ISSN 2181-

КЎПМОДАЛЛИ ГЕНЕРАТИВ ФИРИБГАРЛИК: СУНЪИЙ ИНТЕЛЛЕКТ ОРҚАЛИ ЯНГИ АЛДАМЧИЛИК МОДЕЛИ

Ўзбекистон Республикаси Бош прокуратураси ҳузуридаги Иқтисодий жиноятларга қарши курашиш департаменти Сурхондарё вилояти бошқармаси Денов туман бўлими терговчиси, 2-даражали юрист

Азимов Хайрулло Ғайбуллаевич

Аннотация

Мақола замонавий рақамли муҳитда юзага келаётган янги турдаги фирибгарлик—кўпмодалли генератив фирибгарлик (КГФ)ни илмий-назарий жиҳатдан тавсифлайди. КГФ деганда сунъий интеллект (матн, овоз ва видео генерацияси) асосида ямалган, ижтимоий муҳандислик билан бирлашган ва жиноят жараёнини деярли тўлиқ автоматлаштирувчи алдамчиликлар тизими назарда тутилади. КГФнинг асосий характеристикаси – инсонни ишонтиришда бир вақтнинг ўзида бир нечта модалликни (матн, овоз, видео, ҳужжат) ишга солиши, KYC/AML текширувларини чеклаб ўтишга инфраструктура яратиши ва авторлаштирилган пўшт тўловлари (APP) каби механизмлардан фойдаланиб тезкор монетизацияга эришишидир. Мақолада КГФ учун таҳдид модели, ҳужум ҳаётий цикли, акторлар экотизими, ишонч алоқаларини бузиш усуллари ва рақамли шахсиятни бузиб кириш (дижитал идентитетни ўзлаштириш) сценарийлари назарий модел сифатида баён этилади. Шунингдек, ташкилотлар ва фуқаролар учун профилактика чоралари: овоз-клонга қарши “челленж-кодлар”, кўп омилли автентикация, транзакцияларнинг поведенциал биометрик таҳлили, реал вақтдаги аномалия детекцияси, ливерниесс-текширувлари ва медиа-ватермарк детекторларидан фойдаланиш каби механизмлар таклиф

қилинади. Мақола илмий-назарий характерга эга бўлиб, амалиётда синаш учун эмпирик тадқиқот дастури ва ўлчов кўрсаткичлари ҳам илгари сурилади.

Калит сўзлар

кўпмодалли генератив фирибгарлик; сунъий интеллект; дипфейк; овоз-клонлаш; авторлаштирилган пўшт тўлови (APP); рақамли шахсият; ижтимоий муҳандислик; киберхавфсизлик; аномалия детекцияси; поведенциал биометрика

Кириш

Сўнгги йилларда рақамли инфратузилманинг чуқур кириб бориши натижасида анъанавий фирибгарлик шакллари сунъий интеллект билан қўшилиб кетди. Матн-генерацияловчи моделлар, овозни клонлаш ва видео дипфейк технологиялари фуқаро ва ташкилотларни ишонтиришда янгича психологик таъсир доирасини яратади. Бу ҳолат алдамчиликнинг янги, кўпмодалли генератив босқичига ўтишини англатади. Мақоланинг долзарблиги шундаки, амалдаги кўплаб ҳимоя меъёрлари (масалан, фақат парол ёки фақат қўнғироқ орқали тасдиқ) бундай комплекс ҳужумларга қарши етарли эмас. Шу боис, КГФни тушунтирувчи назарий асос, таҳдид модели ва амалиётга йўналтирилган профилактика стратегиялари ишлаб чиқиш зарур.

Адабиётларни кўриб чиқиш

Кибержиноятчилик бўйича халқаро ҳисоботлар (масалан, полиция ва киберхавфсизлик агентликлари томонидан ҳар йили бериладиган таҳлиллар) онлайн молиявий фирибгарлик, ижтимоий муҳандислик ва дипфейк технологияларининг ўсишини қайд этмоқда. Иқтисодий зарарнинг асосий қисми авторлаштирилган пўшт тўловлари (APP) орқали амалга ошган ҳолатларга тўғри келади: қурбон ўз ўзига ишонган ҳолда тўлов қилади, кейин эса ўғирланган маблағларни қайтариш қийинлашади. Бироқ мавжуд адабиётларда кўпинча алоҳида технологиялар (масалан, фақат овоз-клон ёки фақат фишинг) ёритилади, уларнинг бир вақтнинг ўзида интеграцияланган, автоматлашган ҳужумлар экотизими сифатида таҳлили кам. Шу боис, ушбу ишда КГФ атамаси остида бирлаштирувчи назарий рамка таклиф этилади.

Асосий қисм

Методология

Тадқиқот тури — илмий-назарий. Унда таҳдид моделлаш, сценарийлар инженеринги ва ҳужум ҳаётий циклини (kill chain) концептуал яратиш усуллари қўлланилди. Шу билан бирга, амалиётга татбиқ этиш учун эмпирик дастур таклиф этилди: (i) назоратли қизил-жамоа симуляциялари; (ii) ҳодисалар журнали ва поведенциал биометрика маълумотларини анонимлаштириб таҳлил қилиш; (iii) инсон-омилга боғлиқ қарор нуқталарини психометрия орқали баҳолаш.

Натижалар: КГФ таҳдид модели ва ҳаётий цикл

1) Акторлар ва инфратузилма:

— Генератив муҳит: матн (чат-агент), овоз-клон, видео-дипфейк, ҳужжат генератори.

— Оркестрация: бир нечта агентни бирлаштирувчи сценарийлаштирилган бот-платформа.

— Ишонч каналлари: мессенжерлар, телефон, электрон почта, видеоконф.

— Монетизация: APP тўловлари, крипто алмашинуви, мултиқадам пул ювиш.

2) Ҳаётий цикл (KGF Kill Chain):

(a) Қидириш ва контекст йиғиш — қурбон ҳақида очиқ манбалардан маълумот йиғиш.

(b) Ишонтиришни бошлаш — овоз/видео дипфейк орқали ишончли шахсни тақлид қилиш.

(c) Ишончни мустаҳкамлаш — ҳужжат/скриншот генерацияси, қўнғироқлар занжири.

(d) Транзакцияга йўналтириш — APP, крипто ёки ҳимоясиз пул ўтказмаси.

(e) Изларни йўқотиш — мултиқадам китобот, мул-лар таратма ҳисоби.

3) Асосий сценарийлар:

— “Қариндош овози” сценариysi: тезкор пул сўрови билан қўнғироқ.

— “CFO-спуфинг” сценариуси: компанияда фавқулодда тўловни талаб қилиш.
— “KYC бузиб кириш” сценариуси: дипфейк видео билан ҳисоб очиш.

4) Муваффақият омиллари: кўпмодал таъсир, вақт босими, авторитетга суяниш, ҳуқуқий ва техник назорат нуқталарини айланиб ўтиш.

Профилактика ва муҳофаза архитектураси

— Инсон-омил: кодли сўров (қўнғироқда олдиндан келишилган “челленж-сўз”), икки канал орқали текшириш, тайёр сценарийлар асосида қоидалар.
— Техник: кўпомилли автентикация (парол+қурилма+биометрика), поведенциал биометрика, реал вақт аномалия детекцияси, тўлов лимитлари ва кечиктирилган тасдиқ, аппарат даражасида SIM-swap/номер клонини аниқлаш.
— Медиа хавфсизлиги: овоз/видео ливерниесс тестлари, дипфейк-ватермарк детекцияси, ҳужжат генерациясини анти-бот фильтрлари.
— Ташкилий: APP қайтариш протоколи, ходимлар учун симуляция ва тренинглар, инцидентларга жавоб бериш (IR) режалари.

Хулосалар

Кўпмодалли генератив фирибгарлик (КГФ) — сунъий интеллект орқали ижтимоий муҳандисликни кучайтирувчи, бир неча модалликни бирлаштирган ва жиноий жараённи оркестрациялайдиган янги алдамчилик модели сифатида таклиф этилди. Мақола КГФнинг акторлари, ҳаётий цикли ва ҳимоя чораларини назарий асосда байон қилди. Амалий босқичда КГФга қарши комплекс ёндашув — инсон, технология ва ташкилий сиёсатлар ўртасидаги узвий интеграцияни талаб қилади. Келгуси тадқиқотлар эмпирик симуляциялар, чегараларо маълумот алмашинуви ва хавфлар математик моделлашувига қаратилган бўлиши мақсадга мувофиқ.

Адабиётлар рўйхати

1. FBI Internet Crime Complaint Center (IC3). “Internet Crime Report 2024.”
2. Europol. “Internet Organised Crime Threat Assessment (IOCTA) 2024.”
3. ENISA. “Threat Landscape 2024.” European Union Agency for Cybersecurity.

4. INTERPOL. “Global Crime Trend Report 2024.”

5. NIST SP 800-63-3. “Digital Identity Guidelines.” National Institute of Standards and Technology.

6. ISO/IEC 30107 series. “Biometric presentation attack detection.” 2016–2023.