Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 007:004.056
DOI: https://doi.org/10.24867/28BE35Lazetic

USLUGA UPRAVLJANJA KLJUČEVIMA ZA AMAZON VEB SERVISE

AMAZON WEB SERVICES KEY MANAGEMENT SERVICE

Plema Lažetić, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *Ovaj rad istražuje AWS Key Management Service, ključnu komponentu u AWS-ovom okruženju, fokusirajući se na procese upravljanja kriptografskim ključevima i osiguranje sigurnosti podataka u oblaku. Problemi koje se razmatraju obuhvataju izbor, kreiranje, upravljanje i integraciju ključeva u različitim AWS uslugama. Rezultati istraživanja doprinose razumijevanju primjene sigurnosnih mjera u cloud okruženju i prepoznavanju mogućnosti za poboljšanje prakse upravljanja ključevima u AWS-ovom okruženju.*

Ključne reči: *Usluga upravljanja ključevima na AWS-u, kriptografski ključevi, upravljanje pristupom.*

Abstract – *This paper explores the AWS Key Management Service, a crucial component in the AWS environment, focusing on cryptographic key management processes and data security assurance in the cloud. Issues under consideration encompass the selection, creation, management, and integration of keys across various AWS services. The research findings contribute to understanding the implementation of security measures in the cloud environment and identifying opportunities for enhancing key management practices within the AWS environment.*

Keywords: *AWS Key Management Service, cryptographic keys, access management.*

1. UVOD

U današnjem digitalnom dobu, programiranje u oblaku postaje sve prisutnija paradigma u razvoju softvera. Ova tehnologija omogućava efikasnije korišćenje resursa, skalabilnost aplikacija i olakšano upravljanje infrastrukturom [1].

Amazon Web Services (AWS) izdvaja se kao lider u pružanju infrastrukture u oblacima i različitih usluga za razvoj aplikacija. U okviru AWS-ovog okruženja, AWS Key Management Service (KMS) zauzima značajno mjesto kao ključni alat za upravljanje kriptografskim ključevima i osiguranje bezbjednosti podataka u oblacima.

Ovaj rad istražuje AWS KMS, analizirajući njegovu arhitekturu, funkcionalnosti i praktičnu primjenu.

Fokus je na karakteristikama ključeva, procesu upravljanja ključevima, politikama pristupa i integraciji sa drugim AWS uslugama, kako bi se istražilo kako AWS KMS doprinosi bezbjednosti i poverljivosti softverskih sistema u oblacima.

Kroz detaljnu analizu ovih elemenata, ovaj rad će prikazati ulogu i značaj AWS KMS-a u kontekstu programiranja u oblacima, pružajući uvid u najbolje prakse i uputstva za efikasno korišćenje ove ključne komponente AWS-ovog okruženja.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Srđan Vukmirović, red. prof.

2. AMAZON WEB SERVICES

Amazon Web Services su vodeći provajderi usluga računarstva u oblaku. Pružaju raznolike usluge za izgradnju, upravljanje i skaliranje IT infrastrukture i aplikacija. Njihova globalna prisutnost omogućuje korisnicima pristup računarskim resursima širom svijeta. Model "plaćaj koliko koristiš" eliminiše potrebu za kupovinom skupe hardverske infrastrukture unaprijed. AWS nudi širok spektar alata za zaštitu podataka, uključujući enkripciju i kontrolu pristupa. Svojim korisnicima omogućuje brzo pokretanje aplikacija, skaliranje resursa prema potrebama i plaćanje samo za korištene resurse. Sa preko 25 regija i 80 zona dostupnosti, AWS olakšava implementaciju aplikacija širom svijeta, poboljšavajući latenciju i dostupnost. Ove karakteristike čine AWS nezamjenjivim za organizacije u procesu digitalne transformacije [2].

2.1. AWS servisi

Amazon Web Services predstavlja širok spektar usluga računarstva u oblaku koje se mogu grupisati u sedam osnovnih kategorija, omogućavajući korisnicima da izaberu tačno ono što im je potrebno. Neki od najznačajnijih servisa koji pripadaju osnovnim kategorijama uključuju Amazon Elastic Compute Cloud (EC2) za računarstvo u oblaku, Amazon S3 za skladištenje podataka, Amazon DynamoDB i Amazon RDS za baze podataka, Amazon VPC i Amazon CloudFront za mrežne usluge i isporuku sadržaja, Amazon Redshift i Amazon Athena za usluge analize podataka, Amazon SageMaker i Amazon Rekognition za mašinsko učenje, i AWS IAM i AWS Key Management Service za bezbjednost, identitet i usklađenost [3].

3. AWS KEY MANAGEMENT SERVICE

AWS Key Management Service je usluga koja omogućava korisnicima generisanje, upravljanje i kontrolu kriptografskih ključeva koji se koriste za enkripciju podataka na AWS platformi. Koristeći AWS KMS, korisnici mogu lako stvarati i upravljati ključevima za enkripciju podataka bez potrebe za upravljanjem fizičkim hardverom ili implementacijom složenih kriptografskih algoritama.

Ova usluga pruža visoku sigurnost i pouzdanost, obezbeđujući enkripciju podataka tokom njihovog skladištenja i prenosa, što je ključno za zaštitu osjetljivih informacija u oblaku [4].

3.1. AWS KMS ključevi

KMS ključevi su ključni elementi za AWS Key Management Service, koji omogućavaju enkripciju i dekripciju podataka uz visok nivo bezbjednosti i fleksibilnost u generisanju dodatnih ključeva. Svaki KMS ključ sadrži metapodatke poput identifikatora, specifikacije, upotrebe i stanja ključa, pružajući korisnicima kontrolu i informacije o kriptografskim operacijama.

3.1.1. Osnovne vrste ključeva

Tri osnovne kategorije ključeva u AWS Key Management Service platformi su: AWS Managed key (ključevi koje upravlja AWS), Customer Managed key (ključevi koje upravlja korisnik), i AWS Owned key (ključevi u vlasništvu AWS-a).

3.1.2. Specijalne vrste ključeva

Pored osnovnih tipova ključeva, postoje i posebne vrste ključeva, koji uključuju i asimetrične ključeve, HMAC ključeve i multi-region ključeve.

4. IZBOR KARAKTERISTIKA KMS KLJUČEVA

U ovom poglavlju biće istražene različite karakteristike i opcije prilikom kreiranja ključeva za upravljanje kriptografskim operacijama pomoću AWS Key Management Service.

4.1. Odabir tipa KMS ključa

Izbor odgovarajuće vrste KMS ključa ključan je za bezbjednost podataka i ispravno funkcionisanje sistema. Simetrični ključevi su pogodni za većinu slučajeva, dok asimetrični omogućavaju šifrovanje izvan AWS-a. HMAC ključevi su korisni za integritet i autentičnost podataka. Važno je prilagoditi izbor ključa potrebama sistema za najviši nivo bezbjednosti i funkcionalnosti.

4.2. Odabir namjene KMS ključa

Pri odabiru namjene KMS ključa važno je razmotriti kako će se taj ključ koristiti, bilo za šifrovanje i dešifrovanje, potpisivanje i provjeru potpisa ili generisanje i provjeru HMAC oznaka. Svaki KMS ključ ima svoju specifičnu namjenu, što znači da će biti prilagođen samo jednoj vrsti operacija, što je važno kako bi se izbjeglo korišćenje istog ključa za više vrsta operacija, što može učiniti proizvod podložnijim napadima.

4.3. Odabir ključne specifikacije

Specifikacija ključa je kriptografska konfiguracija koja određuje karakteristike KMS ključa, uključujući tip ključa, kriptografski materijal i podržane algoritme, postavljajući osnove ključa koje kasnije nije moguće promijeniti. Pri odabiru specifikacije ključa važno je uzeti u obzir konkretan slučaj upotrebe i regulatorne zahtjeve, kao i mogućnost različitih cijena koje mogu biti povezane s različitim specifikacijama ključa.

5. UPRAVLJANJE KLJUČEVIMA

Upravljanje ključevima je temeljni aspekt osiguravanja povjerljivosti i sigurnosti podataka u današnjim cloud okruženjima, ključno za osiguravanje integriteta i privatnosti podataka, bez obzira na vrstu informacija. AWS Key Management Service omogućuje organizacijama efikasno generisanje, upravljanje i korištenje kriptografskih ključeva za zaštitu [4].

5.1. Proces kreiranja ključeva

U okviru ovog odjeljka biće objašnjeni različiti načini za kreiranje kako simetričnih tako i asimetričnih tipova ključeva.

5.1.1. Proces kreiranja ključeva putem konzole

Korisnici mogu koristiti AWS Management Console za kreiranje simetričnih i asimetričnih ključeva. Proces obuhvata odabir tipa ključa (simetrični ili asimetrični), namjenu ključa (šifrovanje i/ili dešifrovanje, potpisivanje i/ili verifikacija), unos pseudonima ključa, dodavanje opcionalnih opisa i oznaka, te definisanje korisnika i uloga koje mogu upravljati ključem ili ga koristiti u kriptografskim operacijama.

5.1.2. Proces kreiranja ključeva kroz AWS Command Line Interface (CLI)

Korištenjem AWS CLI-a, korisnici mogu efikasno upravljati sigurnosnim ključevima putem programskog interfejsa. Ova metoda omogućava korisnicima da koriste operaciju CreateKey, koja generiše simetrične ključeve za šifriranje u odabranom AWS regionu ili asimetrične ključeve za potpisivanje i verifikaciju poruka.

5.1.3. Proces kreiranja ključeva putem AWS CloudFormation-a

Kreiranje AWS KMS resursa putem AWS CloudFormation-a omogućava korisnicima da efikasno modeliraju i postave KMS ključeve i pseudonime, oslobađajući ih potrebe za ručnim upravljanjem resursima i infrastrukturom. Ovaj proces obuhvata definisanje ključeva i njihovih atributa, uključujući tip ključa (simetrični ili asimetrični) i druge parametre, kroz tekstualne šablone u JSON ili YAML formatu.

5.1.4. Proces kreiranja ključeva korištenjem AWS KMS API-ja

Korisnici mogu koristiti AWS SDK za podržane programske jezike (Java, .NET, Python, Ruby, PHP ili JavaScript u Node.js.) za interakciju sa AWS KMS putem API-ja. Kroz API, korisnici mogu koristiti operaciju CreateKey za kreiranje novih ključeva u AWS KMS-u. Ovo omogućava širok spektar funkcionalnosti za interakciju sa AWS uslugama putem podržanih programskih jezika.

5.2. Alijasi

Alijasi u AWS Key Management Service su prijateljski nazivi koji se koriste za identifikaciju KMS ključeva umjesto korištenja drugih identifikatora. Njihova nezavisnost od samog KMS ključa znači da akcije koje se izvode na alijasu ne utiču direktno na povezani ključ. Osim olakšavanja prepoznavanja i referenciranja KMS ključeva u različitim situacijama, alijasi omogućavaju i kontrolu pristupa KMS ključevima, čime se olakšava upravljanje pravima pristupa.

Svaki alijas ima jedinstveni Amazon Resource Name (ARN) koji ga identifikuje unutar određenog računa i regije. Mogu se kreirati u različitim regijama, omogućavajući upotrebu istog koda u više regija, pri

čemu se automatski upućuju na povezani KMS ključ u svakoj regiji. Alijasima je moguće upravljati putem AWS KMS konzole, CreateAlias API-ja ili pomoću AWS CloudFormation šablona. AWS KMS API pruža potpunu kontrolu nad alijasima, omogućavajući operacije kao što su kreiranje, pregled, ažuriranje i brisanje alijasa u svakom nalogu i regiji, koristeći ugrađene metode koje su dio AWS SDK. Alijasi su osjetljivi na velika i mala slova i ne mogu se mijenjati nakon što su kreirani.

5.3. Pregled dostupnih KMS ključeva

Pregled dostupnih KMS ključeva je ključan za osiguranje sigurnosti i zaštite podataka u oblaku. Ovaj proces omogućava administratorima efikasno upravljanje ključevima i pristupom, te održavanje statusa sigurnosti i praćenje sigurnosnih parametara.

Pregled je omogućen putem AWS konzole i API-ja, pružajući detaljne informacije o ključevima i njihovim karakteristikama, kao i mogućnost filtriranja i sortiranja radi lakšeg upravljanja resursima. Korištenjem operacija poput ListKeys, DescribeKey, GetKeyPolicy, ListAliases i ListResourceTags putem API-ja, korisnici mogu detaljno upravljati i pratiti svoje KMS ključeve i povezane alijase.

5.4. Omogućavanje i onemogućavanje KMS ključeva

Omogućavanje i onemogućavanje AWS KMS ključeva je ključni dio upravljanja sigurnošću podataka u AWS KMS-u. Ključevi se podrazumijevano omogućavaju prilikom kreiranja, ali ih je moguće onemogućiti kako bi se privremeno isključili iz upotrebe, pružajući korisnicima mogućnost zadržavanja ključeva za buduću upotrebu. Međutim, ključevi koje upravlja AWS ne mogu se onemogućiti ili omogućiti jer su trajno omogućeni za korištenje od strane AWS usluga. Postoje dva načina za omogućavanje i onemogućavanje KMS ključeva: putem konzole i putem AWS KMS API-ja.

5.5. Automatska rotacija KMS ključeva

Automatska rotacija ključeva omogućava sigurnu zamjenu kriptografskog materijala ključeva bez potrebe za promjenom aplikacija ili AWS usluga. AWS KMS periodično generiše nove kriptografske materijale za ključeve koji su omogućeni za automatsku rotaciju, čuvajući pritom sve prethodne verzije.

Rotirani materijal ključa se ne briše dok se ne obriše sam KMS ključ. Rotacija ključeva se može pratiti putem Amazon CloudWatch-a i AWS CloudTrail-a, a podržana je samo za simetrične KMS ključeve koje generiše AWS KMS. Omogućavanje ove funkcije je opcionalno za KMS ključeve kojima upravlja korisnik, dok AWS KMS automatski rotira ključni materijal za KMS ključeve kojima sam upravlja. Ova funkcija donosi nekoliko prednosti, uključujući očuvanje svojstava ključa kao što su ID i ARN, kao i kontinuiranu upotrebu KMS ključeva u AWS uslugama.

5.6.Nadgledanje KMS ključeva

Nadgledanje ključeva u AWS KMS-u je ključno za osiguravanje njihove dostupnosti, stanja i optimalne upotrebe. To je važan korak u održavanju pouzdanosti, dostupnosti i performansi AWS rešenja.

Za tu svrhu koriste se alati poput AWS CloudTrail-a, Amazon CloudWatch-a i Amazon EventBridge-a.

5.7. Brisanje KMS ključeva

Proces brisanja AWS KMS ključeva ima trajne posledice, budući da se ne može povratiti i čini podatke nepristupačnim. Važno je pažljivo razmotriti brisanje ključa, uz procjenu rizika i eventualno isključivanje ključa umesto brisanja. AWS KMS ne briše ključeve osim ako korisnik izričito ne zakaže brisanje, što dodatno ističe važnost pažljivog upravljanja ključevima.

Periode čekanja prije brisanja ključeva pruža dodatnu bezbjednost i mogućnost povratka, a proces brisanja je isti za simetrične i asimetrične ključeve, ali kod asimetričnih ključeva zahtijeva pažljivo planiranje i nadzor radi očuvanja bezbjednosti podataka.

6. POLITIKE UPRAVLJANJA PRISTUPOM AWS KMS RESURSIMA

Upravljanje pristupom AWS Key Management Service resursima predstavlja ključni aspekt sigurnosne strategije unutar AWS okruženja. Različiti mehanizmi omogućavaju organizacijama da precizno kontrolišu ko može pristupiti ključnim resursima i na koji način [4].

6.1. Politika ključa

Politika ključa u AWS KMS predstavlja dokument koji precizira pravila pristupa i dozvole za korišćenje određenog KMS ključa. Svakom KMS ključu mora biti dodijeljena tačno jedna politika ključa, koja detaljno definiše ko ima pristup ključu i na koji način. Politika ključa precizira dozvole za korisnike, grupe ili uloge koje imaju pristup ključu. Izjave u politici ključa definišu koje operacije su dozvoljene ili zabranjene za određene subjekte. Politika ključa se primenjuje samo na KMS ključeve unutar iste AWS regije i može biti ažurirana u bilo kom trenutku kako bi se promijenile dozvole ili pravila pristupa. Pri definisanju politike za AWS KMS, ključni dokument politike treba da sadrži određene elemente, uključujući Version, Statement, Sid, Effect, Principal, Action, Resource i Condition.

6.2. IAM politika

IAM politike su ključni alat u upravljanju pristupom AWS resursima, omogućavajući preciznu kontrolu nad dozvolama i ograničenjima za različite korisnike, grupe i uloge. Ove politike definišu koje akcije mogu biti izvršene nad određenim AWS resursima, pružajući sigurnosni okvir za upravljanje identitetima u AWS oblaku. Kroz kombinaciju IAM politika sa drugim AWS alatima za upravljanje pristupom, administratori mogu prilagoditi pristup različitim AWS resursima u skladu sa potrebama korisnika, osiguravajući time bezbjednost i usklađenost sa regulativama.

Putem IAM konzole ili AWS API-ja, administratori mogu dodeljivati, uređivati i uklanjati IAM politike kako bi prilagodili pristup resursima u skladu sa zahtjevima poslovanja i bezbjednosti.

6.2. Grantovi

Granatovi u AWS KMS-u omogućavaju privremeni pristup određenim KMS ključevima za kriptografske operacije poput šifrovanja i dešifrovanja podataka. Oni se koriste za kontrolu pristupa podacima zaštićenim KMS ključevima, često u AWS uslugama koje zahtijevaju šifrovanje podataka. Prilikom korišćenja granatova, važno

je razumjeti koncepte kao što su ograničenja granata, jedinstveni identifikatori granata i dozvoljene operacije. Kreiranje granata obavlja se putem operacije CreateGrant, gde se navode ključ KMS-a, principali primaoca, dozvoljene operacije i eventualna ograničenja.

Važno je izbeći dupliranje granata i koristiti neutralne nazive kako bi se spriječilo otkrivanje osjetljivih informacija.

7. INTEGRACIJA I UPOTREBA AWS KMS U RAZLIČITIM AWS USLUGAMA

Integracija i korišćenje AWS Key Management Service u različitim AWS uslugama ključni su za sigurnost u oblaku. AWS KMS pruža napredne funkcionalnosti enkripcije i omogućava zaštitu podataka u oblaku. Mnoge AWS usluge, poput AWS CloudTrail-a, Amazon DynamoDB-a, Amazon S3 i drugih, koriste AWS KMS za šifrovanje podataka i upravljanje ključevima. Ova integracija osigurava bezbjednost i poverljivost informacija korisnika u različitim kontekstima.

7.1. AWS CloudTrail

AWS CloudTrail je servis koji omogućava snimanje događaja i aktivnosti na AWS nalogu radi praćenja, analize i bezbjednosnih razloga, uz korišćenje AWS KMS-a za sigurno čuvanje podataka [5].

7.2. Amazon Simple Storage Service

Amazon Simple Storage Service (S3) je usluga za čuvanje podataka u oblaku koja omogućava korisnicima da skladište i koriste podatke iz bilo kog mjesta na internetu, pružajući pristup podacima putem standardnih veb protokola. AWS KMS se koristi za šifrovanje podataka prilikom čuvanja u Amazon S3, omogućavajući visok nivo bezbjednosti [6].

7.3. Amazon WorkMail

Amazon WorkMail je sigurna i kontrolisana usluga za poslovnu e-poštu, koja pruža podršku za različite klijente e-pošte na desktopu i mobilnim uređajima. Za zaštitu ključeva za šifrovanje koristi se AWS KMS, koji omogućava kontrolu nad ključevima i dodatni sloj bezbjednosti [7].

7.4. Amazon Elastic Block Store

Amazon Elastic Block Store (Amazon EBS) omogućuje korisnicima skladištenje i upravljanje podacima na nivou blokova, pružajući dodatni sloj zaštite uz korišćenje AWS KMS-a za enkripciju podataka [8].

7.5. Amazon DynamoDB

Amazon DynamoDB je potpuno upravljana NoSQL baza podataka koja se skalira prema potrebama korisnika, integrišući AWS KMS radi enkripcije podataka na strani servera [9].

7.6. AWS Secrets Manager

AWS Secrets Manager je usluga za čuvanje tajnih informacija koja koristi AWS KMS za šifrovanje i dešifrovanje tih informacija, namijenjena čuvanju osetljivih podataka, kao što su lozinke [10].

8. ZAKLJUČAK

Kroz analizu različitih aspekata AWS Key Management Service, od vrsta ključeva do politika upravljanja pristupom, istaknuta je važnost ove usluge u osiguravanju pouzdane zaštite podataka u klaud okruženju.

Integracija KMS-a sa različitim AWS uslugama demonstrira širok spektar primjena ove usluge.

Dalje unapređenje uključuje detaljnu analizu performansi KMS-a, primjere primjene, komparativnu analizu sa konkurentskim rješenjima i istraživanje relevantnih sigurnosnih propisa i standarda. Takva dodatna istraživanja doprinose dubljem razumijevanju prednosti, nedostataka i implikacija korišćenja AWS KMS-a u praksi.

9. LITERATURA

[1] https://en.wikipedia.org/wiki/Cloud_computing (pistupljeno u martu 2024.)
[2] https://en.wikipedia.org/wiki/Amazon_Web_Services (pristupljeno u martu 2024.)
[3] https://aws.amazon.com/products/ (pristupljeno u martu 2024.)
[4] https://docs.aws.amazon.com/kms/latest/developerguide/overview.html (pristupljeno u martu 2024.)
[5] https://aws.amazon.com/cloudtrail/ (pistupljeno u martu 2024.)
[6] https://aws.amazon.com/s3/ (pristupljeno u martu 2024.)
[7] https://aws.amazon.com/workmail/ (pistupljeno u martu 2024.)
[8]] https://aws.amazon.com/ebs/ (pristupljeno u martu 2024.)
[9] https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html (pistupljeno u martu 2024.)
[10] https://aws.amazon.com/secrets-manager/ (pistupljeno u martu 2024.)

Kratka biografija:

Plema Lažetić rođena je 17. aprila 1999. godine u Trebinju. Osnovnu školu "Sveti Sava" završila je u Avtovcu, dok je gimnaziju, opšti smjer, završila u srednjoškolskom centru "Pero Slijepčević" u Gacku, kao đak generacije. Školske 2018/2019 godine upisuje Fakultet tehničkih nauka u Novom Sadu, na studijski program Primenjeno softversko inženjerstvo. Osnovne akademske studije završila je u predviđenom roku, te školske 2022/2023 upisuje master studije, takođe, na studijskom programu Primenjeno softversko inženjerstvo.
kontakt: lazeticplema@gmail.com