

## META DATALARDAN FOYDALANISH VA META DATALARGA BO'LADIGAN HUJUMLAR

**Xolmatov Elbek Sherzod o'g'li**  
**Madatov Islom Shukurullo o'g'li**  
**Jo'ramirzayev Islomjon Adxamjon o'g'li**  
**Odilov Ozod Rahmatullo o'g'li**

*Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari  
universiteti talabalari*

**Anatatsiya:** maqolada Meta datalardan foydalanish usullari yoritib berilgan hamda virtual Internet olamida meta data larga bo'ladigan hujum turlar o'rganib aniqlangan.

**Kalit so'zlar:** ma'lumotlar bazasi, veb-saytlar, ijtimoiy tarmoqlar, hujum, Virtual shaxsiy bulut (VPC).

Metama'lumotlarning turli shakllaridan har xil usullarda foydalanish mumkin. Tashkilotdagi metama'lumotlarning eng yaxshi ilovalari:

### ✓ **MA'LUMOTLAR BAZASINI BOSHQARISH**

Ma'lumotlar bazasini boshqarish tizimidagi (DBMS) metama'lumotlar ustun nomi va ma'lumotlar qismiga birlashtirilgan qator raqamidan iborat. SQL standarti sxema deb ataladigan metama'lumotlarga kirish uchun standartlashtirilgan usulni taklif qiladi; ammo, barcha ma'lumotlar bazalari bu usulni amalga oshirmaydi. Metadata ma'lumotlarni tartibga solish, sharhlash va so'rashni osonlashtiradi.

Metadata ma'lumotlar bazasida foydalanuvchilarga ma'lumotlarni turlari bo'yicha osongina saralash va filtrlash hamda turli ma'lumotlar to'plamlari o'rtasida aloqalarni o'rnatish imkonini beruvchi katalog bo'lishi mumkin. DBMS katalogi ma'lumotlar yig'ish bilan bog'langan va ma'lumotlar bazasi maqolalarini belgilaydigan ma'lumotlarni o'z ichiga oladi.

### ✓ **VEB-SAYTLARNI QIDIRISH**

Veb-saytlar ularning reytingi va muvaffaqiyatiga sezilarli ta'sir ko'rsatadigan metama'lumotlar bilan o'rnatilgan. Veb-sahifani yaratishda meta sarlavhasi va meta tavsifi kabi metama'lumotlar tafsilotlarini kiritish muhimdir. Meta sarlavhasi sahifaning mavzusini qisqacha tavsiflaydi, bu o'quvchilarga nima kutish kerakligini oldindan ko'rish imkonini beradi.

Meta tavsifi qisqa bo'lsa-da, sahifa mazmuni haqida qo'shimcha ma'lumot beradi. Meta teg faqat sahifa kodida paydo bo'ladi va qidiruv tizimlariga sahifani tasniflashda yordam beradi. Qidiruv mexanizmlari ushbu

metadataning kalit so'zlarni aniqlash va veb-saytni tasniflash uchun ishlatish uchun o'qiydi.

### ✓ **IJTIMOYIY TARMOQLAR**

Ijtimoiy mediadagi meta-ma'lumotlar foydalanuvchilarga o'z kontentini Facebook yoki Twitter kabi platformalarda qanday baham ko'rishni xohlashlarini ko'proq nazorat qilish imkonini beradi. Foydalanuvchilar o'z kontentini optimallashtirishganda, ular optimallashtirilmagan postlardan ko'ra o'z postlaridan ko'proq o'zaro ta'sirga ega bo'lishadi.

Misol uchun, foydalanuvchilar Facebook-da havolalarni nashr qilganda, u postning sarlavhasi, postning qisqacha tavsifi va tanlangan rasm, postning URL manzili va veb-sayt nomi kabi metama'lumotlarni chiqaradi. Foydalanuvchilar o'zlarining postlari qanday ko'rsatilishini optimallashtirish va aniqlash uchun Facebook-da Open Graph va Twitter-dagi Twitter Cards-dan foydalanishlari mumkin.

### ✓ **BELGILASH TILLARI**

Belgilash tillari foydalanuvchilarga hujjatning paragraf yoki sarlavha kabi alohida elementlarini aniqlash imkonini beradi. Ular standart umumlashtirilgan belgilash tilini (SGML) yoki kengaytiriladigan belgilash tilini (XML) o'z ichiga oladi. SGML mashinalar tomonidan o'qilishi mumkin bo'lgan hujjatlarni almashish imkonini berdi. XML ma'lumotni mashinalar tomonidan o'qilishi uchun matnga biriktirish uchun standartlashtirilgan qoidalardan iborat.

U so'zlar, jumlar yoki paragraflar kabi matn qismlarini ular orasidagi narsalarni tavsiflovchi teglarga o'rash orqali ishlaydi. Belgilash tarkibi foydalanuvchilarga turli xil hujjatlarda kalit so'zlarni qidirishga imkon beradi.

### ✓ **ISTE'MOLCHILARNI KUZATISH ILOVALARI**

Chakana savdo va onlayn xarid qilish veb-saytlari ko'pincha iste'molchilarning odatlari va harakatlarini kuzatish uchun metadataning foydalanadi. Ular iste'molchi qurilmasi turi, joylashuvi, xaridlari, bosishlari va saytlarga kirish vaqtlari kabi qonuniy ravishda ruxsat etilgan har qanday ma'lumotlarni to'playdi.

Ushbu ma'lumotlardan foydalanib, ular o'z iste'molchilarining afzalliklari, birlashmalari va odatlarining rasmini yaratadilar va o'z mahsulotlarini ularga sotish uchun foydalanadilar. Ushbu ma'lumot iste'molchilarni segmentlarga ajratishi va ularga maqsadli reklamalarni yuborishi mumkin. Xuddi shunday, hukumatlar veb-faoliyatni kuzatish uchun veb-sahifalar va elektron pochtaerdagi metama'lumotlardan foydalanishlari mumkin. Ushbu ma'lumotlardan ommaviy kuzatuvda foydalanish mumkin.

## ✓ **AXBOROT TASNIFI**

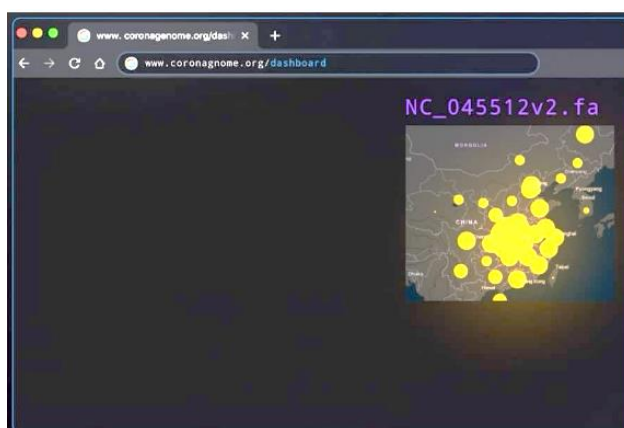
Tasniflash ma'lumotni kerak bo'lganda topish uchun mantiqiy tartibga solishni o'z ichiga oladi. Ushbu ma'lumotni sinflar yoki toifalarga joylashtirish taksonomiya deb nomlanadi va ob'ektlar bilan bog'liq ma'lumotlar metadada hisoblanadi. Foydalanuvchilar ushbu ma'lumotni tarkibga yoki tashqi kontentni boshqarish tizimiga joylashtirishlari mumkin.

Metama'lumotlarni tushunish samarali kontentni boshqarish tizimini (CMS) yaratishda muhim ahamiyatga ega. Taksonomiyalar ichida boshqariladigan lug'atlar mo'ljallangan maqsadni tushunishga yordam beradi. Metadada teglari resurslarni topishda va resurslarni tashkil qilishni yaxshilashda yordam beradi. To'g'ri tasniflangan ma'lumotlar foydalanuvchilarga ma'lumotlarni tahlil qilish va ular bilan ishlashni osonlashtiradi.

### **META DATA GA BO'LADIGAN XUJUMLAR**

IMDS ning 1-versiyasi (IMDSv1) 2012-yilda EC2 nusxalarining boshqa AWS xizmatlari bilan o'zaro aloqada bo'lishi uchun xavfsizroq yo'lni yaratish uchun chiqarilgan. Mijozlar AWS kalitlarini misolda qoldirish o'rniga endi EC2 namunasidan hisob ma'lumotlarini olish va boshqa AWS xizmatlariga AWS API qo'ng'iroqlarini amalga oshirish uchun metama'lumotlar xizmatidan so'rashi mumkin. Misol uchun, agar EC2 namunasi ba'zi mijozlar ma'lumotlariga ega bo'lsa, u ushbu ma'lumotlarni Amazon Simple Storage Service (S3) papkasida saqlash uchun IMDSv1 dan foydalanishi mumkin. Aynan shu qobiliyat hujumchi Capital One mijozlari haqidagi ma'lumotlarni saqlash uchun ishlatiladigan S3 papkadan maxfiy ma'lumotlarni olib tashlash uchun foydalangan.

O'z sinovimizda biz ushbu ma'lumotlarni olish har qanday dasturda qanday ishlashini takrorlay oldik. Bizning misolimizda epidemiologlar jamoasi AWS-da virus genomini tahlil qilish jarayonini ko'rsatadigan ma'lumotlarni vizual ravishda aks ettirish uchun ommaviy boshqaruv paneliga ega bulutli mahalliy dasturni yaratdilar.



Ushbu ilovani ishlab chiqish bosqichida jamoa qiyinchilikka duch keldi. Virtual shaxsiy bulutdagi (VPC) resurslarning aksariyati internetdan yashirin bo'lishi kerak edi. Ularning VPC-dagi ommaviy ko'rish uchun mo'ljallangan yagona resurs asboblari paneli edi.

Ularning ma'lumotlarini joylashtiradigan S3 papka maxfiy bo'lishi kerak edi. S3-dan umumiy boshqaruv paneliga ma'lumotlarni olish uchun ular vositachi sifatida ishlaydigan teskari proksi-serverni qo'shdilar. Buning uchun tezkor Google qidiruvi va uni ilovaga qo'shish uchun bir necha qator kod kerak bo'ldi.



Epidemiologlar jamoasi uchun teskari proksi-server ulardan foydalanish holatlari uchun juda mos keladigan asosiy, oqlangan yechim edi. Ular tushunmagan narsa shundaki, bu ularni katta buzilish uchun qo'ygan.

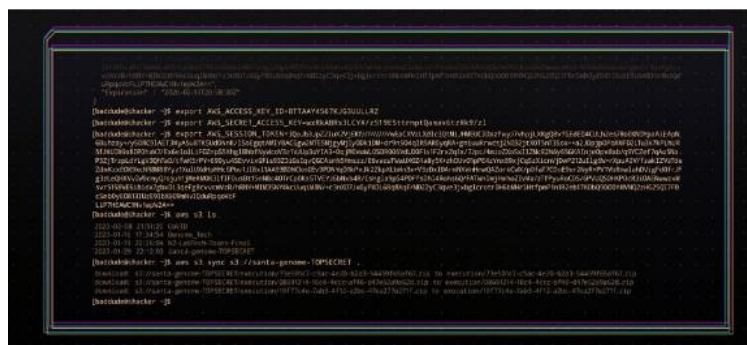
Teskari proksi-server bilan ishlaydigan hisoblash namunasiga shaxsiy S3 papkasiga kirish ruxsati bilan IAM roli tayinlangan. S3-ga kirish uchun teskari proksi-server uchun hisob ma'lumotlari Instance Metadatadan olingan.

Saytga tashrif buyurgan va ularning ma'lumotlari bilan qiziqqan hujumchi jamoa boshqaruv panelida teskari proksi-serverning IP-manziliga murojaat qilganini payqadi. Shundan so'ng hujumchi unga ulanishi mumkinligini tekshirdi. Ulanishni tasdiqlaganidan so'ng, hujumchi teskari proksi-server orqali Instance metama'lumotlariga kira oladimi yoki yo'qligini tekshirdi. Muvaffaqiyat.

Teskari proksi-server va Instance Metadata orqali hujumchi jamoaning shaxsiy S3 saqlash papkasidagi hisob ma'lumotlarini ochdi.



Endi, S3 papkasiga kirish imkoni bilan hujumchi jamoa o'z ilovalari uchun saqlagan juda nozik ma'lumotlarni o'g'irlashi mumkin edi. Buzg'unchi shunchaki maqsadli S3 papkasini boshqa AWS hisobidagi o'zining S3 papkasiga sinxronlashtirdi va ma'lumotlar ularniki edi.



Ushbu hujum turi MITER tomonidan bulutli muhitlar uchun ATT&CK tizimida tasvirlangan 43 ta texnikadan faqat bittasi edi.

### XULOSA

Biz ta'riflagan hujumda teskari proksi-server tashqi so'rovlarning ichki manbalarga kirishiga ruxsat berish uchun noto'g'ri sozlangan. Agar jamoa o'zining hisoblash namunasini IMDSv2 dan foydalanish uchun sozlagan bo'lsa, tashqi tahdid ishtirokchisi tomonidan ruxsatsiz kirish bloklangan bo'lar edi. Skyhigh Security-da bizda bu kabi hujumlarni aniqlash va oldini olishga yordam beradigan bir nechta yondashuvlar mavjud.

AWS bilan to'g'ridan-to'g'ri API integratsiyasidan foydalangan holda, Skyhigh CNAPP har bir EC2 misolida qaysi IMDS versiyasidan foydalanayotganingizni ko'rsatish uchun Amazon CloudWatch – ilova va infratuzilma monitoringi xizmatini doimiy ravishda kuzatib boradi.

### FOYDALANILGAN ADABIYOTLAR:

1. Алтаев Ж. ГИС и земельный кадастр Казахстана. — М.: ARGREVIEW. Современные геоинформационные технологии. - 2003.-№2.-С.2-5.,с14
2. Артамонов Б.Н., Брякалов Г.А., Гофман В.Э. и др. Основы современных компьютерных технологий. — СанктПетербург.: «Корона принт». 2002.-445с.
3. Валков В.М., Вершин В.Е. Автоматизированные системы управления технологическими процессами. —Д.: Политехника, 1991.-269 с.
4. <https://atlan.com/types-of-metadata/#6-usage-metadata>
5. <https://www.skyhighsecurity.com/about/resources/resource-center.html>
6. <https://www.metadataetc.org/metadatabasics/types.htm>