[5] Chen, L., Hu, Y., Wang, R. et al. Green building practices to integrate renewable energy in the construction sector: a review. Environ Chem Lett 22, 751–784 (2024). https://doi.org/10.1007/s10311-023-01675-2
[6] Сардаров Я.Б., Аскерова Б.Г., Алиева Е.М., Алмамедова М.Г. Об Архитектуре Bıg Data Computıng. Наука, Образование, Общество: Актуальные Вопросы, Достижения И Инновации: Сборник Статей Iıı Международной Научно-Практической Конференции. – Пенза: Мцнс «Наука И Просвещение». –2021. – С. 20-24.
[7] Сардаров Я.Б., Иманова З.Б. Использование Больших Данных И Инструментов В Управлении Человеческими Ресурсами. Актуальные Вопросы Современной Науки И Образования: Сборник Статей Xıı Международной Научно-Практической Конференции. В 2 Ч. Ч. 1. Пенза: Мцнс «Наука И Просвещение». - 2021. - С. 77-79.
[8] Sipahi, Banu & SAAYI, Zabihullah. (2024). The world's first "Smart Nation" vision: the case of Singapore. Smart Cities and Regional Development (SCRD) Journal. 8. 41-58. 10.25019/dvm98x09.
[9] Sadhukhan, Pampa & Banerjee, Sahali & Das, Pradip. (2021). Road Traffic Congestion Monitoring in Urban Areas: A Review. 10.1007/978-3-030-70183-3_8.
[10] Pavshe, Abhijit & Sawant, Ankita & Ghadage, Kishor. (2023). The Effect of Security and Privacy on the Internet of Things (IOT). International Journal of Advanced Research in Science, Communication and Technology. 8-12. 10.48175/IJARSCT-9362.

BULUD TEXNOLOGİYASINDA MƏXFİLİK VƏ TƏHLÜKƏSİZİK PROBLEMLƏRİ

Bayramova Qəmzə
Əliyeva Aytən
Azərbaycan Dövlət Neft və Sənaye Universiteti

Xülasə: Məqalədə bir çox müəssisələrin bulud hesablamalarını onun üstünlüklərinə və imkanlarına görə qəbul etdiyindən bəhs edilir. Ancaq bulud texnologiyasına keçid təhlükəsizlik narahatlığına gətirib çıxarır. Ehtiyatla istifadə edilən müasir texnologiyalardan biri də məhz bulud texnologiyasıdır. Bulud texnologiyasında güclü məlumat məxfiliyi təmin edilmir. Bunun üçün də məqalədə məlumat təhlükəsizliyini qorumaq üçün məlumatların saxlanmasının məxfiliyini təmin etməyin vacib olduğu müəyyənləşdirilmişdir.

Açar sözlər: Bulud təhlükəsizliyi, təhlükəsizlik məsələləri, məxfilik, xidmət olaraq proqram təminatı, xidmət olaraq platforma, xidmət olaraq infrastruktur

Giriş

İnternet müxtəlif texniki nailiyyətlərdə hərəkətverici quuvvə kimi rol oynayır və bu texniki nailiyyətlərdən biri də bulud hesablamaları (bulud texnologiyasıdır). İntenetə əsaslanan bulud hesablamaları ünsiyyət və saxlama üçün müəəyən təkliflər irəli sürür. O, internet üzərindən şəbəkələr, xidmətlət,, serverlər və proqramlar kimi resurslara daxil olmağa imkan verir və komputer xidmətlərinin göstərilməsini asanlaşdırır [1]. Şirkətlər bu resursları fizikin olaraq əldə etmək əvəzinə, ehtiyac yarandıqda hər istifadə üçün istifadə haqqını ödəyə bilir və daxil ola bilirlər. Getdikcə idarəetmə xərclərinə və vaxta qənaətə görə bulud hesablamaları daha cəlbedici seçimə çevrilir. Onun geniş şəkildə istifadə edilməsinin səbəblərinə çevik infrastrukturunu, girişinin sadəliyini və şəbəkə mərkəzli strategiyasının olmasını aid etmək olar.

Bulud xidməti istifadəçiləri əvvəlcədən hər hansı öhdəlik tələb olunmadan məhdud resurslarla başlaya bilərlər. Daha sonra tələb artdıqca imkanlar artırıla bilər. Bulud hesablamalarının giriş növünə görə 4 növü var: ictimai, hibrid, icma, şəxsi [2].

1.Şəxsi bulud: özəl müəssisələrin tətbiqinə aiddir ki, bu da məlumatların təhlükəsiz saxlanmasını təmin edir. Şirkət işçilərinə bəzən şəxsi bulud üçün əlçatanlılıq verilə bilər. Bunun da səbəbi

təhlükəsizlik problemlərinə görə uyğun icazələrin idarə edilməsidir. Şəxsi buludun əsas üstünlüyü yüksək təhlükəsizliyin olmasıdır. Şəxsi bulud daha çox həsas məlumatlar üzərində əlavə nəzarət və məxfiliyi qorumaq üçün yüksək məlumat təhlükəsizliyini tətbiq edir. Bundan əlavə, şəxsi buludun çatışmazlığı müəyyən avadanlıqların alışında və digər vacib ödənişlərlə bağlı yüksək xərclərin olmasıdır.

2. İctimai bulud: . İctimai bulud müəyyən resurslardan istifadə etmək istəyən yaxud almaq istəyən şirkətlət tərəfindən paylaşılan bulud hesablamalarının bir növüdür.Bu bulud növü bulud xidmətlərini təklif edən böyük korporasiyalar tərəfindən saxlanılır. Belə korporasiyalara nümunə kimi Amazon Web Xidmətlərini (AWS) göstərmək olar. İctimai bulud müəyyən resurslardan istifadə etmək istəyən yaxud almaq istəyən şirkətlət tərəfindən paylaşılan bulud hesablamalarının bir növüdür. İctimai buludda istifadəçi buludun saxlanması məsuliyyətindən azaddır. Burada xidmətin kəsilməsinə səbəb olan nasazlıq ehtimalı aşağıdır. Buna görə də ictimai bulud xidmətləri etibarlıdır. Ancaq ictimai buludun əsas çatışmazlığı məlumatların qorunması və məxfiliklə bağlı problemlərdir. Məlumatların ötürülməsiz zamanı və ya həssas məlumatlara girişdə nəzarət zəifdir. Bu təhlükəsizlik problemlırinə baxmayaraq, bəzi kiçik firmalar həssas məlumatlarla məşğul olduqları üçün ictimai bulud xidmətlərindən qazanc əldə edə bildilər.

3. İcma buludu: məqsədləri oxşar olan bəzi təşkilatların birlikdə sahib olduğu bulud mühitidir. Eyni zamanda bu təşkilatlar müəyyən tələblər üçün icma buludunda vahid platformadan istifadə edə bilirlər. Bu bulud növü şəxsi buludu xatırladır, ancaq burada dəstəkləyici infrastruktur və hesablama gücü təhlükəsizlik məqsədləri olan iki şirkətin nəzarətindədir. İcma buludu ictimai buluda nisbətən daha bahalıdır və burada məlumatlara giriş lazımi səviyyədə idarə olunmur.

4. Hibrid bulud: şəxsi və ictimai bulud xidmətlərinin birləşdirir. Həmçinin ikidən çox bulud provayderlərinin əhatə edir. Buna görə də iki və daha artıq hesablama platformasında koordinasiya, idarəetmə və əlçatanlığın hamısı hibrid buluda daxildir. Buna əsasən təşkilatlar heç bir məlumatı təhlükəyə atmadan və kənar tərəflərə açıqlamadan ictimai buludun iqtisadi səmərəliliyindən istifadə edə bilər. Digər növlərə nisbətən təşkilatlara daha çox sərbəstlik verir. Hibrid bulud təhlükəsizlik məhdudiyyətlərinə malikdir. Eləcə də burada həssas məlumatlatların sızması halları da baş verə bilər. Bu problemin həll üsullarından bir də bulud resurslarına girişə nəzarət etməkdir.

Bulud yerləşdirmə üsulları vasitəsilə müəyyən təşkilatların arasında istifadəçi məlumatlarının paylaşılması mümkündür. Ancaq bu zaman bəzən icazəsiz məlumatların dəyişdirilməsi kimi hallar baş verir. Bu halların qarşısını almaq üçün hər bir təşkilat məlumatların bütövlüyünə və məxfiliyinə diqqət etməlidirlər. Məlumatların bütövlüyünü yalnız məlumatları şifrələməklə təmin etmək olmur. Bu səbəbdən də bulud texnologiyasından istifadə etmək istəyən istifadəçilər təhlükəsizlik və məxfilik problemlərinə görə narahat olurlar. Bu problemlərlə bağlı 2008-ci ilin avqustunda 244 İT meneceri və onun həmkarlarının daxil olduğu İDC araşdırmasında təhlükəsizlik ən əsas problem olaraq müəyyən edildi. Ümumiyyətlə istifadəçi şəxsiyyətlərini qorumaq və məlumatları təhlükəsiz saxlamaq üçün bulud mühitində məxfilik məsələlərini həll etmək çox vacibdir.

Bulud hesablama modelləri

Bulud hesablamasının üç əsas modeli vardır: SaaS, PaaS, İaaS

İaaS ingilis dilindənn yaranmış " Xidmət olaraq infrastruktur" mənasını verir və fiziki resursların idarə edilməsinə aiddir. İaaS saxlama, hesablama, şəbəkə, əməliyyat sistemləri, yaddaş və verilənlər bazası kimi proqram təminatı təklif edərək məlumat mərkəzi infrastrukturunu əvəz edə bilir. Ümumiyyətlə, İaaS istifadəçilərə müəyyən proqramları və əməliyyat sistemlərini qurmağa imkan verir [3]. İaaS istifadəçilərə bəzi üstünlükləri verə bilir ki, bunlara da misal olaraq istifadəçilərin iş yüklərini daha sürətli, sadə və sərfəli etmək imkanları aiddir.

PaaS isə “ Xidmət olaraq platforma” kimi tərcümə edilir. PaaS hər bir müştəri üçün əlçatan olan və əvvəcədən quraşdırılmış proqram mərhələsidir. PaaS nümunəsi kimi Yahoo-nu göstərə bilərik. PaaS-n əsas məqsədi ilk növbədə məxfilik və həssas məlumatlar üzərində istənilən istifadəçinin nəzarətini artırmaqdır. Bunun üçün də istifadəçi məxfiliyinin köməyi ilə texnikalar və fərdiləşdirilə bilən prqram təminatı quraşdırılır.

SaaS “ Xidmət olaraq proqram təminatı” adlanır. Üçüncü tərəf provayderi müəyyən proqramlar hazırlayır və onları SaaS vasitəsilə müştərilərə onlayn şəkildə əlçatan edir. SaaS internet brauzeri ilə istənilən cihazdan tapşırıqları yerinə yetirə bilir. SaaS müştəri azadlığını təmin edir. Buna səbəb istifadəçilər əvvəlcə heç bir şey quraşdırmadan abunə vasitəsilə ödəniş edirlər.

Bulud hesablamada təhlükəsizlik problemləri

1. İcazəsiz giriş və məlumatların pozulması

Şirkət bulud şəbəkəsinə icazəsiz daxil olan və ya məlumatları köçürmək, ötürmək üçün bəzi proqramlardan istifadə edən hakerlərin hücumuna məruz qalır və məlumatların pozulması halları ilə tez-tez rastlaşa bilirlər. Qorunan və məxfi saxlanılan məlumatların pozulmasını icazəsiz kopyalama, baxılma, ötürülmə, dəyişdirilmə və oğurlama halları təşkil edir.

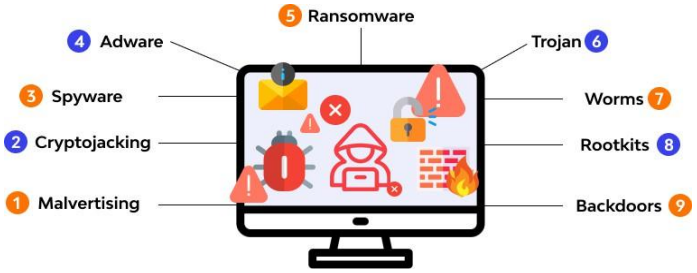
Təhlükəsizlik baxımından ən vacib təhdidlərdən biri məlumatların sızmasıdır [4]. Bunun səbəbi də bulud xidməti təminatçılarının bir neçə müştərinin məlumatlarını saxlamaq üçün eyni infrastrukturdan istifadə etməsidir.

2. Məlumatların itirilməsi, bərpası

Bulud hesablamasında məlumat itkisi təbii fəlakətlər, gözlənilməz hadisələr və aparat və ya proqram təminati ilə bağlı poblemləri nəticəsində baş verir. Bəzən belə hadislər təsadüfən baş verir, bunun üçün də fəlakətin bərpası və ehtiyat nüsxə prosedurlarının olması vacibdir. Bəzi təşkilatlar bulud vasitəsilə məlumatların ötürülməsini imtina edirlər, çünki digər sistemlərlə əlaqə saxlayan zaman məlumatların təhlükəsizliyi yoxdur [5].

3. Haker təhlükələri və zərərli proqram

Zərərli proqram istənilən komputer təhlükələrini təsvir edən bir termindir. Haker hücumları yaxud zərərli proqram hücumçuya hədəf maşın (komputer) üzərində tam və ya qismən nəzarət imkanı verir.



Şəkil 1. Zərərli proqram növləri

Şəkil 1-dən də göründüyü kimi bulud hesablamalarında təhlükə yaradan zərərli proqramların bir neçə növləri var.

- Trojan: Etibarlı fayllarda özünü gizlədən virusdur. Faylların istifadəsi zamanı isə böyük fəsadlara gətirib çıxarır.
- Spyware: kompüterə daxil olmaq, haqqımızda məlumatları toplamaq və üçüncü tərəfə razılığımız olmadan ötürmək üçün nəzərdə tutulmuş zərərli proqramdır.

- Backdoor: sistemin təhlükəsizlik mexanizmlərindən kənara çıxan komputer sistemlərinə və şifrələnmiş məlumatlara daxil olmaq üçün vasitədir. İstənilən bir developer bir backdoor yarada bilər ki, data problemlərini arada qaldıra bilsin və yaxud digər məqsədlər üçün istifadə edə bilsin.

4. Daxili təhlükələr və imtiyazlı istifadəçinin sui-istifadəsi

Bulud hesablamaları təhlükələrinə zərərli insayderlər, sındırılmış istifadəçi hesabları və s. aid edilə bilər. Zərərli insayderlər məqsədyönlü şəkildə təhlükəsizlik seçimlərini səhv təyin edə və ya təhlükəli faylları yükləyə bilərlər.

Bulud arxitekturasında daha yüksək imtiyazlara malik olan istifadəçilərə imtiyazlı istifadəçilər deyilir. Bu istifadəçilərə sistem adminstratorları, inzibati hüquqlara malik səlahiyyətli istifadəçilər aid ola bilər. İmtiyazlı istifadəçilər təhlükəsizlik tədbirlərini söndürməklə, vacib elementləri səhv konfiqurasiya etməklə bulud xidmətlərinə müdaxilə etmək imkanına malikdirlər. Belə xidmətlərin dayandırılması pul itkisinə və müştərilərin nüfuzuna xələl gətirilməsinə səbəb ola bilər [4].

Bulud hesablamalarında məxfilik məsələləri

1. Məlumatın məxfiliyi ilə bağlı narahatlıqlar

Məxfilik problemləri bulud mühitinə görə dəyışır: şəxsi məlumatların qanuni tələblərə əsasən işlənməsinə kim cavabdehdir; buludda saxlanarkən istifadəçilərin məlumatlarının oğurluğunun, icazəsiz satışın və pis istifadənin qarşısını necə almaq olar. Bu sadalananlar həll edilməli bulud xidmətinə daxil olan problemlərdir.

2. Verilənlərə nəzarətin olmaması

Təşkilatlar məlumatların buludlara köçürülməsi zamanı tez-tez nəzarətdən imtina edirlər. SaaS parametrində xidmət təminatçısı məlumatların saxlanılmasına nəzarətə cavabdehdir [6]. Nəzarətin olmamasına təsir edə biləcək bir neçə element:

- Fərdiləşdirmə və konfiqurasiya: Bizneslər tez-tez bulldan istifadə edən zaman bulud provayderlərinin infrastrukturu daxilində işləyirlər, bu isə onların əsas ehtiyaclarını ödəməyə görə ətraf mühiti fərdiləşdirmək imkanını məhdudlaşdırır.
- Məlumat təhlükəsziliyi: Bulud texnologiyasında bir çox təhlükəsizlik tədbirləri olsa da, istifadəçilər kənar şəxslərin məlumatlara icazəsiz girişindən və ya məlumatların itirilməsindən narahat olurlar.

3. Məxfilik qaydalarına uyğunluq

Bulud hesablamalarından danışdıqda,həssas məlumatların qorunması üçün məxfilik qaydalarına uyğunluq mühüm amildir. Bulud hesablamasının məxfilik qanunlarına uyğun olması üçün aşağıdakı amilləri qeyd etmək olar:

- Bulud xidmətinə uyğun provayderin seçilməsi: İlk öncə xidmət təminatçısının məxfilik qanunlarına uyğun olmasını nəzərə almaq lazımdır. Provayderlərin təhlükəszilik tədbirləri, məulmatların qorunması və məxfilik ilə bağlı müqavilələri araşdırılmalıdır. Həmçinin xidmət təminatçısının (CSP) qaydalara uyğun olaraq məlumatları qorumaq üçün təhlükəsizlik tədbirlərindən istifadəsi yoxlanmalıdır.
- Məlumat təhlükəsizliyi və insidentlərə cavab: Buludda şəxsi məlumatlara icazəsiz girişin, onların itirilməsinin qarşısını almaq üçün təhlükəsizlik tədbirləri görülməlidir. Bulud provayderləri əməkdaşlıq zamanı məlumat pozuntuları üçün insidentlərə cavab prosedurları işlənib hazırlanmalıdır.

Məlumatların Emalı Müqavilələri: Bulud provayderləri vasitəsilə məlumatların qorunmasına (DPA) və ya verilənlərin emalı müqaviləsinə (DPA) düzəliş edilməlir.

Buludda Məxfilik və Təhlükəsizlik tədbirləri

Bulud hesablamasında məlumatların qorunması, onların əlçatanlığı, bütövlüyü və məxfiliyi üçün müəyyən tədbirlər görülür.

1) Şifrələmə texnikaları, protokollar

Buludda saxlanılan məlumatların, eləcə də müştəri ilə bulu provayderləri arasında ötürülən məlumatların təhlükəsizliyi və məxfiliyi üçün şifrələmə üsulları və protokollardan istifadə edilir[8].

-Yaddaşın şifrələnməsi: Bulud sistemlərində məlumatların qorunması üçün tez-tez şifrələmədən istifadə edilir. Məsələn Advanced kimi üsullardan istifadə ilə məlumatlar diskdə saxlanmazdan əvvəl şifrələnir. Eyni zamanda bulud provayderləri şifrələmə açarlarını idarə edirlər, ancaq müştərilər öz açarlarını idarə etməyi seçə bilərlər.

-Tranzit şifrələmədə məlumat: Müştəri ilə bulud provayderləri arasında təhlükəsiz şəkildə əlaqə yaratmq üçün SSL/TLS kimi şifrələmə üsullarından istifadə edilir. Məlumatların ötürülməsi zamanı bu protokollar manipulyasiyanın və icazəsiz müdaxilənin qarşısını alaraq onları şifrələyir. HTTPS protoku da təhlükəsiz onlayn əlaqə yaratmaq üçün istifadə edilir.

-Verilənlər bazasının şifrələnməsi: Müəyyən sahələr yaxud sütunlar, hətta verilənlər bazasının şifrələnməsi Şəffaf Məlumat Şifrələmə (TDE) və ya sütun səviyyəli şifrələmə kimi üsullardan istifadə ilə həyata keçirilir.

-Açarların idarə edilməsi: Açar idarəetmə tez-tez bulud provayderlıri tərəfindən təmin edilir, bu isə müştərilərə açarlarını idarə etməyə və təhlükəsiz saxlamağa imkan verir. Şifrələnmiş məlumatların təhlükəsizliyi üçün açarların dügün idarə edilməsi vacibdir.

2) Doğrulama mexanizmləri və giriş nəzarətləri

Bulud hesablamasında giriş məhdudiyyətləri və autentifikasiya əsas komponentlərdir[9]. Bu komponentlərə aid aşağıda bəzi nümunələr verilmişdir:

-Rol əsaslı giriş nəzarəti (RBAC): Buludda RBAC əvvəlcədən təyin olunmuş rollara görə giriş imtiyazları və icazələr vermək üçün istifadə edilir. RBAC adminstratorlara istifadəçi girişini idarə etməyə imkan verir və miqyaslı giriş məhdudiyyətlətini idarə etməyi asanlaşdırır.

-Multi-faktor Authentifikasiya (MFA):Bulud xidmətlərinə daxil olmazdan əvvəl MFA əlavə qoruma təbəqəsi təklif edir ki, bu zaman istifadəəçilər şəxsiyyətin bir neçə formasını verməyə məcbur olur. Doğrulama təhlükəsiziliyini inkişaf etdirmək üçün tez-tez SMS- əsaslı kodlar, autentifikasiya proqramları yaradılır.

3) Təhlükəsizlik auditləri və qiymətləndirmələri

Təhlükəsizlik auditləri və qiymətləndirmələri dedikdə, təşkilatın sistemlərinin, şəbəkələrinin və ya buludda təhlükəsizlik nəzarətlərinin, zəifliklərin nəzərdən keçirilməsi başa düşülür. Təhlükəsizlik auditləri mövcud təhlükəsizlik mexanizmlərinin və nəzarət vasitələrinin hərtərəfli araşdırılmasını tələb edir. Onlar mümükün qüsurları aşkar etmək, təhlükəsizlik siyasətləri və qaydalara uyğunluğu təmin etmək üçün həyata keçirilir. Təhlükəszilik auditinin mühüm xüsusiyyətləri:

- giriş nəzarətinin auditi
- məlumatların mühafizəsi auditi
- infrastrukturun qiymətləndirilməsi
- insidentlərə cavab auditi

Zəifliyin qiymətləndirilməsi buludda, şəbəkədə və proqrmlarrda qüsurların aşkar edilməsini və təhlilinin tələb edir. Bu prosedur müəyyən addımlardan ibarətdir:

- skanlama və qiymətləndirmə,
- risklərin prioritetləşdirilməsi (aşkar edilmiş zəifliklərin dərəcəsinin qiymətləndirilməsi),
-nüfuz testi.

4) Məlumatların ehtiyat nüsxəsi və fəlakətin bərpası

Bulud hesablamasında hər hansı bir hadisə zamanı ehtiyaat nüsxə və fəlakətlərin bərpası məlumatların mövcudluğunu, işin davamlılığını təmin etmək, fasilələrin təsirini məhdudlaşdırmaq üçün vacibdir. Bulud əsaslı ehtiyat nüsxə və bərpa yerli sistemlərdən daha ucuzdur, son dərəcə təhlükəsiz və etibarlıdır.

Nəticə

İT sektorunda bulud hesablamaları sərfəli xidmətlər təklif edərək real paradiqmaya çevrilib. İnternet üzərindən mövcud resurslara daxil olmaq və onlardan istifadə etmək üçün artan tələbatı ödəməyə görə çoxdilliliyi dəstəkləyir. Bununla belə, bulud texnologiyası ciddi təhlükəszilik və məxfilik problemlərini ortaya qoyur. Bu məqalədə bulud hesablamaları ilə bağlı əsas fikirlər və təhlükəszilik məsələləri qeyd edilmişdir. Bulud hesablamalarında təhlükəszilik və məxfilik məsələləri bulud istifadəçilərinin buluddan istifadə edərkən yaranacaq problemləri azaltmaq üçün nəzərdə tutulub. Bunun əsasında bulud təhlükəsiziliyi və məxfilik sahəsində tədqiqatların gələək istiqamətlərinə təsir göstərmək mümkün ola bilər.

Ədəbiyyat

[1]. S.Abdullah və k.Əzmi, " Hesablamada Təhlükəszilik və Məxfilik Problemləri", 2018, Bulud Noyabr https//doi.org/10.1109/cr.2018.8626872.

[2] W. Kong, Y. Lei və J. Ma, "Bulud hesablamalarında məlumat təhlükəsizliyi və məxfilik informasiya problemləri," Beynəlxalq Hesablama Elmləri və Mühəndislik Jurnalı, cild. 16, yox. 3, səh. 215, 2018, doi: https://doi.org/10.1504/ijcse.2018.091772.

[3] YS Abdulsalam və M. Hedabou, "Security and Privacy in Cloud Computing: Technical Review," cild. 14, yox. 1, səh. 11–11, dekabr 2021, doi: https://doi.org/10.3390/fi14010011.

[4] R. Barona və EAM Anita, "Bulud hesablama təhlükəsizliyində məlumatların pozulması problemlərinə dair sorğu: Problemlər və təhdidlər," 2017 Beynəlxalq Konfrans Circuit, Power and Computing Technologies (ICCPCT), aprel 2017, doi: https:/ /doi.org/10.1109/ iccpct.2017.8074287.

[5] A. Narang və D. Gupta, "A Review on Different Security Issues and Challenges in Cloud Computing," IEEE Xplore, 01 sentyabr 2018-ci il. https://ieeexplore.ieee.org/ abstract/document/8675099.

[6] OO Aldawibi, MA Sharf və MM Obaid, "Cloud Computing Privacy: Concept, Issues And Solutions," İyul 2022, doi: https://doi.org/10.1109/isiea54517.2022.9873688.

[7] Pahalage Dona Thuhari, "Mövcud təhlükəsizlik və məxfilik problemləri və Əşyaların İnterneti (IoT) və Bulud Hesablamaları: Baxış," noyabr 2022, doi: https://doi.org/10.1109/ icccis56430.2022.10037730.

[8] I. Gupta və başqaları, Şifrələmə alqoritminin hibridləşdirilməsini tətbiq etməklə bulud saxlamada məlumat təhlükəsizliyi toplusu, 2022. doi:10.36227/techrxiv.20306157.

[9] AR Khan və LK Alnwihel, "A brief review on cloud computing autentication frameworks," Engineering, Technology & Applied Science Research, vol. 13, yox. 1, səh. 9997–10004, 2023. doi:10.48084/etasr.5479.

[10] NK Neeraj və digərləri, "Ethereum Blockchain istifadə edərək Multi-bulud mühitində xidmət səviyyəsində razılaşma pozuntusunun aşkarlanması," 2023 Şəbəkə və Kommunikasiya üzrə Beynəlxalq Konfrans (ICNWC), 2023. doi:10.1109/icnwc57852.2023.101.

[11] K. Almarhabi, A. Bahaddad, and A. Mohammed Alghamdi, “Security Management of BYOD and cloud environment in Saudi Arabia,” Alexandria Engineering Journal, cild. 63, səh. 103–114, 2023. doi:10.1016/j.aej.2022.07.031.
[12] MM Hafiz və FH Mohd Əli, "Evdəki simsiz LAN şəbəkəsində kobud güc hücumunun profilləşdirilməsi və azaldılması," 2014 Beynəlxalq Hesablama Elmi və Texnologiyası Konfransı (ICCST), Kota Kinabalu, Malayziya, 2014, səh. 1-6, doi: 10.1109/ ICCST.2014.7045190.

REVOLUTİONİZİNG PATİENT CARE: THE POWER OF .NET İN CLİNİC MANAGEMENT

Sattarova Gulshan
Rahimova Nazila
Azerbaijan State Oil and Industry University

Abstract
In today's fast-paced world, technology plays a pivotal role in enhancing various aspects of our lives, including healthcare. With the advent of innovative solutions, managing a clinic has become more efficient, streamlined, and patient-centric than ever before. Among these solutions, applications developed using the .NET framework stand out for their versatility, robustness, and scalability.
Keywords : Clinic management software, Healthcare technology, Patient care, Digital health, Electronic health records (EHR), Performance optimization, Data management, Reporting and analytics, Integration capabilities,Patient records management,Billing and invoicing,Disease prediction.

Introduction

Understanding the Need for Clinic Management Software

Clinics, regardless of their size, face a myriad of challenges in day-to-day operations. From appointment scheduling and patient records management to inventory tracking and billing, there's a multitude of tasks that require meticulous attention and organization. Traditional pen-and-paper methods are not only time-consuming but also prone to errors, leading to inefficiencies and potential risks to patient care. This is where clinic management software steps in. By digitizing and automating routine tasks, such software enables clinics to operate more smoothly, allocate resources efficiently, and ultimately deliver better patient outcomes. However, not all software solutions are created equal, and the choice of technology stack plays a crucial role in determining the effectiveness and reliability of the application.

Addressing Healthcare Challenges with Technology

Clinics face a multitude of challenges in delivering efficient and effective care to patients. From managing appointments and patient records to conducting laboratory analyses and making accurate diagnoses, the demands on healthcare providers are ever-evolving. Traditional methods of clinic management often fall short in addressing these challenges, leading to inefficiencies and potential gaps in patient care.

The Power of .NET in Clinic Management

Developed by Microsoft, the .NET framework has emerged as a preferred choice for building robust, secure, and scalable applications across various domains, including healthcare. Here's why .NET is well-suited for clinic management software: