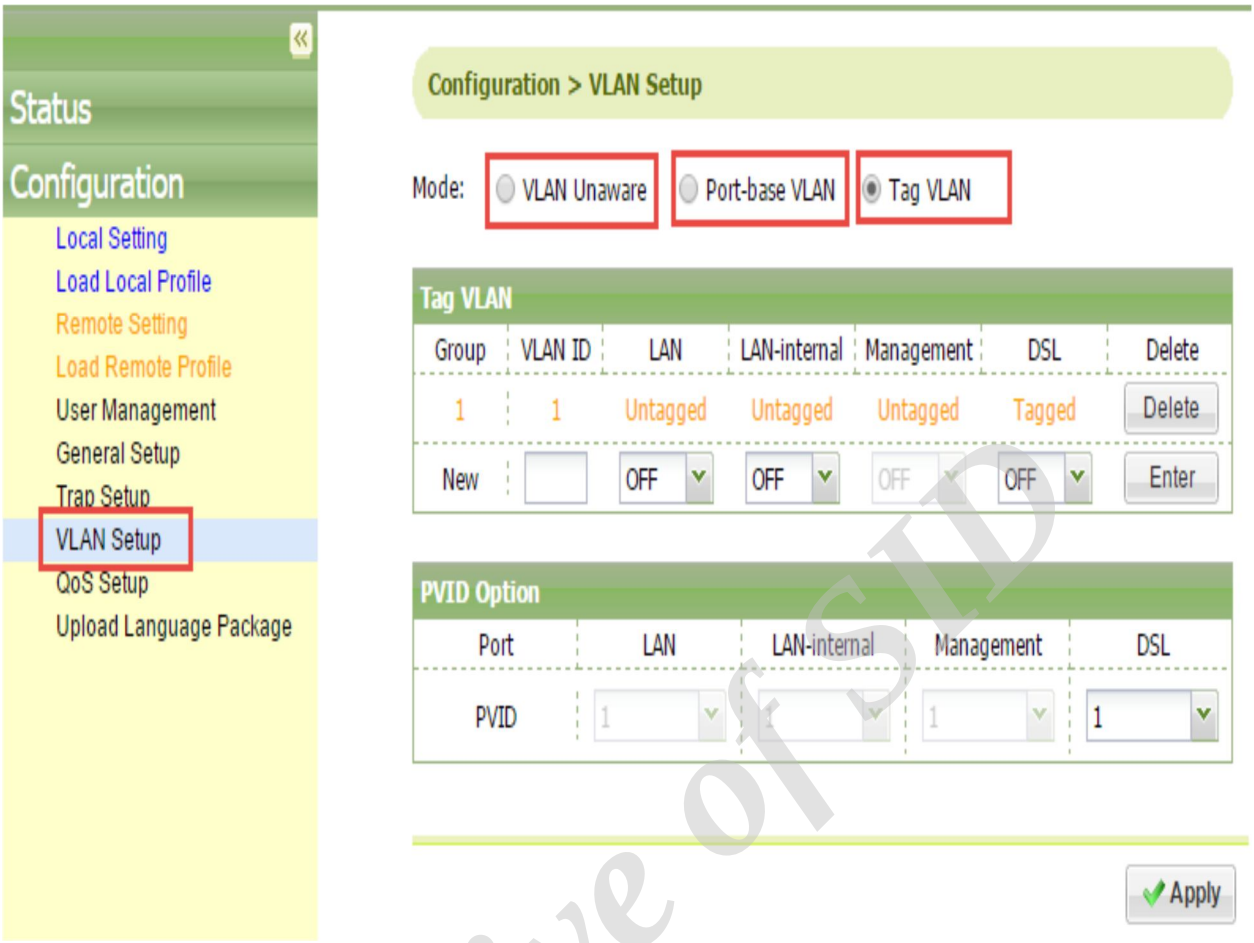
Vlan Setup 6,11

Virtual Local Area Networke به معنی شبکه محلی مجازی میباشد. هر شبکه محلی دارای یک Broadcast domainاست. با ایجاد VLAN میتوان Broadcast را محدود کرد و با این عمل ترافیک شبکه را کاهش داد.در این قسمت شما میتوانید با ایجاد Vlan هریک از پورت های این دستگاه را به آن اختصاص دهید. در قسمت سه گزینه مشاهده می کنید که بدین معنا است:

VLAN Unaware:غیر فعال بودنvlan

Port Base VLAN : میتوان پورت های Lan ، Lan internalو DSL را به Vlan مربوطه اختصاص داد.

VLAN Trunking : Tag Vlanباعث میشود که سوئیچها از فرآیندی استفاده کنند که VLAN Tagging نامیده میشود. همان طور که از نام این فرآیند مشخص است، VLANها برچسب گذاری میشوند، تا هویت بستههای ارسالی و دریافتی مشخص باشد و سوئیچها بدانند کدام فریم متعلق به کدام VLAN میباشد . در حقیقت وقتی بستهای میخواهد از پورت ترانک سوئیچی خارج گردد، سوئیچ به آن بسته یک برچسب می زند، که در آن برچسب شماره VLAN یا (VLAN ID) که این بسته به آن تعلق دارد را قرار می دهد تا از این طریق سوئیچهای دیگر متوجه شوند که بسته دریافتی به کدام یکی از VLAN هایشان مربوط است . اما سوئیچها چگونه VLAN ID را پیدا میکنند؟ برای این کار طبق یک استاندارد، سوئیچ قبل از اینکه فریم را به سوئیچ دیگری ارسال کند، یک Header را به فریم اضافه میکند که VLAN IDدر آن Header قرار میگیرد. بنابراین سوئیچ وقتی فریمی را دریافت می کند اول Header آن را خوانده و VLAN ID آن را چک میکند تا بداند بسته به کدام یکی از VLAN ها تعلق دارد.



شکل11 -7 : VLAN

Maintenance 6,12

در قسمت maintenance :میتوانید پارامتر های مختلفی که مربوط به وضعیت ارتباطی دستگاه میباشد را بررسی کنید

Alarm : میتوان وضعیت ارتباط هر زوج را در هر دو سمت لینک ، یعنی Local و Remote مشاهده نمایید.

Performance History : در این قسمت نیز میتوان پارامتر های ارتباطی را در 15 دقیقه و یا 1 روز کامل مشاهده کرد.

شکل 11-8 : Alarm log

Refrences:

[1]. Chitralekha Bhat, Mithun BS, Vikram Saxena, Vrushali Kulkarni, Sunil Kopparapu." Deploynig Usable Speech Enabled IVR Systems for Mass Use." In Human Computer Interactions (ICHCI) International Conference, ۲۰۱۳

[2]. Zilole Simate, "Investigating the use of interactive voice response (IVR) in medical adherence monitoring." In Medical Information and Communication Technology (ISMICT) ۸th International Symposium,

[3]. Dineshkumar Singh, Divya Piplani, Siddhesh Nar, Srinivasan Karthik, "ICT Platform for Climate Change Adaptation in agriculture." In Communication Systems and Networks (COMSNETS) ۷th International Conference,

[4]. Ansari, Abdullah Mohammad, Md Faisal Nehal, and Mohammed Abdul Qadeer. "SIP-based interactive voice response system using freeswitch epbx." In Wireless and Optical Communications Networks (WOCN), ۲۰۱۳ Tenth International Conference on, pp. ۱-۵. IEEE, ۲۰۱۳
Ericsson Research, 2010 Ninth International Conference on Grid and Cloud Computing, 2010

[5]. https://wiki.freeswitch.org/wiki/Main_Page

[6]. P Y Shinde, R Sheth, "Voip Technology: Analysis of Security Issues." International Journal of Recent Trends in Engineering & Research, 2015

[7]. Eduardo B. Fernandez, Juan C. Pelaez, Maria M. Larrondo-Petrie, "Security Patterns for Voice over IP Networks."International Multi-Conference on Computing in the Global Information Technology, 2007

[8]. Angelos D. Keromytis, "Voice-over-IP security: Research and Practice."IEEE Security & Privacy, 2010

[9]. David Butcher, Xiangyang Li, Jinhua Gho, "Security Challenge and Defence in VOIP Infrastructures." IEEE Transaction on Systems, Man and Cybernetics, 2007

[10]. Angelos D. Keromytis, “A Comprehensive Survey of Vulnerabilities and Academic Research.” SpringerBriefs in Computer Science, 2011

[11]. Thomas Porter, Jan Kanclirz, “Practical VOIP Security” Elsevier, 2006

[12]. Minessale II, Anthony, and Giovanni Maruzzelli. Mastering FreeSWITCH. Packt Publishing Ltd, 2016.

[13]. Diksha Golait, Neminath Hubballi, “Detecting Anomalous Behavior in VoIP Systems: A Discrete Event System Modeling.” IEEE Transactions on Information Forensics and Security, 2017

[14]. Mahsa Hosseinpour, Seyed Amin Hosseini Seno, “Modeling SIP normal traffic to detect and prevent SIP-VoIP flooding attacks using fuzzy logic.” Internationa Conference on Computer and Knowledge Engineering (ICCKE), ۲۰۱٦

[۱٥]. Panagiotis Galiotos, Christos Anagnostopoulos, “Non-conforming behavior detection for VoIP-based network systems.” IEEE International Conference on Communications (ICC), ۲۰۱٦

[۱٦]. H. Hakan Kilinc, Ugur Cagal,” A reputation based trust center model for cyber security.”٤th International Symposium on Digital Forensic and Security, ۲۰۱٦

[۱۷]. Ahmad Ghafarian, Seyed Amin Hosseini Seno, “An empirical study of security of VoIP system.” SAI Computing Conference, ۲۰۱٦

[۱۸]. Jin Tang, Yu Cheng, Yong Hao,” VoIPFD: Voice over IP flooding detection.”INFOCOM IEEE Proceedings, ۲۰۱۲

[۱۹]. Frantz Cadet, Daniel T. Fokum,” Coping with denial-of-service attacks on the IP telephony system.”SoutheastCon, ۲۰۱٦

[20]. Dialogic, SIP Trunking: Enabling Wideband Audio for the Enterprise,

[21]. Magnusson, Janne. "SIP Trunking Benefits and Best Practices." Ingate Systems white paper 2006.

[22]. TAINET, user Manual, G.SHDSL.bis ATM/EFM, GNTU 764/102 , 2016

[23]. Private IaaS Clouds: A Comparative Analysis of OpenNebula, CloudStack and OpenStack, Adriano Vogel, Dalvan Griebler, et al, 2016 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing. 2016

[24]. 2015A Survey on Open-source Cloud Computing Solutions, Patrícia Takako Endo1, Glauco Estácio Gonçalves, et al, VIII Workshop em Clouds, Grids e Aplicações.

[25]. 2014Comparison of multiple IaaS Cloud platform solutions, OMAR SEFRAOUI, MOHAMMED AISSAOUI, MOHSINE ELEULDJ, Recent Researches in Information Science and Applications.

[26]. شرکت تکوین اندیشه برتر، مشخصات فنی مودم های TAINET ، 1395.