فصلنامه آموزش مهندسی ایران، شماره ۳۷، سال دهم، ص۱۴۵- ۱۲۵

طراحی و پیاده سازی سیستم شبکه ای امنیت، نظارت وحفاظت ملی

حسین مهربان جهرمی [۱]، برهان جلائیان [۲]، عباس مهربان جهرمی [۳] و محسن مصلی نژاد [۳]

۱. دانشگاه آزاد اسلامی واحد جهرم، باشگاه پژوهشگران جوان

۲. دانشکده مهندسی برق و کامپیوتر، دانشگاه ملی سنگاپور

۳. دانشکده مهندسی، دانشگاه شیراز

چکیده: در سالهای اخیر، رشد سریع شبکه‌های ارتباطی و فناوری مخابراتی فرصتهای مهم و چالشهای زیادی در خصوص ارتباط بی درنگ[۱]، مانیتوررینگ و کنترل سیستم ها از راه دور ایجاد کرده است. در این مقاله بعد از بررسی سایر تحقیقات پیشین در این زمینه، به معرفی و توسعه کنترل و مانیتورینگ تحت شبکه های کامپیوتری در خصوص امنیت، نظارت و حفاظت مراکز حساس تجاری، نظامی و ... از راه دور پرداخته و در ادامه گامهای طراحی این سیستم ها بررسی شده است. سپس به روش مبتنی بر Web به عنوان یکی از روشهای مبتنی بر شبکه و اهمیت شبکه‌های VPN به عنوان راهکاری برای تأمین امنیت این سیستم کنترل از راه دور بررسی و مزایای VPN بیان شده است. در انتها به مقایسه این روش با سایر روشهای مشابه، توجیه اقتصادی این روش و ویژگیهای آن پرداخته شده است.

واژه های کلیدی: امنیت بلادرنگ، شبکه، کنترل از راه دور، نظارت، Labview و VPN

---

1 . Real time

۱. مقدمه

با پیدایش امکانات نوین مخابراتی و اتوماسیون کامپیوتری، نیازهای جدیدی در زمینه حصول راهکارهایی ایمن، در مواجهه با شرایط بحرانی مطرح می‌شود. نظارت و حفاظت از مراکز حساس بنیادین یک کشور [مانند: بانکها و مراکز تجاری، مراکز نظامی، نیروگاهها، فرودگاهها، ادوات و مرکز مخابراتیPSTN، شبکه مخابراتی تلفن همراه GSM و...] از جمله مسائل اصلی در تأمین امنیت ملی است.

در این خصوص، امروزه درسطح جهان پژوهشهای متعددی انجام می‌شود. این گونه سیستم‌های امنیتی از دو دیدگاه عمده قابل بررسی و پژوهش است:

الف) طراحی ساختارهای مدیریت، تصمیم‌گیری مناسب هنگام ایجاد شرایط بحرانی و چگونگی ارتباط و تبادل اطلاعات بین سیستم‌های مختلف جمع آوری و اعلان داده های وضعیت امنیتی[۱].

در این زمینه الگوهای زیادی مطرح شده است. اطلاع رسانی وضعیت بحرانی به مراکز مسئول امنیتی نقطه عطف مشترک کلیه این روشها ست[۱،۲ و۳]. انتخاب نوع رسانه انتقال اطلاعات از مسائل عمده در طراحی این گونه سیستم ها به شمار می‌رود و می‌تواند محدودیتهایی را برای ساختار سیستم امنیتی مذکور ایجاد کند. استفاده از رسانه‌هایی با امکان توزیع اطلاعات در سطحی وسیع تر و با سرعتی بیشتر مطلوب‌تر است، چون اعلام سریع وضعیت بحرانی یک مرکز حساس به سایر مراکز، امکان آمادگی مقابله آنها، را در صورت وقوع وضعیت مشابه در فاصله زمانی اندک فراهم می سازد[۳].

سیستم‌های هشدار دهنده برای اعلام وضعیت به صورت گسترده از دیگر مسائل اصلی در ارتقای امنیت ملی است. در این سیستم‌ها تجهیزات زیادی در حال نظارت برای وقوع شرایط ویژه هشدار هستند. هنگام وقوع حادثه سایت مذکور، وقوع و شرایط هشدار به LEPC (Local emergency Planning Committee) اعلام می شود. LEPC فرمان روشن شدن هشدار به صورت صوتی، نوری یا . . . ، را به منطقه مورد نظر می دهد. تعیین منطقه وقوع حادثه از روی IP فرستنده در مناطق مورد نظر بررسی می شود و فرمان ALARM به سیستم های هشدار که خود جزیی از شبکه

هستند و تحت TCP/IP کار می‌کنند، فرستاده می شود و شروع به هشدار دادن می‌کنند. در اختراع Lyn Lauterbach, Larid H. Wise [۱۳]، سیستم هشدار گسترده با زیر ساخت شبکه PSTN به منظور ارسال و جمع آوری داده‌ها به ستاد محلی برنامه‌ریزی حوادث(LEPC)، پیشنهاد شده است. هنگام وقوع حادثه یک تماس تلفنی یا رادیویی با LEPC برقرار می شود، سایت وقوع و شرایط هشدار اعلام می‌شود. LEPC موظف است از طریق یک فرستنده رادیویی یک سیگنال (Code Cap Code Assignment Plan) در فضا منتشر کند. CapCode یک هویت الکترونیکی است که در حافظه گیرنده های مورد نظر وجود دارد و گیرنده ها از یکدیگر بدین وسیله تمیز داده می شوند. روش پیشنهادی در این مقاله دو مزیت عمده به سایر موارد مشابه دارد: ۱. تعیین مکان وقوع حادثه به راحتی و با سرعتی بالاتر امکان پذیر است. ۲. با توجه به استفاده از شبکه‌های کامپیوتر نیاز به صرف زمان برای برقراری مکالمه نیست و وضعیت به صورت بی‌درنگ مخابره می‌شود.۳. متمایز ساختن اعلانگرهای هشدار از طریق TCP/IPپیچیدگی سیستم را تا حد زیادی پایین می آورد.

ب. طراحی سیستم های سخت افزاری جمع آوری داده‌ها، نحوه ارسال و مخابره داده ها، توپولوژی و ماهیت اتصالات و ارتباطا ت این زیر سیستم ها

۱. چگونگی حس کردن وضعیت(Sensing)در هنگام جمع آوری آطلاعات

۲. نوع رسانه انتقال دو محور اساسی طراحی در لایه فیزیکی هستند.

جمع‌آوری اطلاعات از مراکز فیزیکی به دو صورت Online و Offline امکان‌پذیر است. در روش Offline بعد از وقوع حادثه سیستم‌های ثبت وضعیت یا اپراتور، داده‌ها را در Database Server ذخیره می‌کنند.

ایجاد Data-Base های بحرانی برای مراکز حساس نیز می‌تواند امکان مرور،جستجو و بررسی وضعیتهای خاص در گذشته را به منظور آمادگی و پیشگیری از وضعیتهای خاص مشابه احتمالی آتی فراهم کند[۲].

سیستم های Real-Time که از موارد جمع‌آوری اطلاعات به صورت Online بر شمرده می‌شود، ضمن برخورداری از کلیه مزایای روش Offline، امکان نظارت و

کنترل بی‌درنگ مراکز حساس در هر لحظه از راه دور وجود دارد. بسته به نوع رسانه انتقال داده‌ها، نحوه دسترسی کاربر یا کاربران و برد سیستم امنیتی از راه دور متفاوت است. اکثر طرحهای امنیت از راه دور مبتنی بر شبکه‌های تلفنی[1] PSTN، خطوط تلفن داخلی PABX یا شبکه تلفن همراه (GSM) به عنوان رسانه انتقال داده‌ها هستند.

Ismail Conkun و Hamid Ardam یک سیستم کنترل از راه دور وسایل منزل و دفاتر اداری مبتنی بر شبکه تلفن را پیشنهاد و طراحی کردند. این سیستم ها ضمن ساده بودن و کارایی خاص در خصوص اتوما سیون خانگی، می‌توانند یکی از گزینه‌های طراحی در سیستم‌های امنیتی کنترل از راه دور باشند[۸ و۱۵]. در روش پیشنهادی در این مقاله با توجه به استفاده از شبکه های کامپیوتر نیاز به صرف زمان برای برقراری مکالمه نیست و وضعیت به صورت بی‌درنگ مخابره می‌شود. در ضمن، با توجه به استفاده از طیف فرکانسیس آزاد بر روی خطوط تلفن[در روش ADSL] یا بر روی خطوط برق [در روش power line carrier PLC] مقادیر زیادی در هزینه سیستم و هزینه کانال مخابراتی نسبت به روشهای سابق صرفه جویی می‌شود. پیچیدگی مدارهای کنترلر در روشهای پیشین از دیگر معایب آنها است.

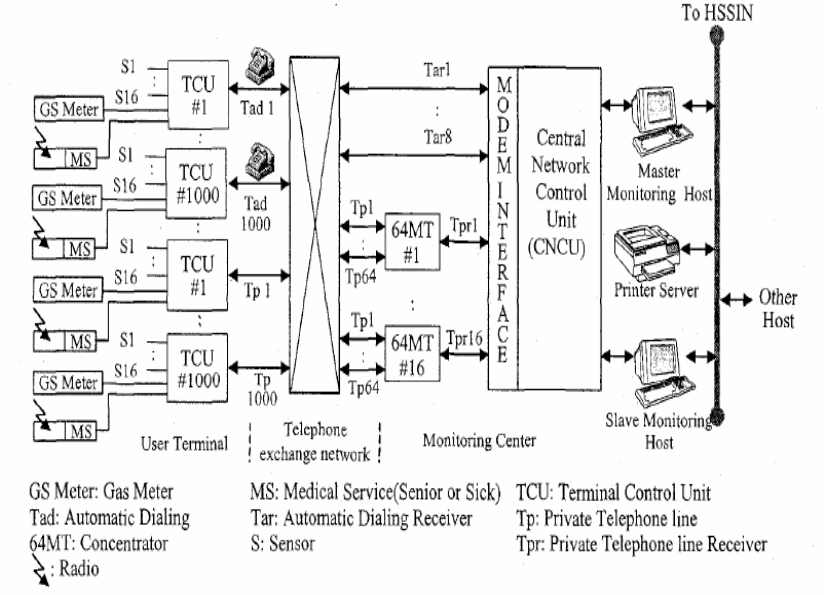
Brian W Pinzon یک سیستم بستن و باز کردن قفل در منازل از راه دور مبتنی بر خطوط تلفن یا کنترل بیسیم با برد کوتاه را پیشنهاد کرده است[۱۶]. این سیستم عیب عمده سایر روشهای مبتنی بر خطوط تلفن را دارد.

A. R. Al-Ali و M. Al-Rousan یک سیستم اتوماسیون تحت JAVA که قابلیت کنترل و مانیتورینگ وسایل خانگی را دارد، ارائه کردند. سیستم یاد شده از یک Embedded Controller محلی مرتبط با وسایل خانگی تشکیل شده که به PC متصل است و نرم افزار های Server تحت JAVA امکان کنترل و نظارت بر آن را

1. Public Switch Telephone Network

از طریق یک Web Browser در هر نقطه متصل به اینترنت به کاربر می‌دهد[۱۳]. استفاده از نرم افزار Labview در روش پیشنهادی ما پیچیدگی طراحی Server را تا حدود زیادی پایین می آورد. همچنین، استفاده از یک شبکه خصوصی بدون اتصال به اینترنت، امنیت را که عامل اصلی در روش مطرح شده است، افزایش می دهد.

P.C Yang و Cheng-Lung Chang ساختار امنیتی منازل APX-Home Security System را مطرح کردند[۱۸]. معماری APX-HSS در شکل ۱ نشان داده شده است. این معماری از سه قسمت اصلی تشکیل شده است: ۱. پایانه کاربر: بخش کنترل پایانه[این قسمت کلیه سیگنالهای ارسالی از یک منزل را که دریافت و فرستاده می شوند ترکیب می‌کند که شامل سیگنالهای امنیتی مانند اعلان حریق، دزدگیر، قفل درها، اعلان نفوذ از پنجره و سیگنالهای دیگر مثل کنتور گاز و ... هستند]؛ ۲) تجهیزات شرکت تلفن؛ ۳) تجهیزات مرکز نظارت.



شکل ۱ : معماری APX-HSS[15]

۲.گامهای طراحی سیستم پیشنهادیمبتنی بر شبکه

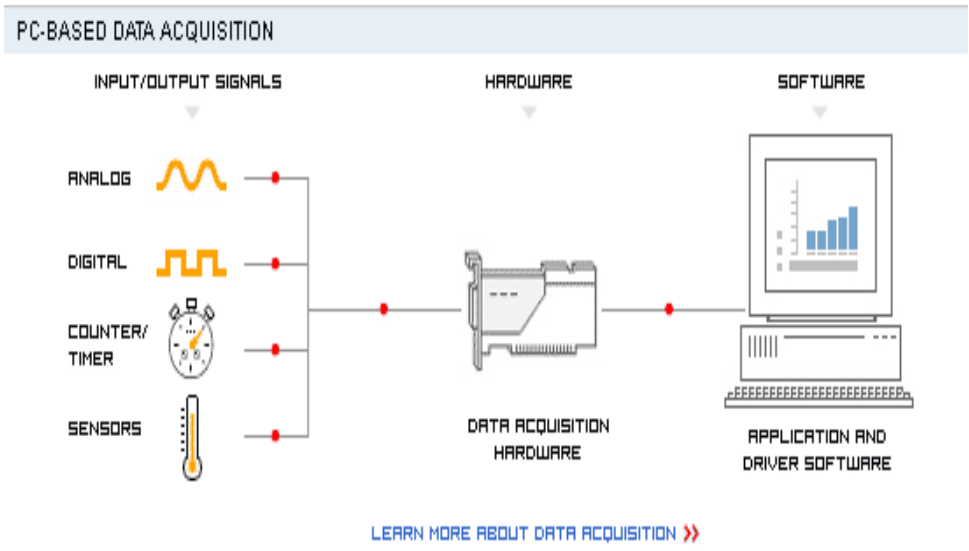
گام اول: شناخت فرایند امنیتی و مدلسازی آن: دراین مرحله باید موارد زیر بررسی شود:

- مشخص شدن ورودی ها و خروجی ها؛
- تعیین هدف از کنترل و نظارت محیط؛
- تشخیص ورودیهایی که کنترل روی آنها انجام می شود (مانند کنترل درها، کنترل دما، وضعیت دزدگیر و ...)؛
- چگونگی ارتباط سیستم دزدگیر مرکز مورد نظر با سیستم پیشنهادی؛
- چگونگی ارتباط سیستم اعلان حریق مرکز مورد نظر با سیستم پیشنهادی؛
- چگونگی ارتباط سایر سیستم های مرکز مورد نظر با سیستم پیشنهادی؛
- تشخیص ورودیهای که کنترل روی آن ها انجام می گیرد؛
- تشخیص خروجیها و اطلاعات حساسی که باید به صورت زمان حقیقی نظارت شوند.

گام دوم: بررسی رفتار و عملکرد فرایند امنیتی و طراحی زیر ساخت سیستم: در این مرحله باید کارت(Data Acquisition- DAQ)مناسب را طراحی یا انتخاب کرد.

DAQ فرایند گردآوری اطلاعات است که در یک مد اتوماتیکی از منابع اندازه‌گیری دیجیتال و آنالوگ مثل حسگرها و قطعات مربوطه عمل می کند.DAQ برای فراهم کردن یک سیستم اندازه‌گیری قابل انعطاف از ترکیبی از اندازه‌گیریهای مبتنی بر PC (سخت افزاری و نرم افزاری) می باشند استفاده می‌کند.

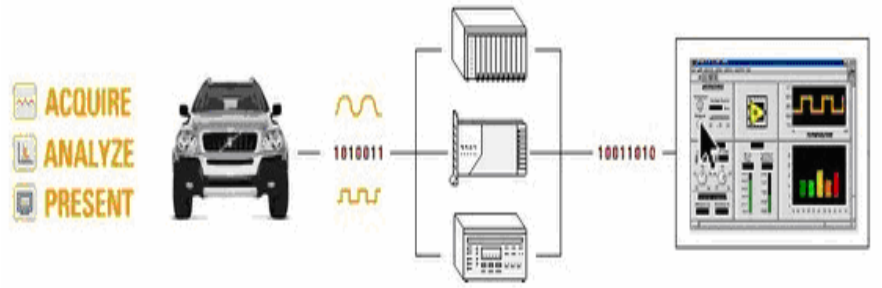
مطابق شکل زیر ورودی‌های DAQ می تواند انالوگ، دیجیتال، شمارنده‌ها، تایمرها و حسگرها باشد که این ورودیها به DAQ وارد می‌شود و خروجی آن به کامپیوتر می‌رود.



شکل۲: نقش DAQ در ارسال سیگنالهای مختلف به کامپیوتر

یک Data Logger به وسیله حسگرهایی کار می‌کند که داده های فیزیکی را به سیگنالهای الکتریکی مانند جریان یا ولتاژ تبدیل می‌کند. سپس، این سیگنالهای الکتریکی به داده‌های باینری تبدیل می‌شوند. داده‌های باینری به سادگی توسط نرم افزار تحلیل و در حافظه سخت PC یا در جاهای دیگری نظیر کارتهای حافظه و CD ها ذخیره می شوند.

شکل۳: ثبت کننده داده

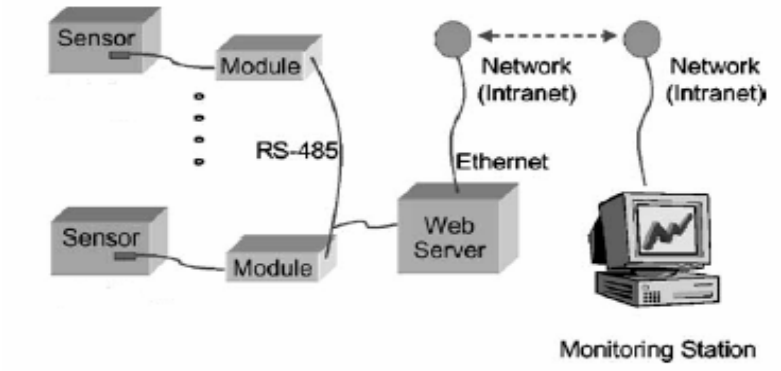


شکل٤: چگونگی کارکرد یک ثبت کننده داده

گام سوم: اجرای کنترل و نظارت به صورت زمان حقیقی برای فرآیند امنیتی موجود.

در این مرحله مراکز مورد نظر مجهز به یک دستگاه کامپیوتر دارای یک کارت DAQ ، یک عدد Web-Cam و یک خط اتصال دایم به شبکه کامپیوتر مورد نظر [برای مثال یک خط ADSL] می‌شوند و امکان ارتباط سیستم با سیستم ضد سرقت Localدر صورت تمایل وجود دارد. بدین ترتیب که سیگنالهای هشدار سیستم Local از طریق کارت DAQ قابل دریافت توسط کامپیوتر مرکز حساس مورد نظر خواهد بود. همچنین، امکان ارتباط مستقیم حسگرهای ویژه امنیتی از طریق Module های طراحی شده مناسب نیز وجود دارد[۴].

در این روش کلیه اطلاعات مرکز بی درنگ بر روی کامپیوتر مرکز ذخیره می‌شود. این کامپیوتر نقش یک Data-Base را برای سایر کامپیوترهای متصل از طریق شبکه دارد.



شکل۵: نحوه اتصال سیستم های امنیتی مرکز حساس به شبکه

گام چهارم: ایجاد یک Interface مناسب در محیط نرم افزار برای اجرای عملیات کنترلی و نظارتی:

در این مرحله یک interface مناسب در محیط نرم افزار برای اجرای عملیات مذکور طراحی می‌شود. به کار بردن سیگنال‌های کنترل زمان حقیقی امری مهم در طراحی سیستم‌های کنترل از راه دور است. این نیاز روشهایی برای فرستادن و دریافت داده را که با سخت افزار و نرم افزارهای مخصوص به خود صورت می‌گیرد گسترش می‌دهد. روشهای زیادی وجود دارد که یک plat form را برای کاربردهای زمان حقیقی معرفی می‌کند. یکی از پر کاربردترین و بهترین آنها در این زمینه Data Acquisition (DAQ) است که روشی برای دسترسی و کنترل اطلاعات یا داده‌ها برای کنترل تجهیزات و مانیتور کردن آنهاست و دقت آنها به قدری زیاد است که ذرات بسیار ریز مانند الکترون آزاد بیم های لیزر را هم می تواند به خوبی نشان دهد. برای کاربردهای مختلف روشهای مختلفی وجود دارد که سیگنالها را به طور Online برای یک فرایند حقیقی مهیا می‌کند که از آن جمله می‌توان روشهای زیر را نام برد:

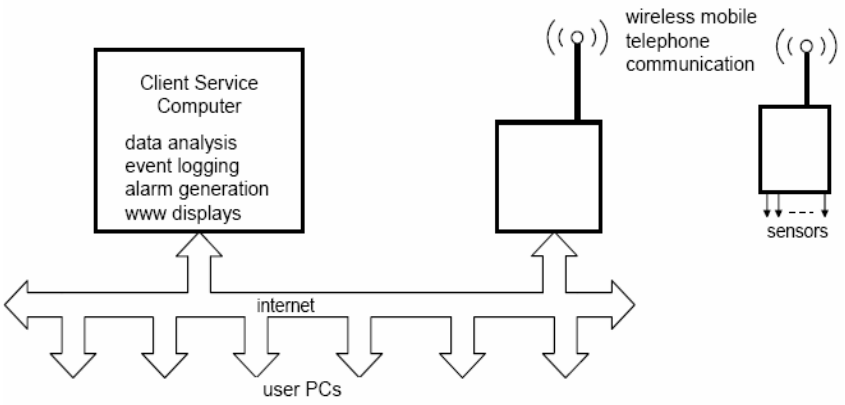
- Visual C++ که داده ها را به پورتهای سریال یا موازی PC می‌فرستد یا دریافت می‌کند و از A/D و D/A نیز استفاده می‌کند.

- نرم افزار LABVIEW که داده‌ها را از یک کارت ورودی / خروجی دریافت می‌کند.
- جعبه ابزار MATLAB Data Acquisition (DAQ) که یک رابطه متقابل با PC برقرار می‌کند .
- جعبه ابزار MATLAB Data Acquisition (DAQ) که از ریا Real Target Windows(RTW) استفاده می‌کند.

با مقایسه موارد یاد شده با یکدیگر به این نتیجه می‌رسیم که در روش اول به برنامه نویسی زیاد و چندین کامپایلر نیاز است. روش دوم دارای دقت زیادی است و پیاده‌سازی طرح ارائه شده در این مقاله نیز بر این مبنا بوده است. روش سوم برای سیگنالهایی که رنج نمونه برداری آنها در فرکانس audio است (از ۸ KHZ تا KHZ ۴۴) مورد استفاده قرار می‌گیرد و برای سیگنالهای فرکانس پایین و سیستم‌های دینامیکی که تقریباً شبیه DC است، مفید نخواهد بود. روش چهارم هم با توجه به کاربرد گسترده نرم افزار MATLAB در دانشگاه و صنعت بسیار مورد استفاده قرار می‌گیرد.

در این پروژه از روش دوم؛ یعنی نرم افزار LABVIEW استفاده شده و طراحی سیستم امنیتی و کنترل و نظارت زمان حقیقی واحد حفاظتی توسط این نرم افزار و استفاده از کارت DAQ صورت گرفته است. Labview تحولی اساسی و نوین در شیوه زبانهای برنامه‌نویسی است. با به وجود آمدن Labview مفهوم برنامه‌نویسی گرافیکی شکل تازه‌ای به خود گرفت و برنامه نویسانLabview بدون نوشتن هیچ کدی برنامه‌های توانمندی را فقط با استفاده از ابزارهای گرافیکی ایجاد کردند. شباهت بسیار زیاد محیط برنامه نویسی Labview با جهان واقعی باعث شده است تا همه کسانی که باLabview آشنا می‌شوند آن را بر سایر زبانهای برنامه نویسی برای ایجاد برنامه-هایشان ترجیح دهند. Labview تنها برای کاربردهای پردازش داده و کنترل تجهیزات استفاده نمی‌شود، بلکه برای کاربردهای همه منظوره مانند پایگاه داده، برنامه‌های آنالیز داده، برنامه‌های ارتباط شبکه یا حتی یک برنامه بازی ساده به کار

می‌رود. Labview همچنین، ابزارهای اضافی متنوعی برای تمام کاربردهای مخصوص کاربر مانند پردازش تصویر، پردازش سیگنال دیجیتال، آنالیز داده، کاربردهای اینترنتی و ... دارد. ویژگی دیگر آن در مقایسه با سایر سیستم‌های امنیتی از راه دور امکان ارسال اطلاعات مرکز مورد نظر به چندین مرکز مجاز بدون نگرانی از مکان فیزیکی آنهاست [مرکز کنترل امنیت می‌تواند در هر جای جهان واقع شود] برای ایجاد این ارتباط‌های جدید به صرف هزینه مجدد نیازی نیست.



شکل٦: توپولوژی سیستم های امنیتی از راه دور مبتنی بر اینترنت

۳. مزیت سیستم های Web Based نسبت به سایر سیستم های امنیتی از راه دور

استفاده از روش Web Based Control [۱۱] امکان استفاده آسان‌تری را از سیستم امنیتی از راه دور به ما می‌دهد، چرا که کاربر ما در هر کجا که باشد فقط با داشتن یک جستجوگر web قادر به اتصال به سیستم امنیتی از راه دور ما خواهد بود. بدیهی است که این گونه سیستم ها نیز دارای معایب خاص خود همچون مشکل امنیت و کمبود سرعت در بعضی موارد ویژه هستند که راهکارهایی برای رفع این مشکلات وجود دارد[۱۲].

٤. نقش استفاده از VPNدر ارتقای سیستم های امنیتی از راه دور مبتنی بر شبکه

VPN در یک تعریف کوتاه شبکه‌ای از مدارهای مجازی برای انتقال ترافیک شخصی است. در واقع، پیاده‌سازی شبکه خصوصی یک شرکت یا سازمان را روی یک شبکه عمومی VPN گویند.

VPN به کمک رمز گذاری روی داده ها درون ِیک شبکه بزرگ همه منظوره مانند Internet یک شبکه کوچک می سازد و فقط کسی که آدرس‌های لازم و رمز عبور را در اختیار داشته باشد می‌تواند به این شبکه وارد شود. مدیران شبکه ای که بیش از اندازه وسواس دارند و محتاط هستند می توانند VPN را حتی روی شبکه محلی هم پیاده کنند. اگر چه نفوذ کنندگان می‌توانند به کمک برنامه های Packet snifter جریان داده‌ها را دنبال کنند، اما بدون داشتن کلید رمز نمی توانند آنها را بخوانند[۱۳].
استفاده از VPN برای یک سازمان دارای مزایای متعددی به قرار زیر است:

- VPN نسبت به شبکه‌های پیاده‌سازی شده با خطوط استیجاری، در پیاده‌سازی و استفاده، هزینه کمتری صرف می‌کند. اضافه وکم کردن گره‌ها یا شبکه‌های محلی به VPN، به دلیل ساختار آن با هزینه کمتری امکان‌پذیر است. در صورت نیاز به تغییر همبندی شبکه خصوصی، نیازی به راه‌اندازی مجدد فیزیکی شبکه نیست و به صورت نرم‌افزاری، همبندی شبکه قابل تغییر است.
- گسترش محدوه جغرافیایی ارتباطی
- بهبود وضعیت امنیت
- کاهش هزینه های عملیاتی در مقایسه با روشهای سنتی نظیر WAN
- کاهش زمان ارسال و حمل اطلاعات برای کاربران از راه دور
- بهبود بهره‌وری
- توپولوژی آسان

۵. صرفه اقتصادی سیستم‌های امنیتی از راه دور مبتنی بر شبکه

طبعاً هزینه این طرح به دلیل نبود نیاز به قطعات سخت افزاری گرانقیمت بسیار پایین است. تنها ادوات مورد نیاز، کامپیوتر متصل به شبکه، یک کارت DAQ و یک خط ADSL است.

شایان ذکر است که سیستم اعلان حریق یا دزدگیر از قبل در مکان مورد نظر نصب شده است و سیستم پیشنهادی نیاز به حسگرهای جدید ندارد و با سیستم پیشین سازگار است. علت دیگر صرفه اقتصادی سیستم این است که به کانال مخابراتی جدید برای سیستم امنیتی از راه دور و هزینه‌های سنگین لازم برای طراحی و پیاده سازی کانال نیازی نیست. [استفاده از طیف فرکانسیس آزاد بر روی خطوط تلفن، در روش ADSLیا بر روی خطوط برق، در روش PLC].

بنابراین صرفه اقتصادی سیستم پیشنهادی از مزایای اصلی نسبت به سایر روش‌های پیشین است.

٦. مقایسه سیستم پیشنهادی مبتنی بر شبکه با سایر سیستم های امنیتی از راه دور

بسته به نوع رسانه انتقال داده‌ها، نحوه دسترسی کاربر یا کاربران و برد سیستم امنیتی از راه دور متفاوت است. بیشتر طرحهای امنیت از راه دور مبتنی بر شبکه های تلفنی، [مانند: PSTN]، خطوط تلفن داخلی PABX یا شبکه تلفن همراه (GSM) به عنوان رسانه انتقال داده‌ها هستند[۲]. برای مثال، سیستم‌های متداول امنیتی منازل مسکونی در کشور آمریکا برای مخابره وضعیت به مرکز پلیس(Security Station911) از شبکه تلفنی شهری (PSTN) استفاده می‌کنند. در این روش در زمانهای اضطراری وضعیت از طریق یک Modem به صورت اتوماتیک به مرکز مسئول مخابره می‌شود. به ازای هر خط تلفن به دلیل ماهیت شبکه‌های مخابراتی، در یک لحظه تنها امکان برقراری ارتباط با یک مرکز مسئول وجود دارد. ارتباط های چند گانه نیازمند استفاده همزمان و موازی از چندین خط تلفن است. برد این گونه سیستم ها به برد شبکه تلفنی مورد

نظر محدود است و بنابراین، استفاده از آنها تنها در سطح داخلی یک منطقه یا کشور معقول است.

ویژگی اصلی مبتنی بر شبکه در مقایسه با سایر سیستم های امنیتی از راه دور امکان ارسال اطلاعات مرکز حساس مورد نظر به چندین مرکز مجاز بدون نگرانی از مکان فیزیکی آنهاست.[مرکز کنترل امنیت می‌تواند در هر جای جهان واقع شود]. برای ایجاد این ارتباط های جدید به صرف هزینه مجدد نیاز نیست. به طور خلاصه این روش پیشنهادی در مقایسه با سایر روشهای پیشین دارای ویژگی های ذیر است:

۱. در هر زمان می‌توان با ایجاد یک ارتباط Real Time با Server مرکز حساس مورد نظر از وضعیتهای مختلف سیستم امنیت آن مانند سیگنالهای هشدار، تصویر و ... به صورت دستی Manual مطلع شد.

۲. در مواقع اضطراری این سیستم دارای قابلیت اعلام وضعیت خود به طور کاملاً اتوماتیک به مراکز مسئول مجاز مانند پلیس ۱۱۰ است.

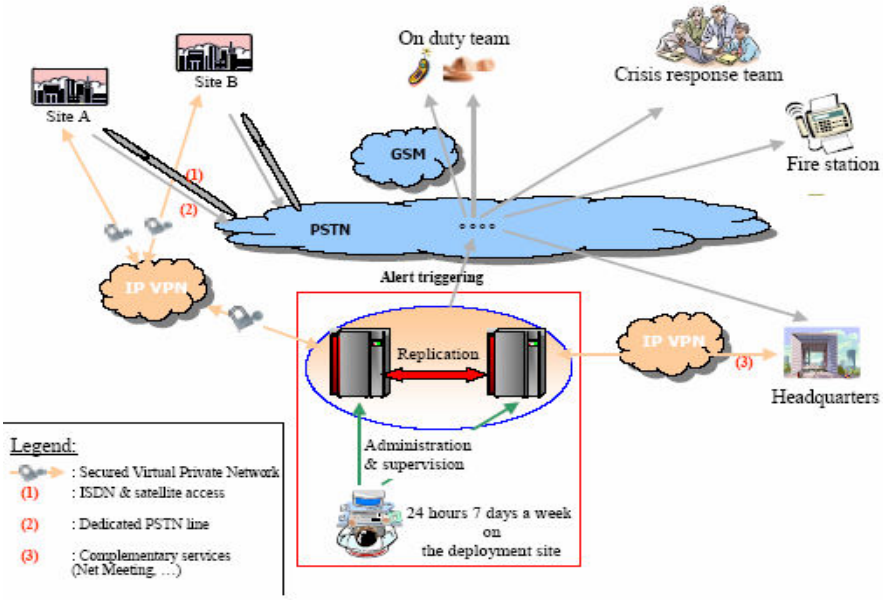
۳. با توجه به استفاده از طیف فرکانسیس آزاد بر روی خطوط تلفن [در روش ADSL] یا بر روی خطوط برق [در روش power line carrier PLC] مقادیر زیادی در هزینه سیستم و هزینه کانال مخابراتی نسبت به روشهای سابق صرفه جویی می‌شود. پیچیدگی مدارهای کنترلردر روشهای پیشین از دیگر معایب آنهاست.

۴. تلفیق سیستم های امنیت از راه دور، مبتنی بر شبکه های تلفنی[1] و مبتنی بر شبکه های کامپیوتری[2]، می‌تواند تأثیر بسزایی در کارایی و کیفیت سرویس[3] این گونه سیستم ها داشته باشد[۲و۳]. در این راهکار سیستم مبتنی بر شبکه کامپیوتر به عنوان پشتیبان و کامل کننده نواقص سیستم دیگر عمل می‌کند. سیستم مبتنی بر شبکه تلفنی قابلیت اطمینان سیستم امنیت از راه دور مورد نظر را، در مواقعی که سیستم مبتنی بر شبکه کامپیوتر درگیر مسائلی خاص می شود، بالا می برد. برد سیستم

---

1 . Telephone-Based Remote Security Systems
2 . Computer Network-Based Remote Security System
3 . QoS Quality of Service

تلفیقی به دلیل بهره برداری از برد هر دو شبکه تلفنی و مخابراتی به میزان چشمگیری افزایش می یابد. یک نمونه ساختار شبکه تلفیقی و توپولوژی اتصال در شکل ۷ مشاهده می شود.



شکل ۷: ساختار شبکه تلفیقی امنیت از راه دور

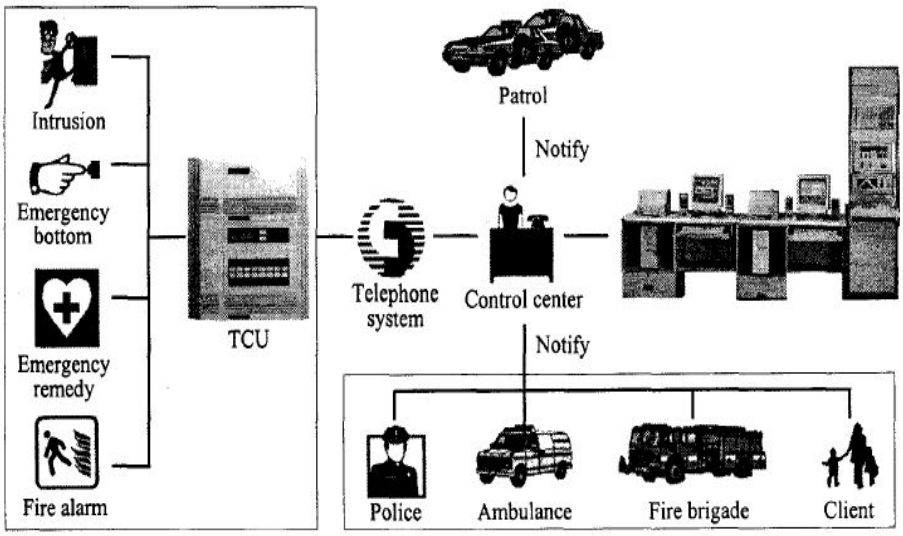
۵. در این روش در صورت همکاری پلیس می توان در مراکز آنها یک Database مرکزی برای کلیه مراکز حساس مورد کنترل در منطقه گذاشت[۷]. اداره پلیس امکان نظارت بر مرکز مورد نظر در هر زمان را دارا خواهد بود و علاوه بر این، در مواقع اضطراری، با دریافت پیامهای هشدار از طرف مکان مورد نظر قادر به اعزام نیروهای خود به محل شوند.

۶. به دلیل بنا شدن این سیستم بر شبکه های کامپیوتر، امکان اتصال کلیه مراکز پلیس یک کشور وجود دارد، بدین معنا که اطلاعات مرکز پلیس محلی قابل دسترس

برای سایر مرکز پلیس خواهد بود. در واقع، مرکز پلیس محلی یک Server داده‌های وضعیت مناطق حساس براساس سایر مراکز پلیس خواهد بود.

۷. امکان اتصال به سایر سیستم های یک مرکز حساس مانند: سیستم اعلان حریق و ... به سیستم برای ارسال به مراکز کنترل مربوط وجود دارد.

۸. این سیستم امنیتی تحت شبکه های کامپیوتر می تواند به عنوان یک سیستم امنیتی چند منظوره هوشمند مورد استفاده واقع شود[۱۶]. این سیستم، همان طور که در شکل نشان داده شده است، از اجزای پیشرفته‌ای مانند Card reader،TCU، پایانه، صفحه کلید، Sensor و غیره تشکیل شده است.در کنار سایر سیستم‌های قدیمی مانند ضد سرقت، اعلان حریق و کنترل دسترسی، مرکز کنترل می‌تواند از سیستم های دیگری همچون خدمات شخص بیمار از راه دور، ثبت اتوماتیک کنتور گاز از راه دور، خدمات بانکی، ارائه internet و سایر خدمات رفاهی و امنیتی پشتیبانی کند.



شکل ۸: معماری سیستم امنیتی چند منظوره هوشمند

۷. ویژگیهای سیستم های امنیتی از راه دور مبتنِی بر شبکه [۸ و ۹]

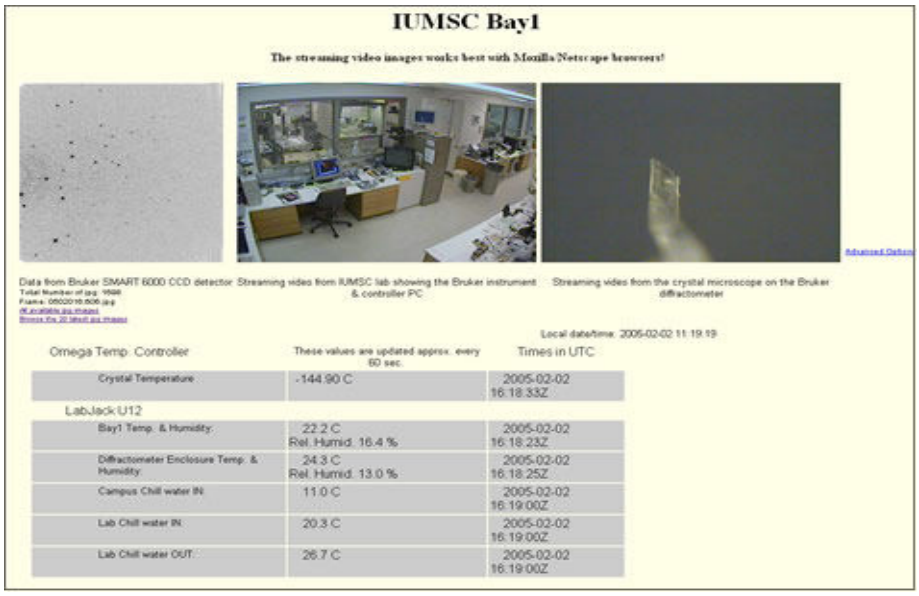
- قابلیت استفاده در کلیه سیستم‌های امنیتی از راه دور از هر نقطه جهان بدون در نظرگرفتن بعد مسافت؛
- امکان احراز هوِیت کاربران متفاوت سِیستم و اختصاص سطوح دسترسی متفاوت به آنها؛
- قابلیت سازگاری با سایِر سیستمهای امنیتی نصب شده بر کلیه مراکز تجاری و بانکها بدون نیاز به اِیجاد تغییر در آنها یا نصب ادوات سخت افزاری مضاعف؛
- امکان نصب به صورت موازی با سایر سیستمهای پیشین؛
- نصب آسان؛
- طرز کار آسان؛
- هزینه پایین.

۸. پیاده سازی

برای پیاده سازی عملی یک سیستم امنیتی از راه دور مبتنی بر شبکه کامپیوتر، شبکه اینترنت به عنوان شبکه کامپیوتر به دلیل وسعت استفاده عمومی انتخاب شده است. در صورت نصب دوربین های امنیتی در مکان حفاظتی، سیستم قابلیت دریافت تصاویر و پردازش بر روی آنها برای ارسال را داراست. تصاویر ارسالی دوربین قابل مشاهده از طریق شبکه است[۵ و۶]. سیستم می‌تواند به نحوی طراحی شود که قابلیت تشخیص حرکت در تصویر را با استفاده از روشهای DIP دارا باشد. بدین صورت، تغییر در تصویر و تشخیص حرکت به منزله ورود شخص غیر مجاز به محوطه حساس تلقی می‌شود و وضعیت بحرانی مذکور بی درنگ (Real-Time) اعلام می شود. یک دستگاه دوربین تحت شبکه (Network Camera) به عنوان سیستم جمع آوری اطلاعات امنیتی انتخاب شده است.

شکل ۹ : Network Camera AXIS 206

دلیل این انتخاب این بوده است که دوربین یکی از بهترین حسگرهای امنیتی است و با استفاده از روش پردازش تصاویر (Digital Image Processing DIP) تقریباً امکان تشخیص هر نوع وضعیت اضطراری و امنیتی وجود دارد.



شکل۱۰: مشاهده تصاویر ارسالی دوربین

سیستم پیاده سازی شده به نحوی طراحی شده است که قابلیت تشخیص حرکت در تصویر را با استفاده از روشهای DIP دارا باشد. بدین صورت، تغییر در تصویر و تشخیص حرکت به منزله ورود شخص غیر مجاز به محوطه حساس تلقی می‌شود که وضعیت بحرانی مذکور بی‌درنگ (Real-Time) اعلام می شود.

۹. نتیجه‌گیری

با توجه به اینکه مسئله امنیت، نظارت و حفاظت اماکن حساس مانند بانکها و مراکز تجاری همواره از مسائل مهم و عمده روز به شمار می‌رود، لزوم داشتن یک سیستم امنیتی یکپارچه مرکزی ما را بر آن داشت تا در این مقاله ضمن بررسی سایر روشهای پیشین به پیشنهاد و توسعه این روشها در خصوص امنیت، نظارت و حفاظت مراکز حساس تجاری از راه دور تحت شبکه های کامپیوتری بپردازیم. این نوع سیستم ها علاوه بر صرفه اقتصادی، دارای مزایای زیادی همچون امکان کنترل سیستم امنیتی از راه دور از هر نقطه جهان بدون در نظرگرفتن بعد مسافت و ... هستند که به آن اشاره شد.

تلفیق سیستم های امنیت از راه دور، مبتنی بر شبکه های تلفنی (Telephone-Based Remote Security Systems) و مبتنی بر شبکه های کامپیوتری می تواند تأثیر بسزایی در کارایی و کیفیت سرویس(QoS Quality of Service) این گونه سیستم ها داشته باشد.

مراجع

1. G. Cybenko and G. Jiangi, "Developing a Distributed System for Infrastructure Protection"; **IEEE IT PRO Magazine** (July | August 2000).
2. L. Carlier, L. Dhaleine, P. Genestier, C. Lac and B. Savina; **Emergency and Rescue: Methodology and Tool for Alert Activation and Crisis Managemen**, Critical Infrastructure Protection (CIP) Workshop (Frankfurt a.M., 29-30 Sept. 2003).
3. G. Jiang, G. Cybenko and D. McGrath, "Infrastructure web**:** Distributed Monitoring and Managing Critical Infrastructures"; Infrastructure Protection and Emergency Management (IPEM) Symposium, 2000.
4. J. M. Hale, "Structural Monitoring for Rare Events in Remote Locations", **Institute of Physics, Journal of Physics**: Conference, Series 15 (2005) 113–118 Sensors & their Applications XIII.
5. S. Lei, J. Haslett, and M. Smith, "A Prototype Internet-Based Security System"; **Circuit Cellar the Magazine for Computer Applications** (August 1999).

6. J. C. Bolot and T. Turletti;"A Rate Control Scheme for Packet Video in the Internet," **Proceedings of IEEE Infocom,** pp.1216-1223.ftp://ftp-p.inria.fr/rodeo/bolot/94. Video_control. ps.gz. 1994.
7. A. Elgamal, F. Seible, F. Vernon, M. Trivedi and M. Fraser, "On-Line Structural Monitoring and Data Management"**; Proceedings 6th Seismic Research Workshop**, California Department of Transportation, Sacramento, California, June 12-13,2001.

۸. حسین مهربان جهرمی، "معرفی پارامترهای مـؤثر در ارزیـابی سیسـتم هـای عملیـات از راه دور"؛ **فصلنامه آموزش مهندسی ایران**، شماره ۳۶، سال نهم، ۱۳۸۶.
۹. ابوالقاسم دائی چیان، "کاربرد فناوری اطلاعات در امنیت سیستم های کنترل صنعتی"؛ **فصـلنامه آموزش مهندسی ایران**، شماره ۳۲، سال هشتم، ۱۳۸۵.
۱۰. فریدون شعبانی‌نیا، "نقـش اینترنـت در آزمایشـگاه هـای آموزشـی وتحقیقـاتی دانشـکده هـای مهندسی"؛ **فصلنامه آموزش مهندسی ایران**، شماره ۳۰، سال هشتم، ۱۳۸۵.

11. D. I. Shin, S. J. Huh, T. S. Lee and I.Y. Kim, "Web-based Remote Monitoring of Infant Incubators in the ICU"; **International Journal of Medical Informatics** (2003).
12. C. D. Knight and S. P. DeWeerth, World Wide Web-based Automatic Testing of Analog Circuits; in Proc. 1996 Midwest Symp, Circuits and Systems, Ames, IA, 1996, pp. 295-298, 1996.
13.(on-line) http://www.microsoft.com/windowsserver2003/technologies/networking/vpn/default.mspx
14. L. Lauterbach, and L. H. Wise, "Altering and Warning System"; **United States Patent**, Feb. 1992.
15. I. Conkun and H. Adram, "A Remote Controller for Home and Office Appliances by telephone"; **IEEE Transactions and Consumer Electronic**, Vol. 44, No. 4, November 1998.
16. A. R. Al-Ali and M. AL-Rousan," Java-Based Home Automation System"; **IEEE Transactions on Consumer Electronics**, Vol. 50, No. 2, May. 2004.
17. W. Brian Pinzon"; Door Locking/unlocking System Utilizing Direct and Network Communication"; **US PATENT,** Aug. 1998.

18. P. C. Yang etc., “APX-Home Security System”; **Aecl Enterprise**, Inc., Taipei Taiwan R.O.C 1994.
19. Sin-Min Tsai, Po-Ching Yang, Shyi-Shioui Wu, Shya-Shiow Sun, “ A Service of Home Security System on Intelligent Netwrok”; **IEEE Transactions and Consumer Electronic**, Vol. 44, No. 4, November 1998.

(تاریخ دریافت مقاله: ۲ /۱۲/۱۳۸۵)
(تاریخ پذیرش مقاله: ۱۳۸۶/۸/۹)