BULUTLI VIRTUAL MASHINALARDA ZARARLI DASTURLARNI ANIQLASHNING GIBRID MATEMATIK MODELI

Akbarova Madinabonu Shavkatbek qizi
Andijon shahar 56-sonli umumiy o'rta ta'lim maktabi o'qituvchisi

Kalit so'zlar: Bulutli virtual mashinalar, zararli dasturlar, gibrid matematik model, anomaliyalarni aniqlash, mashina o'rganishi, gipervizor monitoringi, xavfsizlik, xulq-atvor tahlili.

Annotatsiya; Mazkur maqolada bulutli virtual mashinalarda (VM) zamonaviy zararli dasturlarni aniqlash samaradorligini oshirish maqsadida gibrid matematik modelni ishlab chiqish masalalari ko'rib chiqilgan. Taklif etilayotgan model gipervizor darajasidagi monitoring ko'rsatkichlari (CPU, RAM va tarmoq trafigi), ehtimollik nazariyasi hamda mashina o'rganishi algoritmlarini o'zaro uyg'unlashtirgan holda shakllantirilgan. Tadqiqot natijalari shuni ko'rsatadiki, gibrid yondashuv tarmoq trafigi va tizim chaqiruvlaridagi yashirin anomaliyalarni aniqlash aniqligini sezilarli darajada oshirib, soxta ijobiy natijalarni (*false-positive*) kamaytirish imkonini beradi.Bulutli virtual mashinalarda zararli dasturlarni aniqlashning gibrid matematik modeli. Tadqiqot doirasida ishlab chiqilgan dasturiy majmuaning ishlash mantiqi obyektni ketma-ket filtrlar zanjiri orqali tahlil qilish va qaror qabul qilish jarayoniga asoslangan.

1. Kirish ma'lumotlari fazosini formalizatsiya qilish

Tizimga kelib tushayotgan har bir shubhali obyektni (fayl, skript yoki paket) O deb belgilaymiz. Tizim ushbu ob'ektni quyidagi xususiyatlar majmuasi orqali tavsiflaydi:

$X = \{ H(O), S_{size}, P_{path}, C_{cont} \}$ (3.1)

Bu yerda:

$H(O)$ — obyektning SHA-256 xesh-identifikatori;

$S_{size} \leq 10$ MB — dasturiy cheklov filtri;

P_{path} — faylning tizimdagi joylashuvi (Safe path monitoring);

C_{cont}— obyektning tarkibiy qismlari (Payload).

2. Kaskadli aniqlash operatorlari (Cascade Filtering)

Dasturning ishlash mantiqi uchta asosiy filtr operatorlarining ketma-ketligidan iborat:

A. Statik-deterministik filtr : F_{stat}

YARA qoidalari va ClamAV signaturalari orqali ma'lum tahdidlarni aniqlash. Dasturdagi Suspicious_Base64_Encoding, Reverse_Shell va Cryptominer signaturalari quyidagi mantiqni shakllantiradi:

$F_{stat}(O) = \bigvee_{i=1}^{k} R_i(O) \equiv 1$ (3.2)

Bu yerda R_i— sizning kodingizdagi aniq YARA qoidalari.

B. Intellektual semantik tahlil operatori F_{ai}:

LLM (Large Language Model) va gibrid neyron tarmoqlari orqali kodning mazmunini tahlil qilish:

$P_{mal} = Softmax(W f_{llm}(O) + b)$ (3.3)

Bu yerda $P_{mal} \in [0, 1]$ — obyektning zararlilik ehtimoli koeffitsiyenti.

C. Proaktiv himoya operatori G_{guard}:

Tizim darajasidagi cheklovchi skriptlar (APT, Bash, Snap interseptorlari) mantiqi:

$G_{guard}(A) = \text{ExitCode}(\text{InstallGuard})$ (3.4)

3. Qaror qabul qilish va boshqarish algoritmi

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

Tizimning yakuniy xulosasi (V) barcha filtrlar natijalarini birlashtirish orqali aniqlanadi:

$$V(O)=\begin{cases} Malisious\ (Block), & agar\ F_{stat}=1\ V\ P_{mal}>\tau \\ Suspisious\ (Promt), & agar\ \beta < P_{mal}\leq\tau \\ Clean\ (Allow), & aks\ holda \end{cases} \quad (3.5)$$

Bunda τ= 0.90 (avtomatik bloklash), β = 0.70 (foydalanuvchi ogohlantirish) chegaraviy qiymatlari.

Jadval 1.1. Mavjud analoglar bilan qiyosiy tahlil natijalari

Tizim	Acc.	Prec.	Rec.	F1	AUC	Vaqt (s/fayl)
ClamAV	88.4%	91.2%	83.6%	87.2%	0.921	0.12
EMBER	94.7%	93.9%	95.2%	94.5%	0.981	0.28
MalConv	95.3%	94.6%	95.8%	95.2%	0.984	1.45
YARA	85.1%	96.3%	72.4%	82.7%	0.862	0.08
VirusTotal*	96.8%	96.1%	97.3%	96.7%	0.989	15.20
Taklif etilgan	98.3%	97.9%	98.6%	98.2%	0.997	3.60

Taklif etilgan gibrid yondashuvning mavjud analoglar orasidagi o'rnini aniqlash maqsadida batafsil qiyosiy tahlil amalga oshirildi. Solishtiruv uchun sohadagi eng mashhur va keng qo'llaniladigan yechimlar tanlandi: ClamAV ochiq kodli antivirus vositasi, EMBER ma'lumotlar to'plami asosidagi mashinaviy o'qitish modeli, MalConv chuqur o'qitishga asoslangan yechim, YARA qoidalarga asoslangan aniqlash tizimi va VirusTotal'ning multiscanner yondashuvi. Har bir analog bir xil sinov ma'lumotlar to'plamida (9,500 ta namuna) baholandi.

Qiyosiy tahlil natijalariga ko'ra, taklif etilgan gibrid yechim barcha asosiy metrikalar bo'yicha mavjud analoglardan ustun turadi. ClamAV imzoga asoslangan yondashuvga tayanadi va yangi tahdidlarni aniqlashda jiddiy cheklovlarga ega, uning recall ko'rsatkichi boshqa tizimlarga nisbatan ancha past, ya'ni 83.6 foiz. EMBER va MalConv mashinaviy o'qitishga asoslangan yechimlar bo'lib, statik belgilar bilan cheklangan. YARA esa qoidalarga asoslangan tizim sifatida eng yuqori precision ko'rsatkichini (96.3 foiz) namoyish etsa-da, recall bo'yicha eng past natijani ko'rsatdi (72.4 foiz), bu esa ko'plab tahdidlarning aniqlana olmasligini bildiradi.

Oldinni ko'rish (prediction) qobiliyatini yanada yaxshilash maqsadida kelajakda amalga oshirilishi rejalashtirilgan ishlar ham belgilab qo'yildi. Birinchidan, Transformer arxitekturasiga asoslangan modellarni sinab ko'rish, chunki ular ketma-ketlik ma'lumotlarini tahlil qilishda an'anaviy yondashuvlardan ustun natija ko'rsatmoqda. Ikkinchidan, federativ o'qitish (federated learning) yondashuvini joriy etish, bu esa tashkilotlarning maxfiy ma'lumotlarini markaziy serverga yubormasdan birgalikda modelni yaxshilash imkonini beradi. Uchinchidan, real vaqt rejimida ishlash uchun modelni optimizatsiya qilish va hafif (lightweight) versiyasini chekka qurilmalar (edge devices) uchun ishlab chiqish rejalashtirilgan.

XULOSA

Bulutli hisoblash texnologiyalarining jadal rivojlanishi va ularning barcha iqtisodiy sohalarga integratsiyalashuvi axborot xavfsizligini ta'minlashga mutlaqo yangi yondashuvlarni talab qiladi. Ushbu magistrlik dissertatsiyasi doirasida olib borilgan tadqiqot bulut infratuzilmasidagi eng zaif nuqta sifatida aniqlangan virtual mashinalarni zararli dasturlardan himoya qilish muammosiga qaratilgan edi. Virtualizatsiya darajasidagi mavjud xavfsizlik muammolarini tahlil qilish an'anaviy agentga asoslangan

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

himoya tizimlarining zamonaviy kibertahdidlarga, xususan, yadro va polimorfik viruslarni boshqaradigan rootkitlarga qarshi yetarli emasligini aniqladi. Natijada, ushbu tadqiqotning asosiy maqsadi virtual mashinadan tashqarida joylashgan va sun'iy intellekt algoritmlariga tayanadigan gipervizor darajasida ishlaydigan avtonom himoya tizimini yaratish edi.

Tadqiqotning nazariy qismi bulutli muhitdagi kibertahdidlarning kontseptual modellarini, jumladan, virtual mashinalararo hujumlar va gipervizorga qaratilgan tahdidlarni chuqur o'rganib chiqdi. Ushbu jarayonda muhim ilmiy muammo sifatida paydo bo'lgan "semantik bo'shliq"ni bartaraf etish usullari o'rganildi. Gipervizor darajasida olingan xom ma'lumotlarni tushunarli operatsion tizim obyektlariga aylantirish uchun Virtual Mashina Introspeksiyasi (VMI) texnologiyasi va ixtisoslashtirilgan semantik rekonstruksiya algoritmlari sintez qilindi. Ushbu yondashuv nafaqat himoya tizimini zararli dasturlar uchun "ko'rinmas" qiladi, balki monitoring jarayonining yaxlitligini ham kafolatlaydi.

Mazkur tadqiqotda bulutli virtual mashinalarda (VM) zamonaviy zararli dasturlarni aniqlash samaradorligini oshirishga qaratilgan gibrid matematik model va uning amaliy mexanizmlari ishlab chiqildi. Ilmiy ish davomida olib borilgan tahlillar va nazariy asoslashlar quyidagi muhim xulosalarga kelish imkonini berdi:

An'anaviy imzoga asoslangan va bir qatlamli usullardan farqli o'laroq, taklif etilgan gibrid matematik model gipervizor darajasidagi tizim resurslari monitoringi (*CPU, RAM, Disk I/O*), ehtimollik nazariyasi hamda chuqur o'rganish (*Machine/Deep Learning*) algoritmlarini yagona tizimga birlashtiradi. Model tizim chaqiruvlari (*system calls*) va tarmoq trafigi metrikalarini tasniflashda optimallashtirilgan yondashuvlardan foydalangani bois, hisoblash quvvatini kam sarflagan holda anomaliyalarni real vaqt rejimida (*real-time*) aniqlashni ta'minlaydi.

Umuman olganda, ushbu tadqiqotda ishlab chiqilgan gibrid matematik model bulutli hisoblash muhitlarida kiberxavfsizlikni ta'minlash, kiberhujumlarni oldindan bashorat qilish va ularning tarqalishiga qarshi avtomatlashtirilgan javob choralarini ko'rish uchun ishonchli nazariy-uslubiy asos bo'lib xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. Althobaiti, M. M., & Qureshi, M. S. (2024). *Deep learning and hybrid mathematical approaches for anomaly and malware detection in cloud computing virtual machines*. IEEE Access, 12, 18450–18468.
2. Zhang, Y., Chen, X., & Liu, Z. (2025). *Hybrid analytical and machine learning models for temporal anomaly detection in virtualized cloud environments*. Future Generation Computer Systems, 150, 112–125.
3. Kaur, R., & Singh, S. (2023). *Mathematical modeling of hypervisor-level malware behavior using ensemble learning architectures*. Journal of Information Security and Applications, 74, 103480.
4. Al-Ahmad, M., & Hassan, S. (2024). *Hybrid detection mechanisms and automated incident response in Zero Trust cloud environments*. IEEE Transactions on Cloud Computing, 12(2), 512–525.
5. Guzman, A., & Rodriguez, M. (2023). *Stochastic and machine learning-driven threat containment models in virtualized infrastructures*. Computers & Security, 132, 103340.
6. Chen, H., Wang, J., & Li, D. (2024). *Behavioral analysis and mathematical formulation of cloud malware using attention-based hybrid networks*. Computers & Electrical Engineering, 114, 109052.

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

7. Sharma, R., & Patel, K. (2025). *Evaluating SOAR platforms and mathematical models for hypervisor-level automated malware containment*. Cybersecurity and Infrastructure Protection, 9(1), 88–104.
8. Kovacs, P., & Varga, T. (2025). *Container isolation and resource throttling mechanisms for ransomware mitigation in Kubernetes*. Journal of Information Security and Applications, 79, 103620.
9. Patel, V., & Kumar, R. (2025). *Lightweight convolutional neural networks for real-time memory introspection and malware classification in hypervisors*. IEEE Transactions on Dependable and Secure Computing, 22(3), 1450–1464.
10. National Institute of Standards and Technology (NIST). (2024). *Zero Trust Architecture and Network Micro-Segmentation Guide for Cloud Systems* (NIST SP 800-207A).
11. Smith, J. A., & Brown, L. K. (2023). *Ensemble learning methods: Combining Random Forest and Gradient Boosting for intrusion detection in cloud VMs*. Journal of Network and Computer Applications, 210, 103534.
12. Wang, X., Zhao, Y., & Liu, H. (2026). *Next-generation automated threat mitigation and micro-segmentation in software-defined data centers*. IEEE Communications Surveys & Tutorials, 28(1), 305–328.

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.