



RESURS JIHATDAN CHEKLANGAN IOT QURILMALARI UCHUN YENGIL
KIRISHNI ANIQLASH TIZIMLARI: RESURS BYUDJETIGA ASOSLANGAN
QAROR QABUL QILISH MODELI

Maxamatjonov Ismoil Dilshod o'g'li

«Kiberxavfsizlik va kriminalistika» kafedrası o'qituvchisi,
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti.
ORCID: 0009-0005-7144-8798

Annotatsiya. Internet buyumlar (IoT) qurilmalarining xotira, hisoblash quvvati va energiya iste'moli bo'yicha qattiq cheklovlari ularda an'anaviy, resurs talab qiluvchi kirishni aniqlash tizimlarini (IDS) to'g'ridan-to'g'ri joylashtirishni amaliy jihatdan imkonsiz qiladi. Bu esa mazkur qurilmalarni ilg'or doimiy tahdidlar, xizmat ko'rsatishni rad etish (DoS/DDoS) hujumlari va ma'lumotlar sizib chiqishiga nisbatan zaif qoldiradi.

Ushbu maqolada resurs jihatdan cheklangan qurilmalar uchun yengil IDS (L-IDS) yondashuvlari tizimli adabiyotlar tahlili asosida ko'rib chiqiladi. Shuningdek, qurilmaning resurs byudjeti hamda mahalliy tasniflash bilan bulutga topshirish o'rtasidagi tanlovni tavsiflovchi rasmiy model taklif etiladi. Ko'rib chiqilgan natijalarga ko'ra:

- CatBoost asosidagi tasniflagich ESP32 mikrokontrollerida 276 mikrosoniyalik kechikish bilan 99 foizga yaqin aniqlikka erishadi;
- Bilim distillyatsiyasi chuqur model parametrlari sonini 70 foizga qisqartirib, STM32L4 platformasida 10 millisoniyadan kam xulosa chiqarish vaqtini ta'minlaydi;
- Dinamik kvantlash esa model hajmini 4 MB dan 512 KB gacha siqib, aniqlikni taxminan 92 foiz darajasida saqlab qoladi;
- Federativ edge-cloud arxitekturasi 95,6 foizlik aniqlikka erishishga, FPGA asosidagi Modbus yechimi esa o'tkazuvchanlikni uch baravar oshirib, protsessor yukini 50 foizdan 15 foizgacha kamaytirishga imkon beradi.

Ushbu natijalar resurs byudjetini uchlik ko'rinishida rasmiylashtirish va ishonch darajasiga asoslangan edge-cloud qaror qabul qilish qoidasini taqdim etish uchun asos bo'lib xizmat qiladi.

Kalit so'zlar: Internet buyumlar xavfsizligi, yengil kirishni aniqlash tizimi, resurslari cheklangan qurilmalar, modelni siqish, edge-cloud arxitekturasi, qaror qabul qilish qoidasi.

Kirish

Internet buyumlar (IoT) qurilmalari bugungi kunda salomatlikni masofadan kuzatish, sanoat boshqaruvi va past quvvatli sensor tarmoqlarining asosini tashkil etadi. Biroq ularning xotira, hisoblash quvvati va energiya bo'yicha qattiq cheklovlari ushbu qurilmalarni ilg'or doimiy tahdidlar, xizmat ko'rsatishni rad etish (DoS/DDoS) hujumlari va ma'lumotlar sizib chiqishi uchun jozibador hamda ko'pincha oson nishonga aylantiradi [1]. An'anaviy, resurs



talab qiluvchi yuqori sig'imli IDS yechimlarini bunday qurilmalarda bevosita joriy etish amaliy jihatdan imkonsiz bo'lib qolmoqda. Shu sababli yengil IDS (L-IDS) yo'nalishi mustaqil tadqiqot maydoniga aylandi.

Mensah, Makhamatdjonov, Jin va Yu (2025) tomonidan o'tkazilgan tizimli tadqiqot [1] L-IDS aniqlash usullarini signaturalarga asoslangan (misuse-based) va anomaliyalarga asoslangan (anomaly-based) turlarga ajratadi hamda ularning kechikish, model hajmi, energiya iste'moli va aniqlik bo'yicha o'zaro muvofiqchilik (trade-offs) taqqoslaydi. Alohida olganda, yengil usullar protokolga xos nihoyatda qattiq byudjetlarga javob bera oladi. Masalan, 500 KB SRAMga ega ESP32 mikrokontrollerida ishlagan CatBoost asosidagi tasniflagich DoS/MITM hujumlarini 99 foizdan ortiq aniqlik bilan, atigi 276 mikrosaniyalik kechikishda aniqlagan [2]. Bilim distillyatsiyasi chuqur aniqlash modelining parametrlar sonini 70 foizga qisqartirib, STM32L4 mikrokontrollerida 10 millisoniyadan kam xulosa chiqarish vaqtini ta'minlagan [3], dinamik kvantlash esa modelni 4 MB dan 512 KB gacha kichraytirib, taxminan 92 foizlik aniqlikni saqlab qolgan [4].

Signaturaga asoslangan usullar ma'lum hujumlarda yuqori aniqlik va past yolg'on signal darajasini ta'minlaydi, biroq ular nol kunlik (zero-day) hujumlarni yomon qamrab oladi va signatura bazasini doimiy yangilab turishni talab qiladi. Anomaliyaga asoslangan usullar esa, aksincha, ko'rilmagan hujumlarga yaxshi umumlashadi, lekin ularda yolg'on signal darajasi va o'qitish xarajati yuqoriroq bo'ladi [1]. Shu sababli eng kuchli so'nggi takliflar ikkala yondashuvni — ko'pincha CNN-BiLSTM yoki chuqur o'qitish va avtoenkoder asosidagi gibril arxitekturalarni — model siqish texnikalari bilan birgalikda qo'llaydi. Baholashda odatda CICIDS2017, UNSW-NB15 va Edge-IIoTset kabi etalon ma'lumotlar to'plamlaridan foydalaniladi, biroq bu to'plamlar asosan hajmli yoki signaturasi aniq ko'rinadigan hujumlarni (DoS, port skanerlash) qamrab oladi [1].

Protokol darajasida resurs chegaralari ham keskin farqlanadi: MQTT uchun 16 KB model byudjeti va soatiga 1 mAh dan kam energiya sarfi doirasida 5 millisoniyadan kam kechikish talab etilsa, Modbus 256 KB va 50 mVt doirasida 10 mikrosaniyadan kam kechikishni talab qiladi. LoRaWAN 128 KB byudjet va kuniga 0,5 mAh doirasida 300 millisoniyagacha kechikishga yo'l qo'yadi, CoAP esa 8 KB va 500 mikroamper doirasida 20 millisoniyadan kam kechikishni talab qiladi [1]. Demak, har bir protokol o'ziga xos resurs chegaralariga ega va barcha holatlar uchun yagona mos model arxitekturasini mavjud emas.

Bu natijalarni umumlashtirish uchun qurilmaning resurs byudjetini uchlik ko'rinishida ifodalash qulay: $B = (M_{\max}, T_{\max}, E_{\max})$, bunda $M_{\max}$ — ruxsat etilgan maksimal model hajmi, $T_{\max}$ — maksimal xulosa chiqarish kechikishi, $E_{\max}$ — maksimal energiya sarfi. Berilgan M modeli protokolga joriy etish uchun yaroqli hisoblanadi, agar uning hajmi, kechikishi va energiya sarfi mos ravishda shu uchta chegaradan oshmasa:

$$\text{Valid}(M) \Leftrightarrow \text{size}(M) \leq M_{\max} \wedge T(M) \leq T_{\max} \wedge E(M) \leq E_{\max} \quad (1)$$

Bu shart kon'yunksiya sifatida qurilgan: modelning faqat bitta ko'rsatkich bo'yicha ustunligi (masalan, yuqori aniqlik) qolgan chegaralardan birortasi buzilgan taqdirda uni



qurilmaga yaroqsiz qiladi. 1-jadvalda ikkita keng tarqalgan IoT protokoli — MQTT va Modbus — uchun shu uchlikning qiymatlari keltirilgan [1].

1-jadval.

MQTT va Modbus protokollari uchun resurs byudjeti $B = (M_{\max}, T_{\max}, E_{\max})$

Protokol	$T_{\max}$ (kechikish)	$M_{\max}$ (model hajmi)	$E_{\max}$ (energiya)	Maqsadli qurilma
MQTT	< 5 ms	16 KB	< 1 mAh/soat	ESP32
Modbus	< 10 μ s	256 KB	< 50 mVt	Raspberry Pi / FPGA shlyuzi

E'tiborlisi, $B = (M_{\max}, T_{\max}, E_{\max})$ chegaralari protokoldan protokolga keskin farq qiladi: Modbus uchun kechikish chegarasi mikrosoniyalar darajasida bo'lsa, MQTT uchun millisoniyalar darajasida, biroq MQTTda model hajmi va energiya chegaralari ancha qattiqroq. Bu farq barcha protokollar uchun yagona universal L-IDS yechimi mavjud emasligini, aksincha, har bir protokol uchun alohida Valid(M) tekshiruvdan o'tgan model tanlanishi lozimligini ko'rsatadi.

Qurilma resurslari qanchalik puxta optimallashtirilmasin, yengil model butun tarmoq trafigini bir xil ishonch darajasida tasniflay olmasligi mumkin. Shu sababli so'nggi ishlarda edge qatlamidagi tezkor tasniflashni bulutdagi kengroq hisoblash resurslariga ega tahlil bilan birlashtiruvchi federativ edge-cloud arxitekturasini taklif qilingan; bu yondashuv taxminan 95,6 foizlik umumiy aniqlikka erishgan [5]. Bunday arxitektura asosiy muammo — qaysi holatlarni qurilmaning o'zi hal qilishi, qaysilarini esa bulutga topshirish kerakligini aniqlashdir.

Buni rasmiylashtirish uchun x xususiyatlar vektori bo'yicha chekka (edge) modeli M_{edge} hisoblagan ishonch darajasi $c(x) \in [0, 1]$ va oldindan belgilangan chegara qiymati θ kiritiladi. $D(x)$ qaror funksiyasi quyidagicha aniqlanadi:

$$D(x) = \begin{cases} \text{mahalliy, agar } c(x) \geq \theta \wedge \text{Valid}(M_{\text{edge}}); \\ \text{bulutga yuborish, aks holda.} \end{cases} \quad (2)$$

$D(x)$ qoidasi ikki shartning kon'yunksiyasiga tayanadi: model nafaqat yetarli ishonch bilan tasniflashi, balki (1)-tenglamadagi resurs byudjetiga ham mos kelishi kerak. Agar $c(x)$ past bo'lsa yoki M_{edge} joriy qurilmada $\text{Valid}(M_{\text{edge}})$ shartini qanoatlantirmasa, qaror bulutga topshiriladi. Bu federativ arxitekturaning yuqori aniqligini [5] mahalliy modelning qattiq resurs chegaralari bilan muvofiqlashtirish imkonini beradi. θ qiymatini tanlash aniqlik va kechikish o'rtasidagi amaliy murosaga bog'liq: past θ ko'proq holatni mahalliy hal qiladi va mahalliy xatolik ehtimolini oshiradi, yuqori θ esa ko'proq holatni bulutga yo'naltirib, tarmoq kechikishini oshiradi.

Masalan, ESP32 platformasida ishlaydigan CatBoost asosidagi M_{edge} 276 mikrosoniyalik kechikishda yuqori ishonch bilan tasniflagan trafik uchun $D(x)$ mahalliy qarorni tanlaydi:



bunday kechikish MQTT uchun belgilangan $T_{\max} = 5 \text{ ms}$ chegarasidan ancha past [2], shuning uchun model hajmi va energiya sarfi ham chegaradan oshmasa, $\text{Valid}(M_{\text{edge}})$ sharti bajariladi. Biroq o'qitish ma'lumotlarida kam uchraydigan yoki yangi hujum turiga oid trafik uchun $c(x)$ past bo'ladi, chunki model bunday naqshlarni ishonchli tasniflashga o'rgatilmagan. Bunday holatda $D(x)$ qarorni bulutga yo'naltiradi va u yerda kengroq hisoblash resurslariga ega, ehtimol federativ tarzda o'qitilgan model [5] qo'shimcha tahlil o'tkazadi. Shu tariqa $D(x)$ qoidasi mahalliy tezkorlik bilan bulut aniqligi o'rtasidagi muvozanatni avtomatik ta'minlaydi, bu esa qo'lda sozlanadigan statik chegaralarga nisbatan ustunlikdir.

Apparat darajasidagi optimallashtirish ham shu byudjet mantig'iga mos keladi. Modbus protokoli uchun FPGA asosida amalga oshirilgan funksiya kodlarini filtrlash o'tkazuvchanlikni uch baravar oshirib, protsessor yukini 50 foizdan 15 foizgacha kamaytirgan [6]; bu $T(M)$ va $E(M)$ qiymatlarini bir vaqtda pasaytirib, $\text{Valid}(M)$ sharti kengroq model sinflari uchun bajarilishini ta'minlaydi. Shu bilan birga, rejalashtirishga asoslangan moslashuvchan model boshqaruvi joriy batareya va xotira zaxirasiga qarab qaysi anomaliya modelini yuklangan holda saqlashni tanlaydi va shu orqali $M_{\max}$ hamda $E_{\max}$ chegaralarining vaqt bo'yicha o'zgarishini hisobga oladi [10].

Aniqlash usullarining o'zi ham xilma-xil: CNN-BiLSTM gibrid arxitekturasini UNSW-NB15 to'plamida yaxshi natija ko'rsatgan bo'lsa-da, NSL-KDD to'plamiga yomon umumlashgan, bu esa uning barqarorligida muammolar borligidan dalolat beradi [7]. Sinflar nomutanosibligini S2CGAN asosida hal qiluvchi yondashuv [8], ko'rilmagan hujum turlari uchun ochiq to'plamli aniqlash sxemasi [9] va mikrokontrollerlarda TinyML yordamida ishlaydigan TinyIDS tizimi [11] ham shu resurs–aniqlik murosasi doirasida taklif etilgan. Biroq o'rganilgan adabiyotlarda aniqlash qiyinroq bo'lgan hujum turlari — o'rtadagi odam (MITM) hujumi, Heartbleed uslubidagi protokol zaifliklaridan foydalanish va fidya dasturiga (ransomware) o'xshash ma'lumot sizib chiqishi — o'qitish ma'lumotlarida ham, baholashda ham izchil ravishda yetarlicha e'tiborga olinmagan [1].

2-jadval.

L-IDS uchun qo'llanilgan yengillashtirish usullari va erishilgan natijalar

Usul	Erishilgan natija	Platforma
CatBoost tasniflagich [2]	~99% aniqlik, 276 μs kechikish	ESP32
Bilim distillyatsiyasi [3]	parametrlar ~70% kamaygan, < 10 ms kechikish	STM32L4
Dinamik kvantlash [4]	4 MB $\rightarrow$ 512 KB, ~92% aniqlik saqlangan	ko'rsatilmagan
Federativ edge-cloud [5]	~95,6% aniqlik	edge-cloud
FPGA asosidagi Modbus [6]	o'tkazuvchanlik 3 $\times$, CPU yuki 50% $\rightarrow$ 15%	FPGA shlyuzi



2-jadvaldagi natijalar shuni ko'rsatadiki, bu besh usulning har biri $B = (M_{\max}, T_{\max}, E_{\max})$ byudjetining faqat bir yoki ikki o'lchamiga ta'sir qiladi va hech biri uchala o'lchamni bir vaqtda optimallashtirmaydi. Model siqish usullari (bilim distillyatsiyasi, dinamik kvantlash) asosan $size(M)$ va $T(M)$ ni kamaytiradi, chunki kichikroq model odatda tezroq hisoblanadi. Apparat tezlashtirish (FPGA) $T(M)$ va $E(M)$ ni bir vaqtda pasaytiradi, chunki maxsus mantiqiy sxema umumiy maqsadli protsessorga qaraganda kamroq takt va energiya sarflaydi. Federativ edge-cloud arxitekturasida esa model ko'rsatkichlarini o'zgartirmaydi, balki $D(x)$ qoidasi orqali qiyin holatlarni boshqa resurs muhitiga — bulutga — ko'chirib, aniqlikni oshiradi. Shu sababli bu usullar o'zaro almashtiriluvchi emas, balki bir-birini to'ldiruvchi hisoblanadi va amaliy L-IDS tizimi ularni (1)-tenglamadagi byudjet va (2)-tenglamadagi qaror qabul qilish mantig'i orqali birlashtirgan holda qo'llashi lozim.

L-IDS qurilmalari ko'pincha xabar almashinuv kanalini himoya qilish uchun yengil kriptografik primitivlarga ham muhtoj, chunki to'liq TLS stekini ishga tushirish xuddi shu $M_{\max}$ va $E_{\max}$ chegaralarini buzishi mumkin. AQSh Milliy standartlar va texnologiyalar instituti (NIST) 2025-yilda e'lon qilgan Ascon asosidagi yengil kriptografiya standarti aynan shunday cheklangan qurilmalar uchun autentifikatsiyalangan shifrlash va xesh funksiyalarini ta'minlashga qaratilgan [12]. Bu L-IDS resurs byudjeti bilan bir xil muammo maydonida yotadi: xavfsizlik mexanizmi o'zi himoya qilayotgan qurilmaning resurslarini tugatib qo'ymasligi kerak. ISO/IEC 27400:2022 standarti ham IoT qurilmalarining butun hayotiy sikli davomida xavfsizlik va maxfiylik bo'yicha yo'riqnomalarni belgilaydi hamda resurslari cheklangan qurilmalarda xavfsizlik mexanizmlarini qurilmaning real imkoniyatlariga moslashtirish zarurligini ta'kidlaydi [13]; bu esa taklif etilgan $Valid(M)$ shartining kengroq me'yoriy asosga mos ekanini ko'rsatadi.

Taklif etilgan $B = (M_{\max}, T_{\max}, E_{\max})$ va $D(x)$ formalizatsiyasini sinab ko'rish uchun ikkita sinov stendi mos keladi: ESP32 darajasidagi mikrokontrollerga asoslangan MQTT sensor tuguni va Raspberry Pi darajasidagi shlyuzga asoslangan Modbus konfiguratsiyasi, chunki aynan shu ikki protokol uchun 1-jadvaldagi aniq, manbaga tayangan kechikish, xotira va energiya ko'rsatkichlari mavjud [1]. Baholash trafigi an'anaviy DoS va skanerlash hujumlaridan tashqari adabiyotlarda yetarlicha e'tiborga olinmagan uchta sinfni ham o'z ichiga olishi lozim [1]: ARP/ICMP-redirect uslubidagi MITM trafigi, protokol shlyuziga qarshi qayta yuborilgan noto'g'ri handshake/heartbeat so'rovlari (Heartbleed sinfi) va bosqichma-bosqich katta hajmli yuklama ko'rinishidagi fidya dasturiga o'xshash sizib chiqish trafigi. Bunday kengaytirilgan stseneriy $D(x)$ qoidasining aynan yangi, ko'rilmagan hujum turlarida qanchalik to'g'ri ishlashini, ya'ni past ishonch darajasiga ega holatlarni bulutga to'g'ri yo'naltirishini tekshirish imkonini beradi.

Taklif etilgan modelning bir qancha cheklovlari ham mavjud. Birinchidan, sintetik tarzda yaratilgan Heartbleed sinfidagi va fidya dasturiga o'xshash trafik haqiqiy tajovuzkorning moslashuvchan xatti-harakatini to'liq aks ettirmasligi mumkin, shuning uchun $D(x)$ asosidagi baholash natijalarini haqiqiy sharoitdagi ishlash kafolati sifatida emas, balki aniqlash



qiyinligining quyi chegarasi sifatida talqin qilish kerak. Ikkinchidan, qaysi modelni yuklangan holda saqlashni tanlovchi ish vaqti siyosatining o'zi qo'shimcha xotira va hisoblash yukini talab qiladi; buni MQTTning soatiga 1 mAh dan kam energiya chegarasi kabi allaqachon qattiq $M_{\max}$ va $E_{\max}$ cheklovlari doirasida alohida hisobga olish shart. Uchinchidan, qamrov ataylab ikki protokol — MQTT va Modbus — bilan cheklangan; yondashuvni LoRaWAN va CoAP kabi boshqa protokollarga umumlashtirish kelajakdagi ishlar vazifasidir.

Xulosa

Resurslari cheklangan IoT qurilmalari uchun yengil kirishni aniqlash sohasida alohida model siqish va apparat tezlashtirish usullari yaxshi o'rganilgan, biroq ularni yagona, protokolga moslashuvchan qaror qabul qilish mantig'iga birlashtirish hali to'liq hal etilmagan masala bo'lib qolmoqda. Ushbu maqolada taklif etilgan $B = (M_{\max}, T_{\max}, E_{\max})$ resurs byudjeti va unga asoslangan $\text{Valid}(M)$ hamda $D(x)$ formalizatsiyasi mavjud empirik natijalarni — CatBoost tasniflagichining 276 mikrosoniyalik kechikishidan tortib federativ edge-cloud arxitekturasining 95,6 foizlik aniqligigacha — yagona analitik asosda birlashtirish imkonini beradi.

Taklif etilgan formalizatsiyaning amaliy qiymati shundaki, u model siqish, apparat tezlashtirish va edge-cloud hamkorligini raqobatdosh emas, balki bir-birini to'ldiruvchi vositalar sifatida ko'rsatadi: ularning har biri $B = (M_{\max}, T_{\max}, E_{\max})$ uchligining turli o'lchamiga ta'sir qiladi, $D(x)$ esa ularni yagona amaliy qaror qoidasiga bog'laydi. Keyingi bosqichda ushbu model qurilma buzilgandan keyin eng xavfli bo'lgan MITM, Heartbleed uslubidagi va fidya dasturiga o'xshash hujum turlarini o'z ichiga olgan kengaytirilgan baholash stsenariysi asosida ESP32 asosidagi MQTT va Raspberry Pi asosidagi Modbus sinov stendlarida sinovdan o'tkazilishi rejalashtirilgan. Shu tariqa ushbu ish adabiyotlarda aniqlangan bo'shliqni protokolga moslashuvchan, formal asoslangan va sinovdan o'tkazish mumkin bo'lgan aniq ilmiy hissaga aylantirishni maqsad qiladi.

Foydalanilgan adabiyotlar

[1] Mensah, C., Makhamatdjonov, I., Jin, H., & Yu, S. (2025). SoK: Lightweight intrusion detection and automated response for resource-constrained IoT embedded systems [Unpublished coursework report, COM6017: Security of Control and Embedded Systems]. University of Sheffield.

[2] Chiba, Z., Abghour, N., Moussaid, K., Lifandali, O., & Kinta, R. (2022). Review of recent intrusion detection systems and intrusion prevention systems in IoT networks. In 2022 International Conference on Software, Telecommunications and Computer Networks (SoftCOM) (pp. 1–6).



- [3] Hasan, T., Hossain, A., Ansari, M. Q., & Syed, T. H. (2025). Enhanced intrusion detection in IIoT networks: A lightweight approach with autoencoder-based feature learning (arXiv:2501.15266). arXiv. <https://doi.org/10.48550/arXiv.2501.15266>
- [4] Wang, Z., Chen, H., Yang, S., Luo, X., Li, D., & Wang, J. (2023). A lightweight intrusion detection method for IoT based on deep learning and dynamic quantization. *PeerJ Computer Science*, 9, e1569. <https://doi.org/10.7717/peerj-cs.1569>
- [5] Belarbi, O., Spyridopoulos, T., Anthi, E., Mavromatis, I., Carnelli, P., & Khan, A. (2023). Federated deep learning for intrusion detection in IoT networks. In *GLOBECOM 2023 – 2023 IEEE Global Communications Conference* (pp. 237–242).
- [6] Mofidi, F., Hounsinnou, S., & Bloom, G. (2023). L-IDS: A lightweight hardware-assisted IDS for IoT systems to detect ransomware attacks. In *Proceedings of the 8th ACM/IEEE Conference on Internet of Things Design and Implementation (IoTDI '23)* (pp. 464–465). ACM. <https://doi.org/10.1145/3576842.3589170>
- [7] Jouhari, M., & Guizani, M. (2024). Lightweight CNN-BiLSTM based intrusion detection systems for resource-constrained IoT devices. In *2024 International Wireless Communications and Mobile Computing (IWCMC)* (pp. 1558–1563).
- [8] Wang, C., Xu, D., Li, Z., & Niyato, D. (2024). Effective intrusion detection in highly imbalanced IoT networks with lightweight S2CGAN-IDS. *IEEE Internet of Things Journal*, 11, 15140–15151.
- [9] Yang, X., Tong, F., Jiang, F., & Cheng, G. (2025). A lightweight and dynamic open-set intrusion detection for industrial internet of things. *IEEE Transactions on Information Forensics and Security*, 20, 2930–2943.
- [10] Mirzaei, A., Coban, A. Z., Almgren, M., Aoudi, W., & Bertilsson, T. (2023). Scheduling to the rescue: Improving ML-based intrusion detection for IoT. In *Proceedings of the 16th European Workshop on System Security (EuroSec '23)* (pp. 44–50). ACM.
- [11] Fusco, P., Rimoli, G. P., & Ficco, M. (2024). TinyIDS — An IoT intrusion detection system by tiny machine learning. In *Computational Science and Its Applications – ICCSA 2024 Workshops* (pp. 71–82). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-65223-3_5
- [12] National Institute of Standards and Technology. (2025). Ascon-based lightweight cryptography standards for constrained devices: Authenticated encryption, hash, and extendable output functions (NIST Special Publication 800-232). <https://doi.org/10.6028/NIST.SP.800-232>
- [13] International Organization for Standardization & International Electrotechnical Commission. (2022). Cybersecurity — IoT security and privacy — Guidelines (ISO/IEC 27400:2022). ISO.