بُـسـت

علمي او څېړنيزه مجله

ټوک	ګڼه	کال
دوهم	لومړی	۱۴۰۲

بسم الله الرحمن الرحیم

بُست علمي او څېړنيزه مجله

بُست پوهنتون

دوهم ټوک – لومړی ګڼه

کال – ۱۴۰۲

بُست علمی او څېړنیزه مجله

بُست پوهنتون

د امتیاز خاوند: بُست پوهنتون

مسؤل مدیر: پوهنمل دوکتور ناصر ضیا ناصری

کتنپلاوی:

⇐ پوهندوی رضوان الله مملوال
⇐ پوهنمل عبدالعزیز صابر
⇐ پوهنمل عبدالولي هجران
⇐ پوهنمل حنیف الله باوري
⇐ پوهنیار عبدالولی همت
⇐ پوهنیار بشیر احمد بابا زوی
⇐ خان محمد وفا
⇐ ډاکتر ذبیح الله انوری

⇐ پوهنوال دوکتور احمد جاوید پویش
⇐ پوهنوال دوکتور خال محمد احمدزی
⇐ پوهندوی دوکتور غلام رسول فضلي
⇐ پوهندوی دوکتور علی احمد
⇐ پوهنمل دوکتور عبدالوهاب حکمت
⇐ پوهنمل دوکتور ناصر ضیا ناصري
⇐ پوهندوی نیاز محمد زاهدي

ډیزاین: د بُست پوهنتون دخېرنیزو او فرهنګي چارو مدیریت

د خپرولو کال: ۱۴۰۲

پته: بُست پوهنتون، لښکرګاه،هلمند، افغانستان

د بُست پوهنتون د رئیس پیغام

په نني ژوند کې د یوې علمي مؤسسې یو له مسؤلیتونو څخه دا دی ، چې نه یواځې خپل محصلان د پوهې په ګاڼه سمبال کړي، بلکې د پوهنتون د لوړو زده کړو لرونکو پوهانو او استادانو د علمي زیرمتون څخه داسي څه وخت په وخت راوباسي، چې د ټولنې د ژوند د اړتیاوو د پوره کولو لپاره او یا لږ تر لږه د ټولنې د لوستي قشر د خبرولو او که وکولای شي له هغوی څخه د عمل په ډګر کې د ګټې اخیستنې په موخه ، په کار واچول شي.

و دې موخې ته د رسیدلو لپاره پوهنتون باید یو داسې علمي خپرندویه ارګان ولري، چې په هغه کې د پوهنتون ټول با صلاحیته منسوبین که هغه استاد وي، که کارکوونکی او که زده کړه یال ، خپلې علمي او څیړنیزي مقالې او لیکنې د کاغذ پر مخ باندې کښیښودلای شي.

زما په شخصي آند پدې مجله کې لکه له نوم څخه چې یې ښکاري، باید داسي مسائل را برسیره شي، چې نه یواځې په پوهنتون پورې راګیر پاتې شي، بلکې په عام ډول سره د افغاني ټولنې او په ځانګړي ډول سره د هلمند ولایت د اوسیدونکو و نني او سبا ژوند ته په کتلو سره، بریالیتونونه، ستونزي ، وړاندیزونه او د حل لارې-چارې ، وړاندې کړل شي.هغه وخت به د بُست پوهنتون علمي مجله یواځې د بست پوهنتون نه، بلکې د ټول هلمند ولایت ، آن د سیمي او ټول افغانستان په کچه د پوهې او څیړنې په برخه کې د وخت د غوښتنو سره سم ، د پاملرنې وړ او ځوان نسل ته د یوې سمې لارې د ښودلو په موخه ، یوه محبوبه او پر زیاتو خلکو باندې ګرانه مجله وي او په ټول هیواد کې به خپل مینه وال ولري.

دا مجله به د بُست پوهنتون د مشرتابه، استادانو ، محصلانو ، فارغانو او ټولو مینه د علمي او څیړنیزو مقالو د خپرولو لپاره که هغوی د پوهې په هر ډګر کې چې وي، یو خپرنیز ارګان وي،چې و خپریدلو ته به یې ټول مینه وال په تمه ناست وي.ځومره به پرځای او ښه خبر وي، چې د ټولنې لوستی قشر په تیره بیا د بست پوهنتون محترم استادان ، فارغ شوي او بر حاله محصلان د علمي او څیړنیزو مقالو و لیکلو ته و هڅول شي.

زه د بُست پوهنتون د ټولو منسوبینو په استازیتوب ویاړ لرم ، چې د بُست پوهنتون د علمې مجلې د خپریدلو له امله د محترم مؤسس، محترم علمي مرستیال او د څیړنې له محترم آمر او همدا رنګه د مجلې له ټولو کارکوونکو او پرسونل څخه د زیار او زحمت په ګاللو سره چې مجله یې و خپریدلو ته چمتو کړې ده ، مننه او قدرداني وکړم، ټولو ته د زړه له کومې مبارکي وایم او هیله لرم چې د بُست پوهنتون د علمي مجلې کارکوونکي به خپل رسالت د پوهنتون او ټول هلمندې ولس او په اخرې تحلیل کې د ټول افغان ملت پر وړاندې په پوره او ټینګ عزم سره سرته ورسوي.

په درنښت

ډیپلوم انجنیر محمود سنګین

د بُست پوهنتون رئیس

سریزه

بُست پوهنتون ویاړ لري چې د خپل علمي پرمختګ په لاره کې يې يو بل ډېر مهم او اړين ګام پورته کړ او هغه د بُست د علمي او څېړنيزي مجلې د دوهم ټوک، لومړی ګڼه خپرېدل دي . تر هر څه دمخه د پوهنتون ټولو استادانو، محصلانو او د علم او پوهې د لوی کور مینه والو ته د بُست د علمي او څېړنيزي مجلې د خپرېدلو مبارکي وړاندې کوم او ددې سره جوخت د ټولو ملګرو څخه چې ددې مجلې د جواز په تر لاسه کولو، ترتيبولو او خپرولو کې يې نه ستړې کېدونکې ونډه اخيستې ده د زړه له کومي مننه کوم.

د علمي کور کهول او اړوند کسانو ته ښکاره ده او پوره باور لري چې د نننۍ نړۍ هر اړخيزه پر مختګ د پوهانو د علمي څېړنو د زيار له برکته ممکن سوی او د لوړو زده کړو مؤسسي، اکادميک انستيتوتونه او څېړنيز علمي مرکزونه پکښې مرکزي او پريکنده رول لوبولی دی.

همدې اصل او ارزښت ته په کتو سره بُست پوهنتون غواړي د پرمختللو اکاډميکو نورمونو په رعايت د تدريس، علميڅېړنو او نوښتونو له لاري مسلکي کادرونه وروزي او د معياري تحصيلي اسانتياوو او زمينو په برابرولو سره د ټولنې ځوانانو ته معياري او د لوړ کيفيت لوړې زده کړي وړاندی او د علميڅېړنو پر بنسټ د کره پوهنيزو اثارو د توليد زمينه برابره کړي ، ترڅو د لوړو زده کړو او مسلکي پوهې په ډګر کې د ګټورو مهارتونو په تر لاسه کولو او د خپلو رښتينو اهدافو په لاسته راوړلو سره د ټولنې او هيواد په پرمختګ او رغونه کې رغنده ونډه واخلي او د رښتيني خدمت جوګه شي.

ژمن يو چې د هلمند ولايت، ګاونډيو ولايتونو او په ټول هيواد کي ځوان نسل ته د اسلامي ، ملي او کلتوري ارزښتونو په رڼا کي معياري د علمي او مسلکي لوړو زده کړو او پراخو علمي څېړونو زمينه برابره او ټولني او هيواد ته ژمن او روزل سوي کادرونه وړاندي کړو.

د اوس لپاره د بُست علمي او څېړنيزه مجله يوازي د **سائينسي علومو** په برخه کې علمي او څېړنيزي مقالي او ليکني د چاپ او نشر د تګلارې سره سم مني او خپروي او هيله مند يو چې په راتلونکې کي به نوري برخي هم ور زياتي کړل سي.

ډاډ لرم چې د بُست پوهنتون استادان، محصلان او علمي کارمندان به انشأالله، نن، سبا او په راتلونکې کې د خپلي علمي څېړنيزي مجلې د خپرولو له لاری خپل دغه درونډ خو وياړلی دين (پور) ادأ کړي. همدا ډول ټولو د علم او پوهي څښتنانو او مينه والو ته په مينه سره بلنه ورکوو چي ددی علمي او څېړنيزي مجلي او د بُست پوهنتون د پرمختګ په لاره کي خپلي علمي او څېړنيزي ليکني، آندونه، وړانديزونه او رغنده نيوکي او مرستي د تل په شان راولوروی او د علم ددي ستر کور په ودانولو کي د خپلي ديني، او ملي برخي د اداينې وياړ راوبخښی.

موږ هوډ کړيدي او هيله مند يو چي انشآ الله د وخت په تيريدو سره به د خپل هيواد و بچيانو او ځوان نسل ته د تدريس ، ښه روزني او څېړنيز هاند لپاره اړيني او د پام وړاسانتياوي برابري کړو تر څو په لومړي پړاو کښي خپلو هلمندوالو بيا د سهيل لويديځي حوزي او په پاي کښي و ټولو هيوادوالو ته د يو داسي چوپړ مصدر وګرځي چي زموږ د ځوريدلي اولس او ويجاړشوي هيواد اقتصادي، فرهنګي، سياسي او ټولنيزي ستونزي حل او افغانستان د نړي د پرمختللوهيوادونو په ليکه کي ودريږي.

لړلیک

د مقالی عنوان	د صفحی شمیره
د کندهار په میرویس حوزوي روغتون کي د Sub Mucosal Resection واقعاتو څېړنه ډاکټر زلمی عالمي، ډاکټر ذبیح الله انوري ، ډاکټر سید بسم الله سجادي	۱
د کندهار په میرویس حوزوي روغتون کي په معدوي زخمونوکي د هضمي جهاز د پورتنۍ برخي د وینه بهیدني واقعاتو مطالعه ډاکټر نصرالله نصرت، ډاکټر ذبیح الله انوري، ډاکټر سید بسم الله سجادي	۲
په نوزاد ولسوالۍ کي د انارو د تولید لګښت، ناخالصي ګټي، خالصي ګټي او مارکیټینګ چینلونو اقتصادي تحلیل پوهنیار زمریالی ټنی، پوهندوی ډاکټر علي احمد، حمید الله هدایت	۳
د جوارو پر حاصل او د حاصل پر مرستندویه برخو باندي د پوټاشیم اغیزي پوهنمل محمدیار ملکزی، پوهنیار زمریالی ټنی	۴
د ټولني په سوله او ثبات کي د کرني رول پوهنمل محمد یار ملکزی، پوهنیار زمریالی ټنی	۶
RAINFALL-RUNOFF MODELING OF ARGHANDAB RIVER BASIN IN AFGHANISTAN ABDUL WALI HEJRAN AND ESMATULLAH SANGIN	۷
د DYNAMIC ROUTING پروټوکول عملیاتو ته کتنه محمد ادریس وزیری، خان محمد وفا، جماالدین جمال	۸
د IP ADDRESS په اساس د سیستم د څارني پلي کیدنه خان محمد وفا، جماالدین جمال، سید محمد عادل	۹
د INTERNET PROTOCOL ADDRESS پیژندنه او د هغه پلي کیدنه خان محمد وفا، جماالدین جمال،سید محمد عادل	۱۰
پر کاروربار باندي د معلوماتي تیکنالوژۍ اغیزي ارسلان وطندار ، پوهندوی دوکتور علی احمد، محیب الله امیني	۱۱

د IP address په اساس د سیستم د څارني پلي کیدنه

خان محمد وفا[1]، جماالدین جمال[2]، سید محمد عادل[3]

[1,2,3]معلوماتي ټکنالوژۍ څانګه، کمپیوټر ساینس پوهنځی، بُست پوهنتون

د مسؤل ایمیل آدرس: Khan.jan363w@gmail.com

لنډیز

د Ip based monitoring system in network یو ډول امنیتي سیستم دی چې د انټرنیټ پروتوکول (IP) کاروي ترڅو په یو شبکه کې د مختلف امنیتي وسیلو ترمنځ ډیټا واستول سي ، نوکاروونکو ته د ریښتیني وخت نظارت او تعقیب وړتیا ورکوي. دا ډول سیستم عموما د استوګنیاو سوداګریزو ترتیباتو کې د ننوتلو او وتلو ځایونو، خوندي محیطونو، او نورو حساسو سیمو د څارني او تعقیب لپاره کارول کیږي. د Ip based monitoring system in network یوه لومړنۍ ګټه د لوړ کیفیت ویډیو فوټیج او عکسونو چمتو کولو وړتیا ده چې د انټرنیټ د وصلیدو سره د هرې وسیلې له لاري د لیري ځاي څخه لاسرسی ورته کیدی سي. که مالک د خپلي ودانۍ څخه لیري هم وي د دې سیستم په واسطه د ودانۍ دوامداره څارنه کولي سي د Ip based monitoring system in network بله ګټه اندازه کول دي. ډیری کیمرې او سینسرونه سیستم ته اضافه کیدی سي، او کله چي یو پیښه واقع سي نو هر وسیله کولی سي ټاکل سوي پرسونل ته خبرتیا واستوي، لکه سیستم ته غیرقانوني لاسرسی یا د سیستم د غړو د حرکت کشف. سربیره پردې د Ip based monitoring system in network اکثره د دودیز انلاګ سیستمونو په پرتله خورا ارزانه دي ځکه چي دا سیستمونه د موجوده انټرنیټ زیربنا کاروي او په اسانۍ سره د نورو امنیتي ټیکنالوژیو سره یوځای کیدای سي، لکه سیستمونو ته د لاسرسي کنټرول، د اور وژنې سیستم او د خطر په وخت کي د خبر ورکولو سیستم.

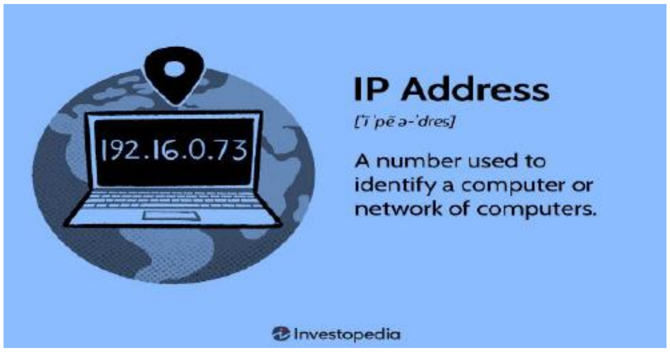
کلیدي کلمې: Monitoring, Internet protocol, network

سریزه

IP Adress د څلورو شمیرو یو سیټ دی. د مثال په توګه 192.158.1.38 یو IP Adress دی. د IP Adress په سیټ کې هره شمیره کېدای سي له 0 څخه تر 255 پوري وي. نو د بشپړ IP Adress رینج له 0.0.0.0 څخه تر 255.255 پوري دی. IP Adress د شمیرو یو string دی چې د پیریود لخوا جلا سوی وي.

IP Adress تصادفي نه دی. IP ادرسونه په ریاضیکي ډول د (Internet Assigned Number Authority (IANA د خوا جوړ او ځاي پر ځاي سوي (IANA) د
Internet Corporation for Assighned Names and (ICANN) Number یوه څانګه ده.

(ICANN): یوه غیر عایداتي موسسه ده چې په متحده ایالاتو کې په 1998 کې رامنځته سوه تر څو د انټرنیټ په security ساتلو کې مرسته وکړي او ټولو ته یې د کارولو وړ کړي. هر وخت چې یو څوک په انټرنیټ کې یو ډومین راجستر کوي، دوی د ډومین نوم یو راجستر کونکي سایټ ته ځي، چې هغه سایټ ICANN ته د ډومین راجستر کولو لپاره یوه اندازه فیس ورکوي(Bhatnagar and Kumar, 2016).



۱ شکل: IP Adress

IP ادرس څنګه کار کوي:

که تاسو غواړئ یوه سئ چې ولې یو کمپیوټر یا بل Device په هغه طریقه نه وصلیږي چې تاسو یې تمه لرئ یا تاسو غواړئ پوه سئ چې ولې ستاسو نیټورک کار نه کوي، نو یه IP ادرس پوهیدل ډېره مرسته درسره کوي.
د انټرنیټ پروتوکول د بلې هري ژبې په څیر کار کوي، د معلوماتو لیږدولو لپاره د ټاکل سوي لارښوونو په کارولو سره د خبرو اترو له لاري ټول Devices د نورو ټولو هغه Devices سره چې ورسره وصل دي معلومات لېږي، استوي او تبادله کوي. د ورته ژبې په ویلو سره په هر ځای کې هر کمپیوټر کولای سي له یو بل سره معلومات شریک کړي.
IP ادرس معمولا د پردې ترشا کار کوي. دا پروسه په لاندې ډول کار کوي:

1. ستاسو کمپیوټر په غیري مستقیم ډول د انټرنیټ سره وصلیږي په لومړي سر کې د انټرنیټ سره وصل نیټورک سره وصلیږي، چې بیا ستاسو کمپیوټر انټرنیټ ته لاسرسی پیدا کوي.
2. کله چې تاسو په کور کې یاست، دا Network به شاید ستاسو Internet service provider(ISP) وي. په کار یا دفتر کې به ستاسو د کمپنی نیټورک وي.
3. ستاسو IP ادرس ستاسو د ISP لخوا ستاسو کمپیوټر ته Assign یا ټاکل کیږي.
4. ستاسو د انټرنیټ فعالیت د ISP له لاري تیریږي او دوی دا ستاسو د IP ادرس په کارولو سره بیرته تاسو ته رسوي. څرنګه چې دوی تاسو ته انټرنیټ ته لاسرسی درکوي، دا د دوی رول دی چې ستاسو وسیله ته IP ادرس وټاکي.
5. ستاسو IP ادرس بدلیدلای سي. د مثال په توګه کله چې تاسو موډیم یا روټر فعال یا بند کړی دا کولای سي IP Adress بدل کړي. یا تاسو کولای سئ خپل د ISP سره اړیکه ونیسئ او دوی کولای سي ستاسو IP Adrress ستاسو لپاره بدل کړي.
6. کله چې تاسو د کور څخه بهر یاست - د بیلګې په توګه، سفر کوئ او ستاسو کمپیوټر ستاسو سره وي نو ستاسو د کور IP ادرس به ستاسو سره نه وي. دا ځکه چې تاسو به انټرنیټ ته د لاسرسي لپاره بل نیټورک (په هوټل، هوایي ډګر، یا کافي شاپ کې وائی فای او نور) کاروئ او یو بل (او لنډمهاله) IP ادرس به کاروئ، چې تاسو ته د ISP لخوا ټاکل سوي وي(Bhatnagar and Kumar, 2016).

د IP Adress ډولونه:

د IP adress مختلف کټګورۍ شتون لري او په هره کټګورۍ کې مختلف ډولونه سته

Consumer IP address

هر فرد یا تجارت چې انټرنیټ ته لاسرسی لري دوه ډوله IP ادرسونه لري: د دوی شخصي IP ادرسونه او د دوی پابلیک IP

ادرسونه. د پابلیک او شخصي اصطلاحات د شبکې د موقعیت پورې اړه لري. یو شخصي IP ادرس په نیټورک کې کارول کیږي، په داسې حال کې چې پابلیک د نیټورک څخه بهر کارول کیږي (Bhatnagar and Kumar, 2016).

Private IP adress

هر Device چې ستاسو د انټرنیټ د نیټورک سره وصلیږي یو شخصي IP ادرس لري. په دې کې کمپیوټرونه، سمارټ موبایلونه او ټابلیټونه شامل دي او هر هغه Device چې بلوتوت یې فعاله وي لکه سپیکر، پرنټر، یا سمارټ تلویزیونونه هم شامل دي. د هغه شیانو ډیریدنه چې د انټرنیټ سره وصلیږي د دې لامل کیږي چې شخصي IP ادرسونه شمیر چې تاسو یې په کور کې لرئ وده ومومي. ستاسو روټر د دغه شیانو د جلا جلا پیژندلو دپاره یوې لارې ته اړتیا لري او دا وسایل هم د یو بل پیژندلو لپاره یوې لارې ته اړتیا لري.
نو په دې خاطر ستاسو روټر Private IP ادرسونه رامنځته کوي چې د هرې وسیلې لپاره ځانګړې پیژندونکې دي چې دوی په نیټورک کې سره جلا کړي (Kalbo el al., 2020).

Public IP address

Public IP adress ستاسو د ټول نیټورک سره تړلی لومړنی IP adress دی. په داسې حال کې چې د نیټورک سره هر وصل سوې وسیله خپل IP adress لري، دوی ستاسو د شبکې د اصلي IP adress کې هم شامل دي. لکه څنګه چې پورته تشریح سوي، ستاسو Public IP ستاسو د ISP لخوا ستاسو روټر ته وړاندې کیږي.
عموما ISPs د IP ادرسو لوی حوض لري چې دوی یې خپلو پیرودونکو ته ورکوي. ستاسو Public IP هغه IP ده چې ستاسو د انټرنیټ د نیټورک څخه بهر ټول وسایل به یې ستاسو د نیټورک د پیژیندلو لپاره کاروي (Kalbo el al., 2020).

د public IP address ډولونه

Static او Dynamic

Dynamic IP addresses

Dynamic IP په اوتومات ډول او په منظم ډول بدلیږي. ISPs د IP ادرسو لوی حوض اخلي او په اتومات ډول یې خپلو پیرودونکو ته ورکوي. د دورې په شکل یې دوي بیا Assign کوي او زاړه IP ادرسونه بیرته په حوض کې اچوي ترڅو د نورو پیرودونکو لپاره وکارول سي. د دې تګلارې دلیل د ISP لپاره د لګښت سپما رامنځته کول دي. د IP ادرسونو منظم حرکت اتومات کول په دې معنی دي چې دوی اړتیا نلري د پیرودونکي IP ادرسونه بیا رامنځته کړي
دا کار په امنیتي لحاظ هم ګټه لري ځکه چې د مثال په توګه که چیرې د IP address استعمالونکي کور ته ولاړ سي نو کله چې IP ادرس بدلو سوې وي نو د مجرمینو لپاره ستاسو د نیټورک انټرفیس هیک کول ستونزمن کوي (Cheng el al., 2017).

Static IP addresses

د Dynamic IP adress برعکس، Static IP adress ثابت پاته کیږي. یوځل چې نیټورک IP adress وټاکي، نو بیا خپل پر حال پاتیږي او نه بدلیږي. ډیری اشخاص او سوداګری Static IP adress ته اړتیا نلري، مګر د هغه سوداګرۍ لپاره چې پلان لري خپل سرور ولري، دا خورا مهم دي چې Static IP adress ولري. دا ځکه چې یو Static IP adress دا یقیني کوي چې هغه ویب پاڼې او ایمیل ادرسونه چې چې ورسره تړلې وي یو ثابت او دوامداره IP adress به ولري - که تاسو حتمي غواړئ چې نور وسایل په دوامداره توګه په ویب کې وموئ نو بیا هم Static IP address ضرور دی (Cheng, C. F., Chou, C. C,2017) .
موږ د Website دوه ډوله IP ادرسونه هم لرو

Shared IP address

Shared IP address هغه IP درسونه دي چې د څو ویبسایټونو ترمنځ شریک وي او په ورته وخت کې څو ویبسایټونو ته کار کوي هغه ویب پاڼې چې د web hosting providers څخه شریک Host اخلي او استفاده ورڅخه کوي معمولا به یو د هغه ویبسایټونو څخه وي چې په ورته سرور کې Host سوې وي دا معمولا د افرادو د ویب پاڼو یا SME ویب پاڼو لپاره استعمالیږي، چیرته چې د traffic اندازه اداره کیدلی سي یا د هغه سایټونه لپاره چې د پاڼو شمیر یې محدود وي.

په دې ډول چې یو ویبسایټ Host سوی وي نو Shared IP adress به ولري.

د Shared IP address ګټې:

1.ارزانه: Shared IP address د Dedicated IP adress په پرتله خورا ارزانه دي ځکه چي ډېرى کاروونکي ورته IP adress شريکوي چي د دې سره IP adress ټول لګښت کموي.

2.تنظيم کول يې اسانه دى:د Shared IP address تنظيم کول اسانه دي او دا کار لږي تخنيکي پوهې ته اړتيا لري چي په دې سره د کوچنيو کاروبارونو او اشخاصو لپاره غوره ثابيتيږي.

3. ښه امنيت: Shared IP address ښه امنيت وړاندي کوي ځکه چي Shared IP address د Host لخوا اداره کيږي، څوک چي د IP adress د څارني او ساتلو مسوليت لري.

4. د منابعو څخه غوره ګټه اخيستنه: د Shared IP address په واسطه کولاى سو د منابعو څخه غوره کار واخلو ځکه چي ډېرى کاروونکي د يوه IP Adress څخه کار اخلي چي په دې سره پر سرور باندې بيروبار کميږي.

5.د تيز ايميل استولو ښه والى: Shared IP address کولاى سي د ايميل استولو ته قوت ورکړي ځکه چي دوي د Email providers لخوا د سپم کيدو چانس لږ لري.

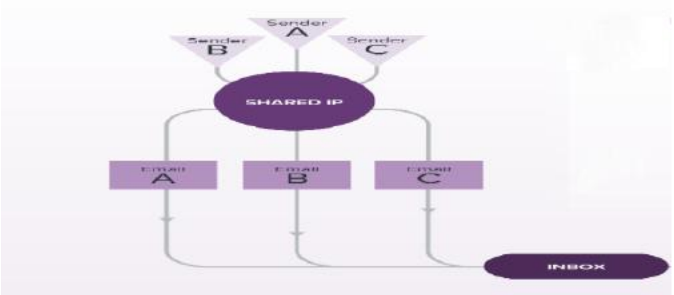
6. غوره SEO:د Shared IP address په واسطه کولاى سو SEO ته وده ورکړو ځکه چي Search engines هغه ويب پاڼي يې د نورو په پرتله انتخاب دي چي IP adresses د نورو معتبرو ويب پاڼو سره شريکوي.

7.د ويب پاڼو فعاليت ښه کوي: Shared IP address کولاى سي د ويب پاڼي فعاليت ښه کړي ځکه چي دوى پر ويبسايټونو د بار توازن او د ويبسايټونو سرچيني په تعادل کي ساتلى سي.

8. د پراخه کيدو وړتيا: Shared IP address د پراخه کيدو وړ دي او کولاى سي د مخ پر ودي سوداګرى اړتياوې پوره کړي.

9.نوي سيستمونو ته ژر خدمت وړاندي کولاى سي: Shared IP address نوي ويبسايټونو ته ژر خدمت وړاندي کولاى سي ځکه چي دوى په اسانى سره د يوه Host څخه بل ته ليداى سي.

10. د ساتلو کم قيمت: Shared IP address د Dedicated IP adress په پرتله لږ ساتني ته اړتيا لري ځکه چي دوى د Host لخوا اداره کيږي(Huang, 2017).



۲ شکل: Shared IP address

څنګه کولاى سو چي خپل IP address مالوم کړو:

ستاسو د روټر Public IP adress چيک کول يې تر ټولو اسانه لاره ده يا هم په Google کي (What is my IP address) سرچ کول چي Google به يې تاسو ته وښيي.

نور ويبسايټونه هم کولاى سي ستاسو IP address ووينې ځکه چي ستاسو روټر سايټ ته د داخليدلو غوښتنه کړې ده او له همدې امله ويبسايټونه ستاسو Public IP address ليدلاى سي. د سايټ IPLocation ستاسو د ISP او ستاسو د ښار نوم هم سره ښوولى سي.

عموما تاسو به يوازي د دې تخنيک په کارولو سره د provider د موقعيت اټکل وکړئ - چيرې چي provider دى، مګر د اصلي Device موقعيت نه. که تاسو دا کار کوئ، په ياد ولرئ چي خپل VPN هم لاګ آوټ کړئ. د Public IP adress د اصلي فزيکي موقعيت د ترلاسه کولو دپاره معمولا تضمين ته اړتيا سته چي ISP ته وسپارل سي.

ستاسو د Private IP adress موندل د پليټ فارم له مخې توپير لري:

په وينډوز کي

- cmd وکاروئ.
- د وينډوز سرچ په کارولو سره د "cmd" سرچ وکړئ.
- بيا په cmd کي د معلوماتو موندلو لپاره "ipconfig" ټايپ کړئ چي مالومات تر لاسه کړى.

په Mac کي:

- د سيستم Preferences ته ولاړ سئ
- نيټورک وټاکئ - او معلومات به ښکاره سي.

په ايفون کي:

- سيټينګ ته ولاړ سئ.

• Wifi انتخاب کړئ او په یوه حلقه کې په "i" کلیک وکړئ () د هغه نیټورک څنګ ته چې تاسو یې لرئ – IP adress به د DHCP تېب لاندې ښکاره سي.

که تاسو اړتیا لرئ په خپل نیټورک کې د نورو وسیلو IP adress چیک کړئ ، روټر ته ولاړ سئ. دا چې تاسو څنګه روټر ته لاسرسی لرئ دا په براند او سافټویر پوري اړه لري چې روټر یې کاروي. عموما، تاسو باید د دې وړتیا ولرئ چې د ورته نیټورک په ویب براوزر کې د روټر gateway IP address ټایپ کړئ نیټورک ته د لاسرسي لپاره. له هغه ځایه تاسو اړتیا لرئ چې یو څه ته ولاړ سئ لکه "attached devices," کوم چې د ټولو وسیلو لیست ښکاره کوي چې اوس مهال یا په دې وروستیو کې په نیټورک کې وصل سوي - په شمول د دوی د IPادرس (Huang, 2017).

د IP address امنیتي خطرونه:

سایبر مجرمین کولای سي ستاسو د IP پته ترلاسه کولو لپاره مختلف تخنیکونه وکاروي. دوه خورا عام یې social engineering او online stalking دي.

برید کونکي کولای سي social engineering وکاروي ترڅو تاسو دوکه درکړي چې تاسو خپل IP ADRESS خپله ښکاره کړي. د مثال په توګه، دوی کولای سي تاسو د سکایپ یا ورته پیغام رسولو اپلیکیشن له لارې ومومي، کوم چې د مخابراتو لپاره IP ADRESS کاروي. که تاسو د دې اپیونو په کارولو سره د ناولده خلکو سره خبري کوئ، نو په دې باید پوه سی چې دوی کولای سي ستاسو IP پته وګوري. برید کونکي کولای سي د Skype Resolver وسیله وکاروي ، چیرې چې دوی کولای سي ستاسو د username څخه ستاسو IP پته ومومي.

سایبر مجرمین کولای سي ستاسو د IP address په معلوموللو لاندي زیانونونه تاسو ته در واړوي

1.د DDoS بریدونه: سایبر مجرمین کولای سي ستاسو د IP ادرس په پیژیندلو سره د (DDoS) بریدونو وکړي کوم چې کولای سي ستاسو نیټورک د وایرس په واسطه د غیري ضروري فایلونو د خلاصولو په واسطه ډیر بیروباري کړي او د دې له امله خراب سي.

2. د پورټ سکین کول: سایبر مجرمین کولای سي ستاسو IP ادرس ستاسو په نیټورک کې د خلاصو پورټونو د سکین کولو لپاره وکاروي چې د دې په واسطه دوی کولای سي ستاسو Devices او ډیټا ته بغیر له اجازې لاسرسی پیدا کړي.

3.پیشینګ: سایبر مجرمین کولای سي ستاسو IP ادرس د پشینګ د ایمیل یا پیشینګ پیغامونو د استولو لپاره وکاروي چې هغه ایمیلونه داسي معلومیږي چې د باوري سرچینې څخه وي، مګر هغه به د حساسو معلوماتو د افشا کولو لپاره ډیزاین سوي وي.

4. د مالویر بریدونه: سایبر مجرمین کولای سي ستاسو IP ادرس ستاسو وسیلو ته د مالویر، لکه ویروسونو یا ransomware استولو لپاره وکاروي ،کوم چې کولای سي ستاسو ډیټا ته زیان ورسوي یا یې غلا کړي.

5. د هویت غلا: سایبر مجرمین کولای سي ستاسو د IP ادرس وکاروي ترڅو ستاسو شخصي معلومات غلا کړي، لکه ستاسو نوم، پته او مالي توضیحات، چې د هویت د غلا لپاره کارول کېدای سي.

6. د هیک کولو هڅي: سایبر مجرمین کولای سي ستاسو IP ادرس ستاسو د Devices یا نیټورک د هیک کولو لپاره وکاروي کوم چې د معلوماتو د غلا یا نورو امنیتي پیښو سبب کېدای سي.

7. Cyber stalking: سایبر مجرمین کولای سي ستاسو IP ادرس ستاسو د آنلاین فعالیت د تعقیب لپاره وکاروي او ستاسو انلاین چلند وڅاري، کوم چې د Cyber stalking یا ځورونې لپاره کارول کېدای سي.

8. جاسوسي: سایبر مجرمین کولای سي ستاسو IP ادرس ستاسو د سازمان یا شخصي ژوند په اړه د استخباراتي یا حساسو معلومات د راټولولو لپاره وکاروي، کوم چې د جاسوسۍ یا بلیک میل لپاره کارول کېدای سي.

9. Botnet attacks: سایبر مجرمین کولای سي ستاسو د IP ادرس په واسطه کولای سي د یوه هیک سوي نیټورک Devices کنټرول کړي چې د بوټنیټ په نوم پیژندل کیږي ، کوم چې د مختلفو ناوړه اهدافو لپاره کارول کېدای سي.

10. شخصیت ته تاوان رسول: سایبر مجرمین کولای سي ستاسو IP ادرس په غیرقانوني یا غیر اخلاقي فعالیتونو کې د ښکیلتیا لپاره وکاروي، کوم چې کولای سي ستاسو شهرت ته زیان ورسوي یا قانوني پایلې ولري. (Fisher and Bolles, 2015)

۳ شکل: د IP address امنيتي خطرونه

Online stalking

مجرمين کولای سي ستاسو د آنلاين فعاليت تعقيبولو سره ستاسو IP پته تعقيب کړي. هر ډول آنلاين فعاليتونه کولای سي ستاسو IP پته ښکاره کړي، د Video games څخه تر ويب پاڼو باندي د کمينټ کولو پوري يوځل چي دوی ستاسو IP پته ولري، بريد کونکي کولای سي د IP website tracking address ته لاړ سي، لکه whatismyipaddress.com، په دې ويبسايټ کې ستاسو IP وليکي او بيا ستاسو د موقعيت په اړه يو نظر ترلاسه کړي. دوی بيا کولای سي open sources معلوماتو ته مراجعه وکړي که دوی وغواړي دا تاييد کړي چي ايا IP پته په ځانګړي ډول ستاسو سره تړاو لري. دوی بيا کولای سي LinkedIn، Facebook، يا نوري ټولنيزي شبکي وکاروي چي دا ښيي چي تاسو چيرته ژوند کوئ او بيا وګورئ چي دا د ورکړل سوي ساحې سره سمون لري که يا.

که سايبر مجرمين ستاسو د IP پته وپيژني، دوی کولای سي ستاسو په وړاندي بريدونه پيل کړي يا حتی تاسو په نښه کړي. دا مهمه ده چي د خطرونو څخه خبر اوسئ او څنګه يې کم کړئ.

دا کارونه هم په خطرونو کي شامل دي:

ستاسو د IP ADRESS په کارولو سره د غيرقانوني شيانو ډاونلوډ کول هيکران د هيک سوي IP ADRESS کارولو په واسطه د غيرقانوني شيانو ډاونلوډ کولو لپاره پيژندل سوي دي او هر هغه څه چي دوی نه غواړي دوی په وپيژيندل سي يا دوی ته راجع سي. د مثال په توګه، ستاسو د IP ADRESS ياني ستاسو د پيژندني په کارولو سره، مجرمين کولای سي غيري قانوني (چي غيري قانوني رانيول او خرڅول کيږي) فلمونه، ميوزيک او ويډيو ډاونلوډ کړي - کوم چي ستاسو د ISP د شرايطو څخه سرغړونه کوي - او ډير جدي، د تروريزم يا د ماشومانو فحشا پوري اړوند مواد ډاونلوډ کړي. دا په دې معنی کېدای سي چي تاسو - ستاسو د ګناه پرته - د قانون په وړاندي مجرم کړي(Fisher and Bolles, 2015) .

۴ شکل: Online stalking

ستاسو د موقعيت مالومول:

که هيکرانو ته ستاسو IP پته مالومه وي، هيکران د geolocation technology په واسطه ستاسو سيمه، ښار او دولت وپيژني. دوی يوازي دې ته اړتيا لري چي په ټولنيزو رسنيو کي يو څه نور سرچ وکړي ترڅو ستاسو کور مالوم کړي او په احتمالي توګه غلا ځيني وکړي کله چي دوی پوه سي چي تاسو په کور کي نه ياست.(Fisher and Bolles, 2015)

په مستقيم ډول ستاسو پر نيټورک حمله:

مجرمين کولای سي مستقيم ستاسو نيټورک په نښه کړي او مختلف بريدونه پيل کړي. يو له خورا مشهور څخه د DDoS بريد دی (distributed denial-of-service)دا ډول سايبر بريد هغه وخت رامنځته کيږي کله چي هيکران هغه ماشينان کاروي چي وختي لا هيک سوي وي يا د هيکينګ تر تاثير لاندي راغلي وي ترڅو د هدف سوي سيسټم يا سرور څخه لوی مقدار غوښتني وکړي او سيسټم کمزوری کړي. دا د سرور د اداره کولو د قدرت څخه خورا ډير ترافيک رامنځته کوي، په پايله کي خدمات ګډوډ وي. دا ستاسو انټرنيټ بندوي. دا بريد عموما د سوداګری او Video games خدماتو پروړاندي پيل کيږي، دا د يو فرد پر وړاندي هم پيښيدلای سي ، که څه هم دا خورا لږ پيښيږي. د دې خطر سره په ځانګړي ډول انلاين ګيميرانو ډير مخ کيږي څکه چي د دوی سکرين د Stream کولو پر مهال ليدل کيږي (په کوم کي چي IP پته مالوميدلی سي.(Liu et al., 2019)

ستاسو Device ته په داخليدو هيک کول:

انټرنيټ د وصلولو لپاره Ports او همدارنګه ستاسو IP پته کاروي. د هر IP ADRESS لپاره په زرګونو Ports شتون لري او يو هيکر چي ستاسو IP

پیژني کولای سي د دې ports په واسطه د نیټورک سره وصل سي د مثال په توګه، دوی کولای سي ستاسو تلیفون ستاسو څخه واخلي او ستاسو مالومات غلا کړي. که یو مجرم ستاسو تلیفون یا بل هر Device ته لاسرسی ومومي، دوی کولای سي په دې کي Malware انسټال کړي.. . (Liu et al., 2019)

څنګه کولای سو چي خپل IP پټ کړو او ساتنه یې وکړو:

ستاسو د IP پته پټول ستاسو د شخصي معلوماتو او آنلاین هویت ساتلو یوه لاره ده.

ستاسو د IP د پټولو دوې لومړنۍ لاري:

1. د proxy server کارول
2. د virtual private network (VPN) کارول

proxy server: یو منځګړی سرور دی چي له لاري یې ستاسو ټرافیک استول کیږي:

• هغه انټرنیټ سرورونه چي تاسو یې ګورئ یوازي د هغه پراکسي سرور IP ادرس ګوري نه ستاسو IP ادرس.

• کله چي دا سرورونه تاسو ته معلومات در استوي، دا یو وار پراکسي سرور ته ځي، بیا د پراکسي سرور څخه تاسو ته راځي.

د پراکسي سرورونو نیمګړتیا دا ده چي ځینې پراکسي سرورونه ستاسو مالومات اخلي - نو تاسو اړتیا لرئ چي د باور وړ پراکسي سرور استعمال کړی دوی کولای سي ستاسو په براوزر کي اعلانونه هم داخل کړي چي تاسو یې وګورئ او دوی پیسې ځیني تر لاسه کړي

VPN غوره حل لار وړاندي کوي:

کله چي تاسو خپل کمپیوټر – یا سمارټ فون یا ټابلیټ – له VPN سره وصل کړئ، وسیله نو Device داسې عمل کوي لکه Device چي د VPN په ځایی نیټورک کي وي.

• ستاسو د نیټورک ټول ټرافیک VPN ته د خوندي اړیکي له لاري لیږل کیږي.

• څکه چي ستاسو کمپیوټر داسي عمل کوي لکه دا چي د VPN په نیټورک کي وي، تاسو کولای سئ چي په خوندي توګه د محلي نیټورک سرچینو ته لاسرسی ومومئ حتی کله چي تاسو په بل هیواد کي یاست.

• تاسو کولای شئ انټرنیټ هم وکاروئ لکه تاسو چي د VPN په موقعیت کي موجود یاست ، کوم چي تاسو ته ګټه لري که تاسو عامه وای فای کاروئ یا غواړئ چي بلاک سوي ویب سایټونو ته لاسرسی ومومئ .(Gashi and Pirangutti, 2019)

Kaspersky Secure Connection

Kaspersky یو (VPN) دی چي د Kaspersky لابراتوار لخوا وړاندي کیږي یو شرکت دی دی چي په روسیه کي موقعت لري.

دا د VPN خدمت د دې لپاره ډیزاین سوی چي کاروونکو ته د انټرنیټ سره د وصلیدو په وخت کي خوندي او شخصي اړیکه اماده کړي، د دوی آنلاین فعالیتونه د احتمالي سایبر ګواښونو څخه ساتي.

د Kaspersky (VPN) یو لړ ځانګړتیاوې وړاندي کوي چي د کاروونکو آنلاین فعالیتونو امنیت او Privacy ته د ودي ورکولو لپاره ډیزاین سوي دی. دا ځانګړتیاوې عبارت دي له:

1. کوډ کول: Kaspersky د نظامي درجې کوډ کولو څخه کار اخلي ترڅو د کاروونکو آنلاین فعالیتونه د هیکرانو، سایبر جنایتکارانو او نورو ناوړه خلکو څخه خوندي کړي. د VPN خدمت پرمختللي Encryption standard (AES) د 256-bit keys سره کاروي کوم چي یو له خورا خوندي Encryption methods څخه شمیرل کیږي.

2. د کارکوونکو معلوماتو ته د نه لاسرسي پالیسي: Kaspersky د کارکوونکو شخصي معلوماتو ته د نه ننوتلو سخته پالیسي لري ، په دې معنی چي د VPN خدمت د کاروونکو آنلاین فعالیتونو په اړه هیڅ معلومات نه راټولوي یا ذخیره کوي. دا ډاډ ورکوي چي د کاروونکو Privacy خوندي ده او د دوی آنلاین فعالیتونه نسي موندل کېدای.

3. په یوه وخت کي څو Devices ته کار کول: Kaspersky په ډیری Devices کي کارول کېدای سي ، په شمول وینډوز ، ماک ، iOS او Android. دا کاروونکو ته اجازه ورکوي چي خپل آنلاین فعالیتونه په خپلو ټولو وسیلو کي خوندي کړي هغه که هر عملیاتي سیسټم وي چي دوی یې کاروي.

4. اتومات وصلیدل:Kaspersky داسي تنظیم کېدای سي چي کله کاروونکي د انټرنیټ سره وصل سي نو په اتوماتیک ډول د VPN سره وصل سي چي بیا دا ډاډ ورکوي چي د کاروونکو آنلاین فعالیتونه تل خوندي دي، حتی که دوی د VPN سره د خپل Device وصل کول هیر کړي وي.

د Kaspersky ګټې:

Kaspersky د کاروونکو لپاره یو لړ ګټې وړاندې کوي چې ځيني يې په لاندې ډول دي:

1. ښه امنيت: د Kaspersky Secure Connection د پوځي درجې کوډ کول کاروي ترڅو د کاروونکو آنلاین فعاليتونه د هيکرانو، سايبر جنايتکارانو او نورو ناوړه لوبغاړو څخه خوندي کړي. دا ډاډ ورکوي چې د کاروونکو حساس معلومات، لکه پاسورډونه، د کریډیټ کارت توضیحات او شخصي معلومات، د هيک کولو څخه خوندي وساتي.

2. د Privacy ساتنه: د Kaspersky Secure Connection د نه Login کيدو سخته پاليسي لري، دا په دې مانا ده چې د کاروونکو آنلاین فعاليتونه بيرته د دوی دخوا لاسرسی نه سي ورته کېدای. دا ډاډ ورکوي چې د کاروونکو Privacy خوندي ده او د دوی آنلاین فعاليتونه شخصي ساتل کيږي.

3. محدودو سايټونو ته لاس رسی: Kaspersky کاروونکو ته اجازه ورکوي چې محدودو ويبسايټونو ته لاسرسی ومومي، لکه geo-restricted ويب پاڼې او د streaming services ته (Gashi and Pirangutti, 2019).

کله باید VPN استعمال کړئ:

د VPN کارول ستاسو IP پته پټوي او ستاسو ترافیک د جلا سرور له لارې ویبسایټونو ته رسوي ، کله چې تاسو آنلاین یاست نو خورا خوندي مو ساتي.

هغه وخت چې کېدای سي تاسو VPN استعمال کړی

کله چې Public IP کاروئ:

کله چې د Public Wi-Fi نيټورک کاروئ، حتی هغه چې پاسورډ ولري، . که یو هيکر په ورته وائی فای نيټورک کې وي نو د VPN استعمال به غوره وي، که هيکر په ورته واي فاي نيټورک کې وي نو دا ورته اسانه ده چې ستاسو ډيټا وپلټي. اولنی سيکيوريټي چې اوسط Public Wi-Fi وړاندې کوي په نيټورک کې د نورو کاروونکو څخه قوي محافظت نه کوي. د VPN کارول به ستاسو ډيټا ته اضافه سيکيوريټي ورکړي او تاسو ته ډاډ درکوي چې ستاسو ټولې اړیکې خوندي دي.

کله چې سفر کوی:

که تاسو یو بهرني هیواد ته سفر کوئ - د بیلګې په توګه، چين، چيري چې د فيسبوک په څير سايټونه بند سوي دي - یو VPN کولای سي ستاسو سره د هغه سايټونو چې په هغه هيواد کې بند وي د خدماتو په لاسرسي کې مرسته وکړي.

د VPN په واسطه کولای سی چې د سټریمینګ خدمات وکاروئ کله چې تاسو په خپل هيواد کې لاسرسی ورته لرئ ، مګر د نړیوالو حقونو مسلو له امله په بل هيواد کې شتون ونلري نو د VPN په واسطه يې کارولی سی. د VPN کارول تاسو ته دا وړتيا درکوي چې خدمات داسي وکاروئ لکه تاسو چې په کور کې یاست. مسافرين ممکن د VPN کارولو پرمهال ارزانه هوايي کرايه هم پيدا کړي، ځکه چې نرخونه د يوې سيمې څخه تر بلې سيمې پورې توپير لري.

کله چې تاسو په انلاین ډول د دفتر څخه ليرې کار کوئ

دا په ځانګړي توګه د کوويډ وروسته په نړۍ کې عامه سوه ،ځکه چې ډیرو خلکو د دفتر څخه ليرې کار کوی. ډيری وختونه کار کوونکي دې ته مجبوره کيږي چې د کمپنی د امنيت د خونديتوب دپاره د کمپنی خدماتو ته د لاسرسي دپاره VPN استعمال کړي کله چې تاسو په دفتر کې نه یاست یو VPN چې ستاسو د دفتر د سرور سره وصل دی کولای سي تاسو ته د داخلي شرکت نيټورک او سرچينو ته لاسرسی درکړي کله چې تاسو په کور کې نه یاست دا ستاسو د کور د نيټورک لپاره هم کاريدلی سي.

کله چې فقط تاسو یو څه شخصي حريم غواړی

حتی ستاسو د کور په آرامۍ کې د ورځني موخو لپاره د انټرنيټ د کارولو دپاره د VPN کارول یو ښه نظر کېدای سي. هرکله چې تاسو ويبسايټ ته لاسرسی وموميئ ،هغه سرور چې تاسو ورسره وصل یاست ستاسو IP ادرس ته داخليږي او ستاسو ټول معلومات کولای سي لکه: ستاسو د سرچ عادتونه ، هغه څه چې تاسو يې کليک کوئ ، تاسو څومره وخت په یوه ويبسايټ کې تيروی. دوی کولای سي دا معلومات د اعلاناتو پر شرکتونو خرڅ کړي چې هغه شرکتونه بيا تاسو ته د دې مالوماتو پر اساس اعلانات ښيي له همدې امله په انټرنيټ کې اعلانونه ځينې وختونه ډير شخصي مالوميږي لکه ستاسو دپاره چې وي: دا ځکه چې داغسي هم دي. ستاسو IP ادرس ستاسو د موقعيت تعقيبولو لپاره هم کارول کېدای سي، حتی کله چې ستاسو د Location بند وي. د VPN کارول په ويب کې ستاسو د نښانو د پريښوولو مخنيوی کوي.

خپل موبایل هم مه هیروئ. موبایل هم IP ادرس لري او تاسو شاید دا د خپل کور د کمپیوټر په پرتله په ډیرو ځایونو کي وکاروئ، کیداي سي د Public Wifi سره یې هم وصل کړی کله چي تاسو د داسي یوه نیټورک سره وصلیږی چي باور نه باندي لری نو دا به ښه وي چي په خپل گرځنده تلیفون کي VPN وکاروئ(Gashi and Pirangutti, 2019).

په انټرنیټ کي د Privacy یا شخصي حریم د ساتلو دپاره نوري لاري:

Change privacy settings on instant messaging applications

هغه اپلیکیشنونه چي ستاسو په موبایل کي انستال دي د IP ادرس د هیک کولو لویه سرچینه ده. د میسیج استولو او نورو زنگ وهلو اپلیکیشنونه د سایبر جنایتکارانو لخوا د وسیلي په توگه کارول کېدای سي. که چیري تاسو د IM اپلیکیشن انستال کړئ نو هغه یوازي هغه خلکو ته د مسیج او زنگ اجازه ورکوي چي تاسو یې نمبر لری او د هغو خلکو زنگ او میسیج نه مني چي تاسو یې نه پیژنئ. نو ستاسو د Privacy settings بدلول ستاسو د IP ادرس پیدا کیدل سختوي ځکه چي هغه خلک چي تاسو نه پیژنیي ستاسو سره اړیکه نسي نیولای.

بې مثاله او رقم په رقم پاسورډونه کار کړی

ستاسو د Device پاسورډ یوازینی خنډ دی چي کولای سي خلک ستاسو Device ته د لاسرسي څخه منعه کړي. ځینې خلک د خپلو وسایلو ډیفالټ پاسورډونو کاروي(هغه پاسورډ چي د کمپنۍ دخوا ورکړل سوی دی)

چي دوی د هیک دپاره ښه جوړ دي. ستاسو د ټولو حسابونو په څیر، ستاسو Device باید یو ځانگړی او پیاوړی پاسورډ ولري چي مالومول یې اسانه نه وي. یو پیاوړی پاسورډ د غټو او کوچنیو حروفونو، شمیرو او خاصو حروفونو مخلوط دی چي دا کار به ستاسو د Device د IP ادرس د هیک کولو پروړاندي په خوندي کولو کي مرسته وکړي (Pirangutti, P .2019).

د پیشینگ د ایمیلونو او خطري سافټویرونه او ویرسونو په اړه محتاط اوسئ:

د مالویر او Device tracking softwares غټه برخه د پیشینگ د ایمیلونو له لاري انستال سوی دي. کله چي تاسو د کوم سایټ سره وصل شئ، دا سایټ ستاسو IP ادرس او د Device موقعیت ته لاسرسی پیدا کوي، چي دا کار د هیک لاره اسانه کوي. کله چي د نامعلوم خلکو ایمیلونه خلاصوی نو محتاط اوسئ او د هغه لینکونو کلیک کولو څخه ډډه وکړئ چي تاسو unauthorized سایټونو ته بیایي. هغه شیان چي تاسو ته یې خلک په ایمیلونو کي در استوي ډیر پام ورته کوی حتی که داسې ښکاري چي د مشهور سایټونو او مشروع سوداگری څخه دي(Pirangutti, P .2019).

یو ښه انټي وایرس استعمال کړی او Update

یو ښه انټي ویروس سافټویر انسټال کړئ او Update یې وساتئ. د مثال په توگه ، Kaspersky's Anti-Virus protection تاسو ستاسو په کمپیوټر او Android وسیلو کي د ویروسونو څخه ساتي ، ستاسو پاسورډونه او شخصي اسناد خوندي او ذخیره کوي او هغه ډیټا خوندي ساتي چي تاسو یې د VPN د استعمال په وخت کي لیږئ او ترلاسه کوئ(Gashi and Pirangutti, 2019).

د دې کارونو له لاري د سایبر جنایتکارانو د پراخه بریدونو پر وړاندي خوندي پاته کیدلی سو

IP based monitoring system

Ip based monitoring system د نیټورک د امنیت یو اړین اړخ دی، ځکه چي دا د سوداگری خاوندانو او د نیټورک مسوولینو ته اړین وسایل ورکوي تر څو هغه څوک چي غیري قانوني نیټورک ته داخل سوی وي وپیژني او مخنیوی یې وکړي، احتمالي بریدونه بند کړي او په نیټورک کي کوم شکمن فعالیت وپیژني. د IP ادرس څارنه د د نیټورک دهغه ترافیک دوامداره او دقیقه څارنه هم ده ، کوم چي په نیټورک کي د نور Devices سره اړیکه ساتي. تاسو په ډیري اسانی سره کولای سئ چي د IP Adress په مدیریت سره خپل د نیټورک اړیکي وڅارئ، بې له دې چي هر وار د سیستم د امنیت دپاره سیستم ته تاییدي ورکړی سیستم اداره کړي چي څوک ستاسو د خصوصي شرکت سرورونو او ډیټابیسونو ته لاسرسی لري. په اصل کي، دا د آنلاین غلا په څیر کار کوي. ستاسو کارمندان به اړتیا ونلري چي هر وار سیستم ته د ننوتلو دپاره پاسورډ یا بله طریقه د سیکیوریټي دپاره استعمال کړي که ستاسو د شرکت Network یو ثابت IP Adress ولري، دا د Cloud سرچینو ته لاسرسی اسانه کوي. د امنیت او راحت دا کچه د نن ورځې په سختیو کي چي موږ د انلاین کار کولو په وخت کي ورسره مخ کیږو اړینه ده.

د IP اداره هم د ډیجیټل میلمنو لیست سره ورته ده. تاسو کولای شئ خپل شبکي ته د لاسرسي لپاره ځانگړي IP Adress فعاله کړئ ترڅو یوازي هغه کارونکي چي اجازه لري وکولای سي د شرکت ډیټا او سرچینو ته

لاسرسی ومومي د دې پرځای چې ټول کار کوونکي لاسرسی ورته ولري د IP مدیریت د دې دمخه هیڅکله دومره ښه نه وه .,Ghazanfari et al) 2016)

۵ شکل: IP based monitoring system

د Ip based monitoring system ګټې:

ډیر مایکرو خدماتو، ډیټابیسونو، اپلیکیشنونو او نورو تخنیکي شیانو دپاره چې هر یو یې IP Adress لري ادراه ډیره سخته ده د دې IP Adresses سهي ساتل د وسیلو د مناسب ارتباط او متقابل عمل لپاره خورا مهم دي. راځئ چې د IP Adress کنټرول کلیدي ګټې زده کړو

۱: د لیرې ځای څخه سیسټم ته لاسرسی او د لاسرسي کنټرول خوندي کیدل:

ستاسو ټیم کولای سي د IP اجازه لیست په کارولو سره د دفتر او شخصي کمپیوټر څخه د دفتر د نیټورک سرچینو ته په خوندي ډول لاسرسی ومومي. د نن ورځې پراخه هایبرډ شبکې تاسیساتو کې ، ډیری شرکتونه د بدلیدو وړ لاسرسي ته اړتیا لري ترڅو دواړه دننه او کلاوډ امنیت مشکلات کم کړي.

د دې کنټرول لپاره یوه مؤثره طریقه چې ستاسو کوم کارمند ځانګړي شرکتونو ته لاسرسی لري د IP اجازه لیست دی. د دې په کولو سره تاسو کولای سئ ډاډ ترلاسه کړئ چې ستاسو همکاران یوازې هغه سرچینو ته لاسرسی لري چې دوی ورته اړتیا لري او د سوداګرۍ حساس معلومات نلري. دا ممکن هغه اشخاص چې اجازه نه لري ودروي چې شخصي معلوماتو او حساسو معلوماتو ته د لاسرسي هڅه وکړي.

۲:پوخ اعتبار

د غلط ترتیب، منازعې فرعي نیټونو او د IP Adress شخړو د پام وړ خطر تل په هغو شبکو کې شتون لري چې پراخیږي. دا خطرونه د شرکت په ټوله Network منفي اغیزه لري او د شبکې مدیرانو کار نور هم اضافه کوي.

د بشپړ ډومین نوم (FQDN) غوښتنه کولو سره، کوم چې د DNS په سرور کې چې د درختي په رقم جوړښت لري د ډومین نوم او دقیق ځای موږ ته راښیي، IPAM سافټویر دا خطرونه کموي او د ستونزو حل کولو وخت اوږدوي.

۳: لږ پیچلتیا

IPAM سافټویر د IP Adress مدیریت ساده کولو کې د مرستې لپاره د یوازینۍ مرکزي ذخیرې څخه کار اخلي. د IP Adress ځای په اړه معلومات د سیمه ایز انټرنیټ راجستر (RIR) څخه ترلاسه کوي. IPAM د مدیرانو سره د نیټورکو په موندلو کې مرسته کوي، عامه او خصوصي IP Adresses اداره کوي او په خو ترل سوي Hosts کې ډاټا راټولوي.

د IP Adress موخه دا ده چې د Devices او د هغه سایټ چې ضرورت دی ورته ترمنځ اړیکه رامنځته کړي. د IP Adress په ځانګړي ډول په انټرنیټ کې هر وسیله پیژني. د IP پرته، د وسیلو سره د اړیکې کومه لاره نسته. د کمپیوټري وسیلې ممکن د هغه سایټونو چې ضرورت یې دی، ورته اړیکه ونیسي لکه ویبسایټ او سټریمینګ خدمات د IP Adress څخه مننه ، چې ویبسایټونو ته لیدونکي هم ورپیژني.

د IP د شمیرې په کتلو سره، دا ممکنه ده چې د اشخاصو هیوادونه، ښارونه، عرض البلد او طلول البلد او ISP (د انټرنیټ خدمت چمتو کوونکي) مالوم کړي. د دې سیسټمونو په واسطه تاسو کولای سئ چې په اسانۍ سره هغه خلک وپیژني چې سایبر جرمونه کوي

د IP based monitoring systems ګټه دا ده چې دوی د دودیز سیسټمونو په پرتله ډیر د پراخه کیدو وړ دي. SaaS شرکتونه د اتوماتیک پراخه کیدو ځانګړتیا لري چې دوی ته اجازه ورکوي چې سرورونه او زیربناوې د غوښتنې سره سم وساتي، که یو کاروونکي وي یا 10,000.

دا پراخه کول کولای سي د IP based monitoring systems د دودیزو سیسټمونو په پرتله خورا ارزانه او اغیزمن کړي چې ممکن د ودې لپاره د پام وړ د هارډویر اپ ګریډ یا بدیلیدو ته اړتیا ولري.

په نهایت کې د IP based monitoring systems د دودیزو سیسټمونو په پرتله خورا پرمختللي ځانګړتیاوې او ورتیاوې وړاندې کوي. د مثال په

توګه سینسرونو او IoT وسیلو کارول چي کولای سي یوازي د امنیت محافظت هاخوا ډیټا او Insights چمتو کړي. سربیره پردې د IP based monitoring systems ممکن د دې توان ولري چي لوی ډاټا تحلیل کړي او کاروونکو ته ارزښتناکه بصیرت او سپارښتنې وړاندي کړي.

په ټولیز ډول، په داسي حال کي چي د IP based monitoring systems د دودیز سیستمونو سره د پرتلې وړ نه دي د IP-based سیستمونو کارولو ډیري ګټي ممکن دوی کاروونکو ته ډیر د خوښي وړ وګرځوي(Ghazanfari et al., 2016)

د IP based monitoring system ډیزاین او تطبیق:

د IP based monitoring system د څارني سیستم یو ډول دی چي د انټرنیټ پر پروتوکول (IP) کیمرې او نورو د نیټورک وسیلو په کارولو تکیه کوي ترڅو د فعالیت څارنه او ثبت وکړي. دا سیستم د امنیت او خوندیتوب د موخو لپاره د استوګنې او سوداګریز چاپیریال دواړو کي انسټال کېدای سي. د IP based monitoring system په ډیزاین کي په عموم ډول د هغه ساحو مالوموول شامل دي چي نظارت ته اړتیا لري ، د مناسبو IP کیمرو او نور د نیټورک وسیلې غوره کول، د شبکي ټوپولوژي ډیزاین کول، د سافټویر او هارډویر اجزا configure کول شامل دي. د implemetation د مرحلې په جریان کي ، IP کیمرې به نصب سي ، د نیټورک وسایل به configure سي او سافټویر به ترتیب سوی وي ترڅو د پیښو د لیري لیدلو ، ثبت کولو او د پیښو خبرتیا ته زمینه مساعده سي.

د انټرنیټ د وصلیدو سره سم دا سیستم له هر ځای څخه د لاسرسی وړ دی او دا د نورو امنیتي سیستمونو لکه الارمونو او د access control سیستمونو سره یو ځای کېدلای سي. د IP based monitoring system یوه له مهمو ګټو څخه دا ده چي موږ یې اندازه غټولای او کوچنی کولای سو. سیستم د لینو یا کیبلونو پرته د اضافي IP کیمرې یا د نیټورک د وسیلو په اضافه کولو سره په اسانی سره پراخه کېدای سي. بله ګټه د نورو امنیتي سیستمونو سره د ادغام وړتیا ده، د جامع او تیز امنیتي حل لپاره ډیر ښه سیستم دی. په ټوله کي، د IP based monitoring system ډیزاین او تطبیق کولو دپاره نیټورک ډیزاین، امنیت او سافټویر configuration کي تخصص ته اړتیا سته. دا مهمه ده چي د وړ مسلکي کسانو سره کار وکړو ترڅو ډاډ ترلاسه سي چي سیستم په سمه توګه ډیزاین سوی او د غوره فعالیت او امنیت لپاره پلي سوی(Ghazanfari et al., 2016)

٦ شکل: د IP based monitoring system ډیزاین او تطبیق

څنګه کولای سو چي د IP based monitoring systems په سمه توګه استفاده کړو:

د دې لپاره چي ډاډ ترلاسه سي چي دا سیستمونه په سمه توګه کاریږي د دې لپاره ډیر نظرونه سته چي باید په پام کي ونیول سي چي ځیني یې په لاندي ډول دي.

1. **خپل سیستم په احتیاط سره پلان کړئ**: مخکي له دې چي د IP based monitoring systems د خپلي کمپنۍ لپاره فعاله کړی دا مهمه ده چي سیستم په احتیاط سره پلان کړئ. په دې کار کي د هغه ساحو پیژندل شامل دي چي نظارت ته اړتیا لري، د اړتیا وړ کیمرو شمیر او ډول مشخص کول او د مناسب سافټویر او هارډویر غوره کول ډیر مهم دي. دا هم مهمه ده چي د رڼا، د هوا شرایط او احتمالي امنیتي ګواښونه هم په پام کي ونیسئ کله چي د سیستم د جوړولو لپاره پلان جوړوی.

2. **سمې کیمرې غوره کړئ**: هغه کیمرې چي د IP based monitoring systems کي کارول کیږي کولای سي د سیستم په اغیزمنتوب کي د پام وړ اغیزه ولري. دا مهمه ده چي هغه کیمرې غوره کړئ چي د هغه چاپیریال لپاره مناسبي وي چیرې چي دوی کارول کیږي، لکه د کور دننه یا بهر کیمرې او داسي کیمرې انتخاب کړي چي مناسب ریزولوشن ولري او ساحه ښه معلومولای سي.

3. **د نیټورک صحي bandwidth استعمال کړی**: د IP based monitoring systems د شبکې په بینډ ویت تکیه کوي ترڅو د کیمرې څخه د څارني سافټویر ته د ویډیو ډیټا واستوي.

دا مهمه ده چي ډاډ ترلاسه سي چي شبکه کافي بینډ ویت لري ترڅو چي د موجوده کیمرو استعمال ممکن کړي او د شبکي د بندیدو مخه ونیسي.

4. **د لوړ کیفیت د څارني سافټویر وکاروئ**: د څارني سافټویر چي د IP based monitoring systems کي کارول کیږي د هغ سیستم اغیزمنتیا

خورا مهمه ده دا مهمه ده چې داسي سافټویر غوره کړئ چې د باور وړ وي، کارول يې اسانه وي او د سيسټم نظارت او اداره کولو لپاره اړين اپشنونه وړاندي کوي د دې سیسټمونو څخه ځيني مشهور سيسټمونه يې په په لاندي ډول دي

Milestone XProtect, Genetec Security Center, Axis Camera Station

5. سيسټم خوندي کړئ: د IP based monitoring systems د سایبر ګواښونو سره مخ دي، نو دا مهمه ده چې د سيسټم خوندي کولو لپاره ګامونه پورته کړئ. په دې کي د قوي پاسورډونو کارول ، د Two factor authentication او د سافټویر او Firmware اپډیټ کول شامل دي ترڅو د امنيت د زيانونو څخه خوندي پاته سو.

6. د کاروونکو روزنه: مناسبه روزنه د دې لپاره اړينه ده چې ډاډ ترلاسه سي چې کاروونکي د IP based monitoring systems په اغیزمنه توګه کاروي. په دې کي د څارني سافټویر د کارولو روزنه، د ویډیو فوټیج ته د لاسرسي او ليدلو روزنه او امنيتي پيښو ته د ځواب ويلو روزنه شامله ده.

7. د سيسټم ساتنه او د خرابيدو مخنيوی: منظمه ساتنه د دې لپاره مهمه ده چې ډاډ ترلاسه سي چې د IP based monitoring systems په سمه توګه کار کوي. په دې کي د کيمرو او لينزونو پاکول ، Firmware د تازه معلوماتو لپاره چیک کول او په منظم ډول د سیسټم ازمويل شامل دي ترڅو هر ډول ستونزې وپيژني او حل يې کړي(Ghasemi et al., 2018).

د IP based monitoring systems ډولونه:

د IP based monitoring systems کي ډير ډولونه شتون لري لاندي ډولونه يې عموماً کارول کيږي:

Network monitoring systems -1:

د نيټورک څارني سيسټمونه يوه مهمه وسيله ده چې د سازمانونو سره مرسته کوي د دوی د کمپيوټري زيربنا او د نيټورک فعاليت او حالت تعقيب کړي. په نننی نړۍ کي په ټيکنالوژۍ باندې د ډيريدونکي تکيې(تکيه) سره ، دا د سازمانونو لپاره د هر وخت څخه ډيره مهمه سوې ده چې د نيټورک د نظارت ټکنالوژي ولري ترڅو ډاډ ترلاسه کړي چې د دوی نيټورک په ښه توګه فعاليت کوي.

د نيټورک څارنه د نيټورک د فعاليتونو تعقيب کولو پروسې ته وايي ترڅو غلطياني کشف او ستونزې حل کړي او د نيټورک د صحي ساتنې دنده ترسره کړي ترڅو د نيټورک اغيزمن او اسانه عمليات يقيني کړي. د نيټورک په څارنه کي د نيټورک شتون او د خدماتو کيفيت ساتلو لپاره د وسايطو، ټرافيک او ډيټا فعاليت څارنه شامله ده. د نيټورک څارنه د مختلفو تخنيکونو او وسايلو په کارولو سره پلي کېدای سي. د نيټورک د څارني سيسټمونو ډيری ډولونه شتون لري، پشمول د packet sniffers ، uptime monitors، bandwidth analyzers او log file analyzers.

راځئ چې دا سيسټمونو هر يو جلا جلا تشريح کړو:

Packet Sniffers: پاکټ سنيفير کولای سي د نيټورک په پاکټونو کي د مداخلې او تحليل کولو سره د نيټورک فعاليت وپيژندلو کي مرسته وکړي. Packet Sniffers کولای سي پاکټونه د مختلفو پروټوکولونو، ادرسونو يا اپليکيشنونو مطابق فلټر کړي او کولای سي پاکټ ډيکوډ او ښکاره کړي. د پيکټ سنيفيرونه کولای سي د نيټورک د مديرانو سره د نيټورک د مختلفو مسلو په پيژندلو کي مرسته وکړي، لکه د خنډونو پيژندل، غير معمولي ترافيک يا ضعيف فعاليت په ګوته کول او د نيټورک د امنيتي مسلو پيژندل. د پيکټ سنيفيرونه د ستونزو حل کولو موخو لپاره هم کارول کېدای سي ، ځکه چې دوی کولای سي کله چې د نيټورک erors پرمهال پاکټونه ونيسي. په هرصورت، د پيکټ سنيفيرانو لپاره ځينې محدوديتونه شتون لري، لکه د کوډ سوي ټرافيک په نيولو کي ناتواني او د ورک سوي پاکټونو احتمال کله چې په نيټورک کي ډير بيروبار وي.

Uptime Monitors: د اپټايم مانيټرونه د دې لپاره کارول کيږي چې ډاډ ترلاسه سي چې د نيټورک وسايل لکه روټرونه ، سويچونه او سرورونه آنلاين دي او په غوره توګه کار ترسره کوي. د اپټايم نظارت وسيلې د نيټورک د وسيلو د شتون څخه د ډاډ تر لاسه کولو او مديرانو ته خبر ورکوي که چيرې يوه وسيله آفلاين سي يا شتون ونلري. د اپټايم څارني وسيلې کولای سي د هارډوير يا سافټوير لخوا رامنځته سوي د نيټورک ستونزې پيژندلو کي مرسته وکړي او کولای سي د خراب فعاليت يا ناکام وسيلو پيژندلو کي هم مرسته وکړي. دوی د وخت په تيريدو سره د نيټورک د وسيلو د فعاليت او وضعيت تعقيبولو لپاره هم کارول کېدای سي ، ترڅو د تکراري نيټورک مسلو پيژندلو کي مرسته وکړي.

Bandwidth Analyzers: د بانډ ويت تحليل کونکي د نيټورک د ترافيک د نظارت او تحليل لپاره کارول کيږي ترڅو د ترافيک کارولو patterns وپيژني ، د بينډ ويت کارول وڅاري او د نيټورک فعاليت اصلاح کړي د بانډ ويت شنونکي کولای سي له مديرانو سره د خنډونو په پيژندلو کي مرسته وکړي، د ترافيک لومړيتوب پاليسی پلي کړياو د QoS

(Quality of Service) اداره کړي. د بينډ ويت شنونکي معلومات تحليلوي لکه د نيټورک پروټوکولونه، سرچينې، د هدف ادرس او د پورټ شميره ترڅو د بينډ ويت کارونې Patterns وپيژني او د شبکې عمومي فعاليت کې بصيرت رامنځته کړي. دوی کولای سي له مديرانو سره د احتمالي امنيتي مسلو په پيژندلو کي هم مرسته وکړي، لکه د DDOS بريدونه او د ترافيک غير معمولي نمونې وپيژني چي ممکن نيټورک ته احتمالي غير مجاز لاسرسي په ګوته کړي.

Log File Analyzers: د لاګ فايل تحليل کونکي د نيټورک د وسيلو لخوا د رامنځته سوي لاګ فايلونو د نظارت کولو لپاره کارول کيږي ، لکه روټرونه ، سويچونه او سرورونه.

Log File Analyzers د نيټورک د فعاليت د تحليل کولو ، د سيستم غلطيو پيژندلو او د ستونزو حل کولو دندې ترسره کولو لپاره هم استعماليږي.

د لاګ فايل تحليل کونکي کولای سي له مديرانو سره د مسلو پيژندلو کي مرسته وکړي لکه د سافټوير يا هارډوير ناکامي ، د نيټورک بنديدل او د هيکرانو بريدونه. دوی کولای سي د مشکوکو پيښو په پيژندلو او د امنيتي مسلو پيژندلو کي هم مرسته وکړي لکه د غير مجاز لاسرسي هڅي يا د سيستم لاګونو کي غير متوقع بدلونونه. د لاګ فايل تحليل کونکي د نيټورک د وسيلو څخه د راټولي سوي لاګ ډيټا په تحليل کولو سره کار کوي.

د نيټورک څارني سيستمونه د سازمانونو لپاره خورا مهم دي ترڅو ډاډ ترلاسه کړي چي د دوی کمپيوټري زيربناوې او شبکه په اسانی او اغيزمنه توګه کار کوي. د نيټورک څارني سيستمونه د نيټورک فعاليت ته بصيرت ورکوي، د نيټورک امنيت ته احتمالي ګواښونه مسولينو ته ورپيژني او د نيټورک د مسلو سمدستي حل کول اسانه کوي.

2- Security monitoring systems : د امنيت د څارني سيستمونه د دې لپاره ډيزاين سوي دي چي کله کوم شکمن يا غير مجاز فعاليت په ځانګړي ځای يا ملکيت کي پيښيږي نو دا سيستمونه يې کشف کړي او مسوولينو ته خبرتيا ورکړي. په دې وسايلو کي امنيتي کيمرې، د حرکت کشف کونکي، الارمونه، د لاسرسي کنټرول سيستمونه او د بايومتريک تصديق کولو وسايل شامل دي. د دې سيستمونو لومړنی دنده د غلا او غلا امکانات کمول، د ورانکاری کمول او د کوم جرم په صورت کي چارواکو ته شواهد وړاندي کول دي. د امنيت څارني سيستمونه په مختلفو ترتيباتو کي کارول کيږي، لکه د استوګنې کورونه، سوداګريز ځايونه، عامه ځايونه او دولتي تاسيسات. دوی په مختلفو ځايونو کي د امنيت په ښه کولو او د جرمونو د کچي په کمولو کي اغيزمن ثابت سوي دي.

3- Server monitoring systems : د سرور نظارت سيستم يوه وسيله ده چي د سرور يا سرورونو فعاليت او روغتيا څارنه او اداره کولو لپاره استعماليږي. دا د سرورونو او اپليکيشنونو مناسب فعاليت ډاډمن کولو لپاره يو مهم سيستم دی دا سيستمونه نه يوازي د احتمالي ستونزو او د دوی د لاملونو په پيژندلو کي مرسته کوي بلکي د ورته مسلو د حل لپاره وړانديزونه هم وړاندي کوي. د سرور د څارني سيستم ګټې: 1. د سرور فعاليت ښه کوي: کله چي يو سازمان د سرور څارني سيستم ولري نو کولای سي چي په ريښتيني وخت کي د سرور فعاليت تعقيب او تحليل کړي او کله چي د سرور په فعاليت کي کومه ستونزه رامنځته کيږي نو دا سيستم کولای سي د IT ټيم ته خبر ورکړي. دا سيستمونه سازمانونه ته د دې توان ورکوي چي د احتمالي ستونزې ساحې وپيژني او اصالح يې کړي مخکي له دې کوم تاوان پيښ کړي 2. د سازمانونو د خدماتو د بنديدو وخت کموي: د څارني سيستمونه سازمانونو ته دا توان ورکوي چي په فعاله توګه احتمالي مسلې په ګوته کړي، کوم چي د سازمانونو د خدماتو د ځنډ وخت کموي او د هري پيښې مخه نيسي چي کېدای سي د معلوماتو ضايع کيدو، عوايدو ضايع کيدو او شهرت ته زيان رسيدو لامل سي 3. د لګښت سپما: د سرور څارني سيستمونه سازمانونو ته وړتيا ورکوي چي مخکي له مخکي د Upgrade او د سيستم د ظرفيت اړتيا اټکل او پلان کړي، کوم چي د غير پلان سوي، قيمتي Upgrade خطر کموي او د هارډوير عمر زياتوي. 4. د امنيت زياتوالی: د سرور څارني سيستمونه د IT ټيم ته اجازه ورکوي چي د مخکينی ټاکل سوي امنيتي پاليسيو په وړاندي د سرور فعاليت تعقيب کړي او هر ډول غير مجاز لاسرسی يا شکمن فعاليت کشف کړي. 5. ښه عکس العمل: د څارني سيستمونه له سازمانونو سره مرسته کوي چي د IT ټيم ته اجازه ورکړي چي د سرور لاګ تعقيب کړي، ذخيره يې کړي او راپور يې ورکړي تر څو په مؤثره توګه د هغو معيارونو چي د امنيت دپاره ټاکل سوي دي وڅاري په دې توګه د معلوماتو امنيت ډاډمن کېدای سي.

4- Application monitoring systems : د Aplication نظارت سيستمونه د هر هغې سوداګرۍ لپاره اړين دي چي د خپلو کارونو لپاره پر سافټويرونو باندې تکيه کوي دا سيستمونه د سوداګرۍ سره مرسته کوي

چې د دوی داپلیکیشنونو د فعالیت او روغتیا څارنه وکړي، دوی ته اجازه ورکوي چې مشکلات کشف او ځواب ورکړي مخکې لدې چې دا مشکلات پر سوداګرۍ اغیزه وکړي. د اپلیکیشن نظارت سیستمونو هدف د اپلیکیشن روغتیا او فعالیت ښه کول دي. په دې کې د سیستم مسلسل کار کول او د ځواب ویلو څارنه هم شامله ده او همدارنګه د سرچینو صحي کارول هم شامل دي لکه د CPU او میموري کارول.

هدف دا دی چې په اپلیکیشنونو کې مشکلات ژر تر ژره وپیژني او حل یې کړي تر څو د اپلیکیشن د ځنډ وخت کم کړي او د عاید او پیرودونکي رضایت له لاسه ورکولو مخه ونیسي.

د اپلیکیشن نظارت سیستمونه د سیستم ، اپلیکیشن او نیټورک څخه د معلوماتو په راټولولو سره کار کوي. دا ډاټا بیا د ګرافونو، خبرتیاو او ډشبورډونو په بڼه تحلیل او ښودل کیږي او سیستم احتمالي مسلې پیژني او د IT ټیم ته خبرتیا لیږي ترڅو دوی ژر تر ژره اقدام وکړي او ستونزه حل کړي. د څارني سیستم عموما په یو لوپ کې کار کوي چې لاندي مرحلې پکې شاملې دي:

1. د معلوماتو راټولول: لومړی ګام د مختلفو سرچینو لکه لوګو، میټریکونو او پیښو څخه د معلوماتو راټولول دي.

2. د معلوماتو لنډیز جوړول: کله چې معلومات راټول سي، دا په یوه مرکزي ځای کې پروسس او ذخیره کیږي.

3. د معلوماتو تحلیل: ډاټا بیا د مختلفو الګوریتمونو او تخنیکونو په کارولو سره تحلیل کیږي ترڅو Patterns وپیژني.

4. د ډیټا وړاندي کول: د ډیټا د تحلیل وروسته ډیټا د ډشبورډونو ، Notifications له لاري IT ټیم ته وړاندي کیږي

5- Environmental monitoring systems: د چاپیریال د څارني سیستمونه د چاپیریال د مختلفو اړخونو لکه د تودوخې، رطوبت، د هوا کیفیت، د اوبو کیفیت، وړانګو او شور کچه اندازه کولو او ثبتولو لپاره کارول کیږي. دا سیستمونه عموما په صنعتي، روغتیایي، تعلیمي او څیړنې ترتیباتو کې کارول کیږي ترڅو د پروسو، تجهیزاتو او خلکو لپاره د چاپیریال غوره شرایط ډاډمن کړي.

نن ورځ په مارکیټ کې د چاپیریال د نظارت د سیستمونو مختلف ډولونه شتون لري. ځینې یې یوازې کار کوي او ځینې یې د نورو سیستمونو سره یو ځای کیږي تر څو د چاپیریال نظارت په ښه ډول تر سره سي.

دا چې کوم ډول سیستم باید استعمال سي دا په دې پوري اړه لري چې څومره دقیقه ډیټا په کار ده.

د تودوخې او رطوبت نظارت سیستمونه د چاپیریال نظارت سیستمونو ځینې عام ډولونه دي. دا سیستمونه په یوه خونه یا ودانۍ کې د هوا د تودوخې او رطوبت د څارلو لپاره کارول کیږي. دا سیستمونه عموما په صنعتي تاسیساتو، د ډیټا په مرکزونو او روغتونونو کې کارول کیږي ترڅو د تجهیزاتو او پروسو لپاره غوره شرایط ډاډمن کړي.

د تودوخې او رطوبت څارني سیستمونه ممکن په موزیمونو، آرشیفونو او نورو تاسیساتو کې هم وکارول سي چیرې چې د اثارو او اسنادو د ساتنې لپاره د چاپیریال کنټرول خورا مهم دی. کومو سازمانونو ته چې د کارمندانو خوندیتوب او روغتیا اړینه وي د هغو سازمانونو لپاره د هوا د کیفیت د څارني سیستمونه اړین دي(Kuo et al,. 2015).

پایله

د IP based monitoring systems په یو ټاکل سوي ځای کې د فعالیتونو یا پیښو څارلو لپاره کارول کیږي. دا د IP کیمرې کاروي چې په نیټورک کې د ویډیو سیګنالونه ګیروي او استوي. عکسونه بیا په سرور کې زیرمه کیږي ، کوم چې د انټرنیټ سره د وصلیدو سره له هر ځای څخه لاسرسی ورته کېدای سي. دا ډول سیستم د ریښتیني وخت د نظارت زمینه مور ته برابروي او معمولا د امنیت سکتور او همدارنګه په ګودامونو او تولیدي تاسیساتو کې کارول کیږي. د I IP based monitoring systems معمولا د دودیز انلاګ کیمرو په پرتله د لوړ ریزولوشن عکسونه اخلي، د دې سره په فوټیج کې د خلکو او شیانو پیژندل اسانه کیږي. ځینې سیستمونه د حرکت کشف ټیکنالوژۍ سره یو ځاي راځي، کاروونکو ته خبرداری ورکوي کله چې د دې سیستم په تر څار لاندي ساحه کې حرکت تر سره سي. دا ډول سیستم د پراخیدو وړ دی، سوداګریو ته دا اجازه هم ورکوي چې د اړتیا سره سم خپل سیستم په ډیرو ځایونو کې فعاله کړي. په ټوله کې، د IP based monitoring systems ستاسو په شاوخوا کې د څارني ساتلو، ستاسو د کور یا سوداګرۍ لپاره د خوندیتوب او امنیت لوړولو لپاره یو پیاوړی وسیله ده.

اخځليکونه

1. Bhatnagar, G., & Kumar, V. (2016). Survey of IP-based surveillance system. International Journal of Advanced Research in Computer Science, 7(5), 205-211.

2. Cheng, C. F., Chou, C. C., & Huang, P. C. (2017). Design and implementation of a real-time IP camera-based surveillance system. Journal of Intelligent and Fuzzy Systems, 33(1), 59-67.

3. Fisher, R., & Bolles, R. (2015). Real-time IP-based video surveillance. Proceedings of the AAAI Conference on Artificial Intelligence, 29(1), 1977-1983

4. Gashi, G., & Pirangutti, P. (2019). Analysis of IP-based surveillance systems. Journal of Sensors, 2019, 1-11

5. Ghazanfari, A., Adibniya, A., & Pourgharibshahi, M. (2016). IP-based surveillance system with human detection. IEEE Access, 4, 649-657.

6. Ghasemi, Z., Moarefdoost, M., & Khansari, M. (2018). A novel IP-based video surveillance system using deep convolutional neural networks. Computers & Electrical Engineering, 65, 419-427.

7. Kuo, C. P., Lin, Y. C., & Chen, T. H. (2015). Real-time IP-based video surveillance system using Hadoop architecture. Journal of Electrical and Computer Engineering, 1-9.

8. Kalbo, N., Mirsky, Y., Shabtai, A., & Elovici, Y. (2020). The Security of IP-Based Video Surveillance Systems. Sensors, 20(17), 4806. https://doi.org/10.3390/s20174806

8. Li, Y. K., Ma, Y., & Wang, C. Q. (2018). A novel IP-based real-time surveillance system with object tracking. Information Fusion, 36, 64-74.

9. Liu, J., Tian, J., Hu, Z., & Zhang, C. (2019). A distributed IP-based surveillance system for resource-constrained edge devices. International Journal of Distributed Sensors, 19(6), 1397.

10. Liu, H., Tang, C., Wu, S., & Wang, H. (2011). Real-time video surveillance for large scenes. https://doi.org/10.1109/wcsp.2011.6096963.

10. Näslund, M., & Olofsson, J. K. (2015). Evaluation of IP-based video surveillance systems. International Journal of Computer Networks & Communications, 7(2), 55-66.

11. Qian, Y., Hu, Y., Mao, W., & Liu, P. (2017). An IP-based intelligent surveillance system for railway environment. International Journal of Distributed Sensor Networks, 13(10), 1-8.

12. Shu, D., Zhang, L., Ge, L., & Tian, M. (2019). A novel IP-based surveillance system with automatic object size estimation. Measurement, 131, 450-458.

Sun, Y., Li, J., & Chen, H. (2016). A novel IP-based image .13 retrieval system for large-scale surveillance. Journal of .Visual Communication and Image Representation, 33, 15-24

IP Based Monitoring System Implementation

Khan Mohammad wafa*[1], Jamaludin Jamal[2] and Sayed Mohammad Adil[3]

[1,2,3]Department of Information Technology, Computer Science Faculty, Bost University, Email: Khan.jan363w@gmail.com

Abstract

د Ip based monitoring system in network یو ډول امنیتي سیستم دی چې د انټرنیټ پروتوکول (IP) کاروي ترڅو په یو شبکه کي د مختلف امنیتي وسیلو ترمنځ ډیټا واستول سي ، نوکاروونکو ته د ریښتیني وخت نظارت او تعقیب وړتیا ورکوي. دا ډول سیستم عموما د استوګنیاو سوداګریزو ترتیباتو کې د ننوتلو او وتلو ځایونو، خوندي محیطونو، او نورو حساسو سیمو د څارني او تعقیب لپاره کارول کیږي. د Ip based monitoring system in network یوه لومړنی ګټه د لوړ کیفیت ویډیو فوټیج او عکسونو چمتو کولو وړتیا ده چې د انټرنیټ د وصلیدو سره د هرې وسیلې له لاري د لیري ځاي څخه لاسرسی ورته کیدی سي. که مالک د خپلي ودانی څخه لیري هم وي د دې سیستم په واسطه د ودانی دوامداره څارنه کولي سي د Ip based monitoring system in network بله ګټه اندازه کول دي. ډیری کیمرې او سینسرونه سیستم ته اضافه کیدی سي، او که چي یو پیښه واقع سي نو هر وسیله کولی سي ټاکل سوي پرسونل ته خبرتیا واستوي، لکه سیستم ته غیرقانوني لاسرسی یا د سیستم د غړو د حرکت کشف. سربیره پردې د Ip based monitoring system in network اکثره د دودیز انلاګ سیستمونو په پرتله خورا ارزانه دي ځکه چي دا سیستمونه د موجوده انټرنیټ زیربنا کاروي او په اسانی سره د نورو امنیتي ټیکنالوژیو سره یوځای کیدای سي، لکه سیستمونو ته د لاسرسي کنټرول، د اور وژني سیستم او د خطر په وخت کي د خبر ورکولو سیستم.

کلیدي کلمې: Monitoring, Internet protocol, network

BOST

Academic & Research National Journal

Valume Issue Year

2 1 2023