ღრუბლოვანი ტექნოლოგიები და უსაფრთხოების პრობლემები

გურამი ასანიშვილი

თ.ს.უ ზუსტ და საბუნებისმეტყველო მეცნიერებათა

ფაკულტეტის დოქტორანტი

ხელმძღვანელი: მანანა ხაჩიძე

თბილისი 2018

აბსტრაქტი

ღრუბლოვანი ტექნოლოგიების გამოჩენამ რადიკალურად შეცვალა ინფორმაციული ტექნოლოგიების ინფრასტრუქტურა, არქიტექტურა, პროგრამული უზრუნველყოსფის შემუშავების მოდელები და მისი მიწოდების ვარიანტები. ინფორმაციული ტექნოლოგიების ევოლუციური ნაბიჯები მეინფრეიმიდან სერვერი/კლინეტის მოდელისკენ ხოლო შემდეგ ღრუბლოვანი ტექნოლოგიებისკენ, რომელიც თავის თავში მოიცავს გრიდ ტექნოლოგიებსაც, Cloud ტექნოლოგიებში გამოიყენება ისეთი ტექნოლოგიები როგორიცაა: კომუნალური და ავტონომიური გამოთვლები, არქიტექტურის ინოვაციური განლაგეგები. ღრუბლოვან ტექნოლოგიებზე სწრაფმა გადასვლამ წარმოშვა რიგი უსაფრთხოების პრობლემები, რისკები და გამოწვევები, რის შედეგადაც ტრაციციული დაცვის მექნიზმები უარესდება და ზოგჯერ უშედეგო ხდება.

Abstract

The recent emergence of cloud computing has drastically altered everyone’s perception of infrastructure architectures, software delivery and development models. Projecting as an evolutionary step, following the transition from mainframe computers to client/server deployment models, cloud computing encompasses elements from grid computing, utility computing and autonomic computing, into an innovative deployment architecture. This rapid transition towards the clouds, has fuelled concerns on a critical issue for the success of information systems, communication and information security. From a security perspective, a number of unchartered risks and challenges have been introduced from this relocation to the clouds, deteriorating much of the effectiveness of traditional protection mechanisms

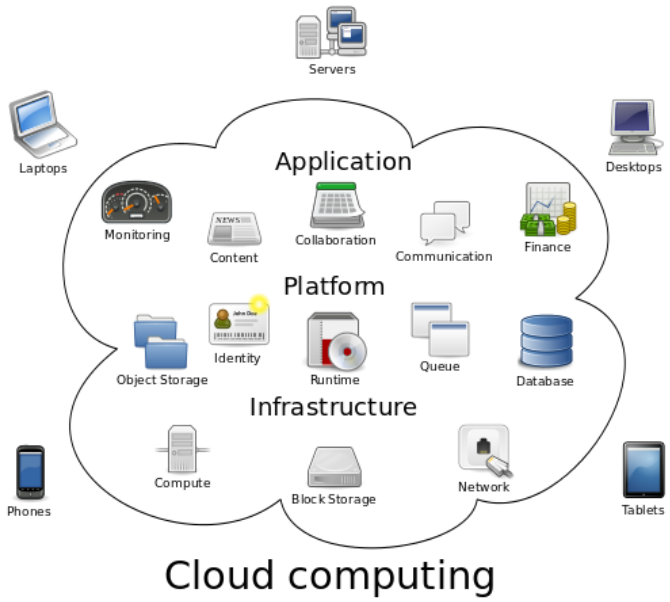
გასაღები სიტვები: ინფომაციული უსაფრთხოება, უსაფრთხოების პრობლემები, ღრუბლოვანი ტექნოლოგიები,ღრუბლოვანი ტექნოლოგიები და უსაფრთხოების პრობლემები

Keywords: Information security, Security problems , Cloud technology, Cloud technology and Security problems

რა არის ღრუბლოვანი ტექნოლოგიები?

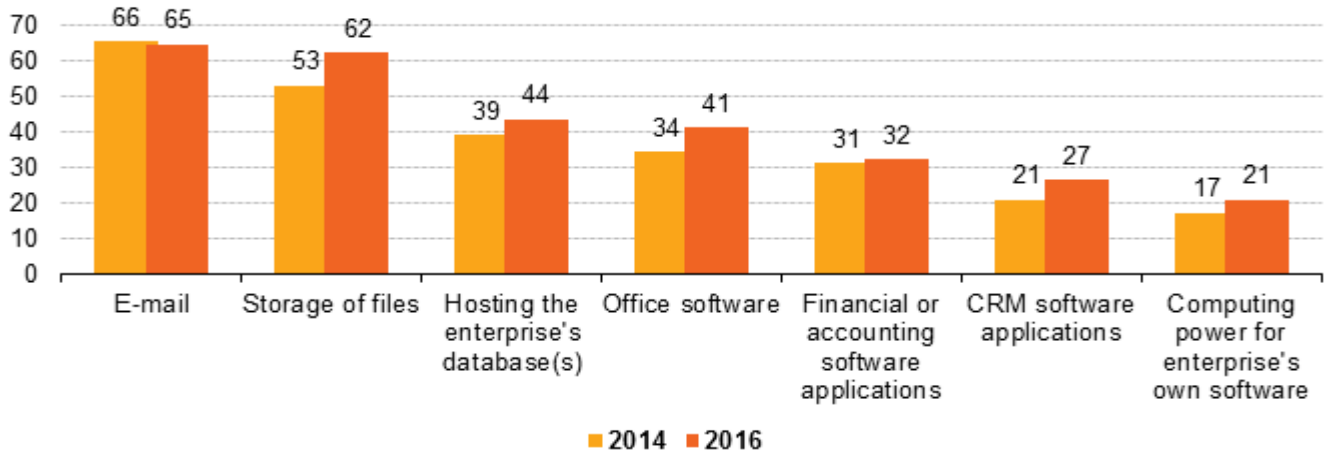
ღრუბლოვანი გარემო (cloud) ეს არის სერვერების ქსელი, სადაც ყოველ სერვერს აქვს განსხვავებული ფუნქცია. ღრუბლევანი ტექნოლოგიების ისტორია სათავეს იღებს 1963 წლიდან, როდესაც DARPA (the Defense Advanced Research Projects Agency) შეიმუშავა პროექტი რომლის თანახმად ერთი კომპიუტერის გამოყენება უნდა შეძლებოდა 2 ან რამდენიმე მომხმარებელს ასევე მათ გამოიყენეს სიტყვა ვირტუალიზაცია, რომელიც აღნიშნავდა თანამადროვე ვირტუალიცაისს საწყის იდეებს. პროექტი თანდათან განვითარდა და 21 საუკუნეში მიაღწია დიდ წარმატებას.

ღრუბლოვანი ტექნოლოგიების ძირითადი იდეა მდგომარეობს იმაში, რომ ზოგიერთ სერვერზე შესაძლოა გაშვებული იყოს აპლიკაცია ან რაიმე მომსახურება და სერვისი. ღრუბლოვანი ტექნოლოგიების გამოყენებით საჭირო აღარ არის ცალკემდგომი აპლიკაცია ან სერვისი რომელიც გაშვებულია ყოველი მომხმარებლის კომპიუტერზე ცალცალკე. დამატებით ღრუბლოვანი გარემო საშუალებას გვაძლევს გავაზიაროთ ტექნოლოგიები და რესურსები ისე რომ მასზე დაშვება ჰქონდეს რამდენიმე მომხმარებელს. მომხმარებლის თვალსაზრისით ღრუბლოვანი გარემო არის შავი ყუთი, რომელსაც იგი მიმართავს მაგრამ არ იცის და არ აინტერესებს თუ რა ხდება ყუთის შიგნით. ღრუბლოვანი ტექნოლოგიების არჩევით ჩვენ შეგვიძლია გარკვეული ვალდებულებები გადავიტანოთ სხვა გარემოში, რაც ბიზნესის უკეთ მართვის საშუალობას მოგვცემს.



ადრეულ პერიოდში თითოეულ სერვისზე გამოყოფილი იყო თითო ფიზიკური სერვერი, შესაბამისად ყოველ მონაცემთა დამუშავების ცენტრში მუშაობდა ათასობით სერვერი,რომლებიც მოიხმარდნენ დიდ რესურსებს და დანახარჯებს. ღრუბლოვანი ტექნოლოგიების გამოყენებით კი ეს პრობლემა საგრძლობლად შემცირდა, დღესდღეისობით შესაძლებელია ერთ ფიზიკურ სერვერზე გაეშვას რამდენიმე ვირტულური სერვერი, რაც საშუალებას გვაძლებს მაქსიმალურად გამოვიყენოთ სერვერის ფიზიკური მახასიათებლები.

მსოფლიო სტატისტიკის მიხედვით ღრუბლოვანი ტექნოლოგიობი დღესდღეისობით ერთ-ერთ ყველაზე პოპულარულ გადაწყვეტილებად ითვლება მონაცემთა ცენტრებში მონაცემების მართვის და დამუშავების მეთოდოლოგიაში.



ღრუბლოვანი ტექნოლოგიების პოპულარობის მიზებებად შეძლება ჩაითვალოს შემდეგი უპირატესობები:

- ვირტუალური მონაცემთა სანახის ცენტრი მომხმარებლებს საშუალებას აძლებს ჰქონდეთ წვდომა მონაცემებთან ნებისმიერი ადგილიდან, მაშინ როცა მონაცემთა სანხის ადგილმდებარეობას მნიშვნელობა არ აქვს;
- საეკსპლატაციო ხარჯების მაქსიმალურად შემცირების შესაძლებლობა;
- ვირტუალური სერვერები ხელს უწყობს სერვერების კონსოლიდაციას, რაც საშუაძლებას გვაძლევს გამიყენოთ რამდენიმე პოსტინგი ერთ ვირტუალურ მანქანაზე.
- გაუმჯობესებული მდგრადობა და მოქნილობა.

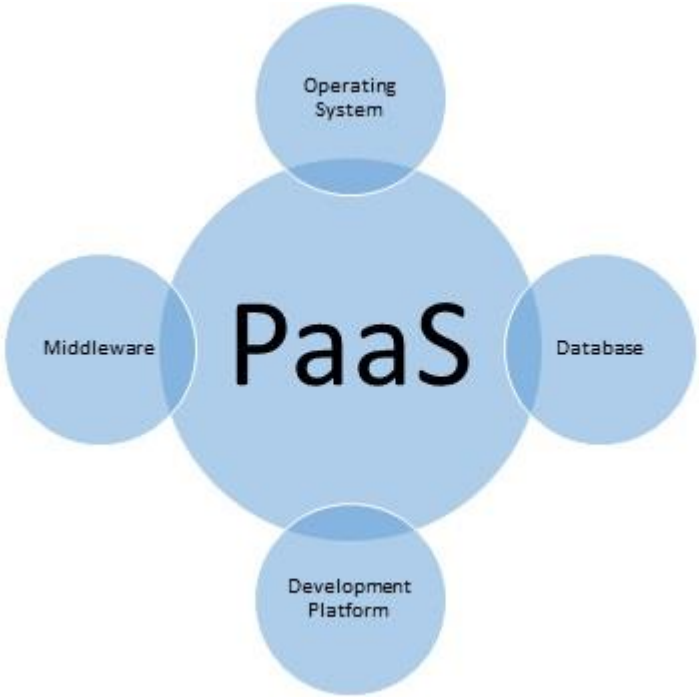
თანამედროვე კომპიუტერულ სისტემებში გამოიყენება სამი ტიპის ღრუბლოვანი გარემო: ღია, დახურული და პიბრიდული.

- ღია- ღია ტიპის ღრუბლოვანი გარემოში მომხმარებელს შეუძლია, ნებისმიმიერ დროს და ადგილიდან ინფორმაციაზე წვდომა
- დახურული- დახურული ტიპის ღრუბლოვანი გარემოს აქვს იგივე მახასიათებლები და ბენეფიტები რაც ღია ტიპისას , იმ გასხვავებით რომ დახურილი ტიპის გარემოში მომხმარებლების წვდომა შეზღუდულია.
- ჰიბრიდული- ჰიბრუდული ტიპის ღრუბლოვან გარემოში გაერთიანებული როგორც ღია ასევე დახურული ტიპის მახასიათებლები.

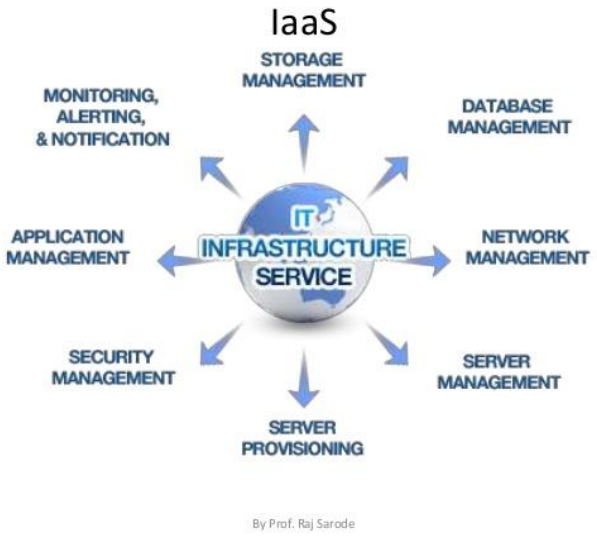
გარდა გარემოს ტიპებისა, ღრუბლოვან ტექნოლოგიებში არსებობს სერვისების მოდელები რომლებიც დიდ როლს თამაშობს. ძირითადად განისაძღვრება სამი ტიპის სერვისული მოდელი: Software as a Service (SaaS), Platform as a Service (PaaS) , Infrastructure as a Service (IaaS).

- Software as a Service (SaaS) - წარმოადგენს მექანიზმს რომლიც მდგომარეობს ღრუბლევან გარემოში არსებული პროვაიდერის აპლიკაციის გამოყენებაში. აპლიკაცია ხელმისაწვდომია პროვაიდერის სერვერებზე კლიენტის მხარეს არსებული რაიმე ინტერფესის სახით (მაგალითად web პორტალი). მომხმარებელი არ აკონტროლებს ბაზისურ ღრუბლოვან ტექნოლოგიას, ისეთი როგორიცაა ქსელთან კავშირი, ოპერაციული სისტემები, მონაცემთა სახები და ა.შ.

- Platform as a Service (PaaS) – ამ გარემოში შესაძლებელია პროგრამული ენების გამოყენება, ბიბლიოთეკების მართვა და ასევე პროგრამული უზრუნველყოფის შემუშავება, ისევე როგორც SaaS -ში აქაც მომხმარებელი არ აკონტროლებს ბაზისურ ღრუბლოვან ტექნოლოგიას, ისეთი როგორიცაა ქსელთან კავშირი, ოპერაციული სისტემები, მონაცემთა სახები და ა.შ.



- Infrastructure as a Service (IaaS)- წარმოადგენს მონაცემების სანახ სისტემას, დამუშავებას, ქსელის ინფრასტრუქტურას და სხვა გამოთვლითი რესურსების უზრუნველყოფას სადაც მომხმარებელი შეძლებს შეიმუშავოს, გაუშვას და განავითაროს მისი პროგრამული უზრუნველყოფა. მომხმარებელი არ მართავს ინფრასტრუქტურას, მაგრამ აქვს კონტროლი ოპერაციულ სისტემაზე და შეზღუდულად შეუძლია ქსელის კომპონენტების მართვაც.



ყველა ამ კომპონენტის გამოყენებით და საშუალებით თანამედროვე ინფორმაციული ტექნოლოგიებში ღრუბლოვანი ტექნოლოგიები უფრო დიდი პოპულარობით სარგებლობს და მისი გაყენების სტატისტიკაც მაღალია

ინფრასტრუქტურის უსაფრთხოება

ინფორმაციულ ტექნოლოგიებში რაც უფრო მაღალია რაიმე პროდუქტის გამოყენება, მით უფრო დიდა რისკი ინფორმაციული უსაფრთხოებისა. SaaS, PaaS და IaaS სერვის მოდელებში ძირითადა მოქმედებს სამი ტიპის უსაფრთხოების დონე: ქსელის, ჰოსტის და აპლიკაციის, რადგან ეს მოდელები უცხო არ არის შესაბამისად მათი მართვა გაადვილებულია. თითოეულ სერვისზე მოქმედებს კონკრეტული უსაფრთხოების დონე ამოცანის შესაბამისად.

ქსელის დონე

ქსელის დონის განხილვის დროს უნდა გავითვალისწინოთ ის რომ თუ რომელი ღრუბლოვანი ტექნოლოგიების ტიპი გამოიყენება ღია თუ დახურული. დახურილი ტიპის ქსელის დონის სტანდარტულ ტოპოლოგიაში არსებული საფრთხეები და რისკები არ შეცვლილა, ძირითად პრობლებას წარმოადგენს ღია ტიპის ღრუბლოვანი გარემო, სადაც ნებისმიერ მომხმარებელს შეუძლია მისი შეუზღუდავად გამოყენება.

ღია ღრუბლოვანი გარემო გარემოს გამოყენების შემთხვევაში არსებობს ოთხი ტიპის რისკი:

- მონაცემთა მთლიანობის და კონფიდენციალურობის დაცვა მისი ტრანზიტის დროს როგორც ღრუბლოვანი გარემოდან ასევე მის შიგნით;
- საიმედო წვდომის უზრუნველყოფა ყველა რესურზე, რომელსაც იყენებს მომხმარებელი;
- ინტერნეტზე ორიენტირებული რესურსების ხელმისაწვდომობის უზრუნველყოფა
- ქსელის მოდელების და დომენების დონეების შეცვლის შესაძლებლობა.

ჰოსტის დონე

PaaS და SaaS-ისგან განსხვავებით IaaS-ის კლიენტები პასუხისმგებლები არიან ჰოსტების უსაფრთხოების უზრუნველყოფაზე. გასათვალიწინებელია ის რომ თითქმის ყველა IaaS მომსახურეობა დღეისვის ხელმისაწვდომია ჰოსტის დონეზე.

IaaS-ჰოსტის უსაფრთხოება უნდა კლასიფიცირდებოდეს შემდგნაირად:

ვირტუალიზირებული ჰოსტის უსაფრთხოება: პროგრამული უზრუნველყოფა რომელიც იმყოფება იმაზე მაღლა ვიდრე ჩვეულებრივი აპარატურა, ყოველთვის იმყოფება კლიენტის მხრიდან საფრთხის ქვეშ,რადგან კლიენტს შეუძლია ვირტუალური ეგზემპლარების როგორც შექმნა ასევე განადგურებაც.

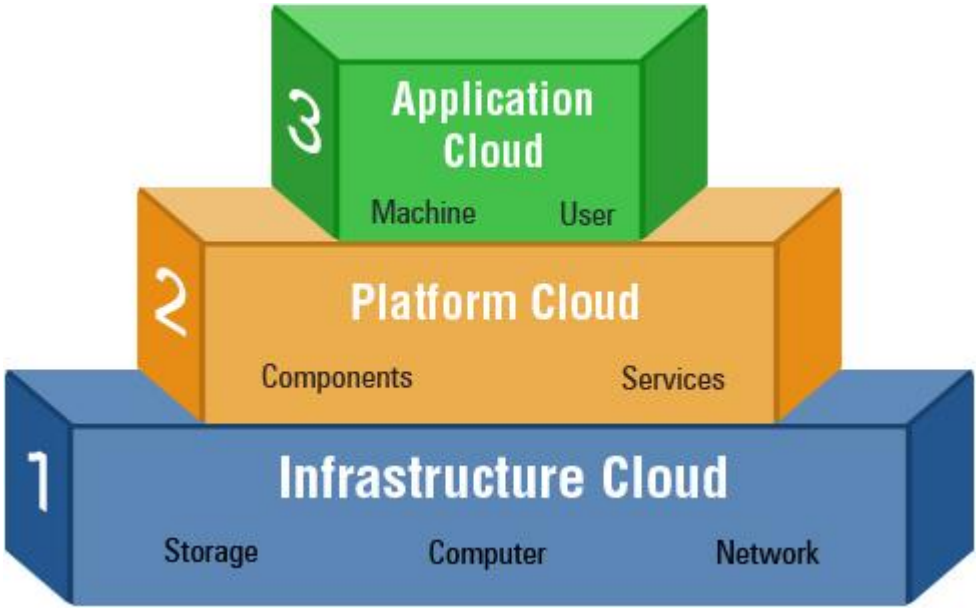
კლინეტის დროებითი OS ან ვირტუალური სერვერის უსაფრთხოება: ოპერაციულის სისტემის ვირტუალური ეგზემპლარი, რომელიც წარმოადგენს ვირტუალიზაციის ზედა ფენას ასახავს კლიენტის გემოვნებას თუ რომელი ოპერაციული სისტემა იყენებს იქნება ეს Linux, Microsoft თუ Solaris, შესაბამისად განსხვავებული ოპერაცილ სისტემბებს სჭირდებათ სხვადასხვა უსაფრთხოების მექანიზმები.

აპლიკაციის დონე

ნებისმიერ დაწესებულებაში თუ აპლოკაციის დონის უსაფრთხოება უნდა იყოს კრიტიკული. დღესდღეისობით ინფორმაციული უსაფრთხოების მექანიზმები საშუალებას გვაძლევს მაქსიმალურად მოვახერხეთ აპლიკაციის დონე, თუმცა ისიც აღსანიშნავია, რომ საფრთხეები დაცვის მიუხედავად იზდება და ვითარდება.

ინფორმაციის უსაფრთხოების საფრთხეები ღრუბლოვან ტექნოლოგიებში

მიუხედავად იმისა რომ ღრუბლოვანი გამოთვლები დღეს უკვე აღარ წარმოადგენს შედარეით ახალ ტექნოლოგიებს, ინფორმაციული უსაფრთხოების თვალსაზრისით მაინც რჩება სუსტ წერტილად. ტექნიკური თავისებურების გამო , რომელიც გამოყენება მის ასაგებად, შეიძლება განვიხილით რომ მასზე მოქმედებს ის ტანდართული საფრთხეები რაც სხვა ინფორმაციული ტექნელოგიების მიმართულებაში ეს განპირობებულია იმით რომ ღრუბლოვან ტექნოლოგიებში გამოიყენება კომპლექსური მიდგომა , რაც გულიხმოვს რამტენიმე ტექნოლგიის გაერთიანებას ისეთი როგორიცაა, სერვერული მხარე და ქსელის მხარე, რთული ურთიერთ ჩართვებით და დიდი მოცულობის ტრაფიკით, ხოლო რაც უფრო დიდია ტრაფიკი სააფრთხეც პროპორციულად იზრდება. როგორ უკვე ავღნიშნე ღწუბლოვანი ტექნოლოგიების არქიტექტურა სამი ურთიერთ დამოკიდებული ფენისგან შედგება ესენია: ინფრასტრუქტურა, პლატფორმა და აპლიკაცია.



ნებისმიერი ამ ფენებისგან შესაძლოა იყოს არამდრაგი პროგრამულად ან კონფიგურაციის შეცდომებისკენ, რომელსაც როგორც წესი უშვებს მომხმარებელი ან სერვისის პროვაიდერი. უფრო მეტიც ღია ტიპის მულტიდომენური და მრავალ მომხმარებლიანია სისტემები მსუყე ნადავლია პოტენციური ცუდისმსურველი მესამე პირებისთვის. ღრუბლოვანი სერვისები და ტექნოლოგიებზე მოქმედებს რამდენიმე ტიპის საფრთხე ისეთი როგორცაა: მონაცემთა მთიალობის დარღვევა, კონფიდენციალურობა და რესურსებზე წვდომა ისინი შესაძლებელია გახდნენე პლატფორმა სხვა უფრო საშიში შეტევებისა.

სხვა სერიოზული პრობლემა რომელიც ახლავს მონაცემების დაცვას Cloud-ში ეს არის კლიენტის მხრიდან ვერ ხერხდება სერვისევის აუდიტი და უსაფრთხოების მექანიზმების კონტროლი, მაგალითად ლოგ ფაილების შემოწმობა.

ვირტუალური მანქანები რომლებსაც Cloud ტექნოლოგიებში იყენებენ დინამიურია, შესაძლებელია მათი კლონირება და სხვა ფიზიკურ სერვერზე გადატანა. მსგავსი მოქმედება მოქმედებს მთლიან ინფორმაციულ უსაფთრთოებაზე , თუმცა უნდა აღინიშნოს რომ იმ ოპერაციული სისტემის სისუსტის გამოვლინება რომელსაც იყენებს ვიტუალური მანქანა ხდება დროთა განმავლობაში. ღრუბლოვან ტექნოლოგიებში მნიშვნელოვანია დაფიქსირდეს უსაფრთხოების სისტემების მდგომარეობა და იგი არ უნდა იყოს დამოკიდებული Cloud-ის ადგილმდებარეობაზე.

Cloud ტექნოლოგიებში არსებული საფრთხეებად შესაძლებელია განისაზღვროს შემდეგი:

- საერთო ტექნოლოგიური ხარვეზები: რესურსების გაზრდის გამო უმნიშვნელო შეტევაც შესაძლოა დიდ პრობლემად გადაიქცეს. მაგალითად ღრუბლოვანი გაზიარების სერვისები.
- მონაცემთა დარღვევა: იმის გამო რომ Cloud-ში დიდ რაოდენობით მონაცემები მოძრაობს, შესაბამისად იზდება ალბათობა იმისა რომ ამ მომაცემების მთლიანობა დაირღვეს.
- Denial of Service (DoS): ისევე როგორც სხვა გამოთვლითი სისტემებისთვის შეტევა მეტად აქტუალურია, რადგან მას კონკრეტული მიმართულებით შეტევის დროს შეიძელბა გათიშოს cloud სერვისები.
- საინექციო ხარვეზები: იგულისხება ისეთი დეფექტები და ხარვეზები რომელიც დამოკავშირებულია SQL-თან.
- ხელმისაწვდომობა- ღრუბლოვან ტექნოლოგიებში ერთ-ერთი მნიშვნელოვანია რომ სერვისები ხელმისაწვდომი იყოს ყოველთვის და ნებისმიერი ადგილიდან.

კონტრზომები და კონტროლი

თანამედროვე Cloud ტექნოლოგიებში გამოიყენება მსგავსი უსაფრთხოების და დაცვის მექანიზმებიც რაც სხვა ინფორმაციული ტექნოლოგიების მიმართულებაში, მხოლოდ იმ განსხვავებით, რომ Cloud ტექნოლოგიებში ეს მიდგომები კომპლექსურია, იმ მიზეზით , რომ Cloud გაერთიანებულია ქსელის ინფრასტრუქტურა, სერვერული ინფრასტრუქტურა , მონაცემთა სანახი სისტემები და ა.შ ყოველ მათგანს სჭირდება დაცვის ინდივიდუალური მიდგომა, მაგრამ საერთო ჯამში მაინც შეძლება ჩამოყალიბდეს ზოგადი დაცვის მექანიზმები. ესენია:

- End-to-end შიფრაცია: იმის გამო რომ მონაცემები შესაძლოა მოძრაობდნენ დიდი დაშორების ლოკაციებზე, აუცილებელია მთლიანი ტრაფიკი შიფრაცია მონაცემების უსაფრთხოდ გადაცემისთვის.
- მავნე პროგრამებზე სკანირება: End-to-end შიფრაციის გამო უსაფრთხოების ეკრანები ვერ კითხულობენ მონაცემებს და ვერ ამოწმებენ მათ საზიანოობას, შესაბამისად აუცილებელია მავნე პროგრამებზე სისტემის სკანირება და მათი კონტროლი რომ არ ამოხდეს სისტემის დაზიანება და შემცირდეს რისკები.
- მომხმარებლის ვალიდაცია: Cloud-ის სერვისების პროვაიდერმა, უნდა უზრუნველყოს ყოველი მომხმარებლის დაცვა ავტორიცაზიის დროს, რომ არ მოხდეს მესამე პირის მიერს მომხმარებლის ანგარიშის ხელშიჩაგდება.
- დაცული ინტერფეისი და API: ინტერფესის და API-ის დაცვა ერთ-ერთი მნიშვნელოვანი და კრიტიკური ფაქტორია. შესაბამისა სერვისების პროვაიდერმა დიდი ყურადღება უნდა მიაქციოს მის დაცვას და კონტროლს.
- შიდა შეტევები: სერვესიების პროვაიდერმა უნდა უზრუნველყოს თანამშრომლების და შიდა სერვისების სკრინინგი და უსაფრთხოება იმისთვის, რომ არ მოხდეს ინსაიდერული შეტევები.
- უსაფრთხო ლივერსირებული რესურსები: სერვესიების პროვაიდერმა უნდა უზრუნველყოს გაზიარების და მრავალდონიანის სისტემების უსაფრთხოება-მონიტორინგი იმისთვის რომ ღრუბლოვანმა ტექნოლოგიებმა გამართულად იმუშავოს.

დასკვნა

ღრუბლოვან ტექნოლოგიებში დაცვის მექანიზმები იზრდება რისკების პროპორციულად, უმეტესად იმის გამო პოტენციური საფრთხეების აღმოჩენა დაგვიანებით ხდება. ღრუბლოვან ტექნოლოგიების რთული არქიტექტურა, ინფრტრასტუქტურა , მონაცემებიდ დიდი რაოდენობა და ქსელში კოლოსარული ტრაფიკი ქმნის უნიკალურ და სერიოზულ საფრთხეს ყოველი მომხმარებლისთვის. ასევე მომხმარებელმე უნდა გაითვალისწინოს ის რისკები რომელიც უკავშირდება ღრუბლოვან ტექნოლოგიების გამოყენებას. ყოველივე ამის გათვალისწინებით სერვისების პროვაიდერებმა უნდა შექმნან სამუშაო უსაფრთხო გარემო , დაიცვან მომხმარებლები მესამე პირების საფრთხეებისგან და გაითვალისწინონ ინფორმაციული უსაფრთხოების რეკომენდაციები, რომ დროულად მოხდეს კრიტიკური რისკების აღმოჩენა და მათი გაუვნებელყოფა.