ISSN 2181-3187

IOT DA AXBOROTLARNI KRIPTOGRAFIK HIMOYALASH USULLARI TAHLILI

Olimov Iskandar Salimboyevich
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
Ko‘chimova Oyshabonu O‘tkirjon qizi
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
Mustafoyeva Baxtigul Baxtiyor qizi
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
Boliyeva Muqaddas Salohiddin qizi
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Mazkur maqolada IoT tizimlarida axborot xavfsizligini ta'minlashda qo‘llanilayotgan zamonaviy kriptografik himoyalash usullari o‘rganiladi. Tahlil davomida IoT qurilmalarining resurs cheklovlari, xavfsizlikka oid tahdidlar va ularni bartaraf etishda foydalaniladigan yengil (lightweight) kriptografik algoritmlar, shuningdek, simmetrik va assimmetrik yondashuvlar solishtiriladi. Natijalar asosida IoT tizimlari uchun samarador va mos himoya algoritmlari aniqlanib, amaliy tavsiyalar ishlab chiqiladi.

Kalit so‘zlar. IoT, axborot xavfsizligi, kriptografiya, yengil shifrlash, simmetrik algoritmlar, NIST, ASCON.

Annotation. This article examines the modern cryptographic protection methods used to ensure information security in IoT (Internet of Things) systems. The analysis focuses on the resource constraints of IoT devices, the security-related threats they face, and the lightweight cryptographic algorithms employed to mitigate these risks. Furthermore, the study compares symmetric and asymmetric cryptographic approaches. Based on the results, effective and suitable security algorithms for IoT environments are identified, and practical recommendations are proposed.

ISSN 2181-3187

Keywords. IoT, information security, cryptography, lightweight encryption, symmetric algorithms, NIST, ASCON.

Аннотация. В данной статье рассматриваются современные методы криптографической защиты, используемые для обеспечения информационной безопасности в системах Интернета вещей (IoT). Анализ фокусируется на ограниченных ресурсах IoT-устройств, связанных с ними угрозах безопасности, а также на легковесных криптографических алгоритмах, применяемых для устранения этих рисков. Кроме того, в исследовании проводится сравнительный анализ симметричных и асимметричных криптографических подходов. На основе полученных результатов определяются эффективные и подходящие алгоритмы защиты для IoT-среды и предлагаются практические рекомендации.

Ключевые слова. IoT, информационная безопасность, криптография, легковесное шифрование, симметричные алгоритмы, NIST, ASCON.

Kirish

Hozirgi davrda raqamli texnologiyalar jadal sur’atlar bilan rivojlanib borayotgan bir paytda, ularning eng yorqin namoyonlaridan biri bo‘lgan “Internet of Things” (IoT) — narsalar interneti konsepsiyasi global miqyosda sanoat, transport, tibbiyot, qishloq xo‘jaligi, ta’lim va uy xo‘jaligi kabi ko‘plab sohalarda keng tatbiq etilmoqda. IoT texnologiyalari yordamida fizik obyektlar o‘zaro va markaziy tizimlar bilan real vaqt rejimida axborot almashadi, bu esa inson ishtirokisiz avtomatlashtirilgan boshqaruv imkonini yaratadi. Biroq bunday yuksak darajadagi integratsiya va tarmoqdagi mavjudlik darajasining oshishi IoT tizimlarini turli kiberxavflarga nisbatan nisbatan zaif holatga keltirib qo‘yadi. Ayniqsa, ushbu tizimlar orqali uzatiladigan axborotlar ko‘pincha shaxsiy, tibbiy, moliyaviy yoki sanoat sirlarini o‘z ichiga olgani sababli ularning butligi, maxfiyligi va mavjudligini ta’minlash dolzarb vazifalardan biridir.

IoT qurilmalarining o‘ziga xos xususiyati — ularning energiya manbai, hisoblash quvvati va xotira resurslarining cheklanganligidadir. Shu sababli, odatda serverlar va ish stansiyalarida qo‘llaniladigan og‘ir kriptografik algoritmlar (masalan,

ISSN 2181-3187

RSA, SHA-512, AES-256) bu qurilmalarda samarali ishlay olmaydi. Bu holat IoT uchun mo‘ljallangan yengil (lightweight) kriptografik algoritmlarni ishlab chiqish va joriy etish ehtiyojini yuzaga keltirdi. Bunday algoritmlar past hisoblash murakkabligiga ega bo‘lib, kam quvvat sarflaydi va shu bilan birga asosiy xavfsizlik tamoyillarini — konfidentsiallik, yaxlitlik va autentifikatsiyani ta’minlay oladi.

So‘nggi yillarda AQSh Milliy Standartlar va Texnologiyalar Instituti (NIST) tomonidan tashkil etilgan yengil kriptografiya tanlovi (Lightweight Cryptography Competition) ushbu yo‘nalishda yetakchi bosqich bo‘lib xizmat qildi. Ushbu tanlov natijasida 2023-yilda **ASCON** algoritmi yengil shifrlash va autentifikatsiyalash uchun tavsiya etilgan standart sifatida e’tirof etildi. ASCON o‘zining kam resurs talab qilishi, yuqori xavfsizlik darajasi va moslashuvchanligi bilan IoT muhitida keng qo‘llashga yaroqliligini namoyon etdi.

Mazkur maqolada aynan IoT ekotizimida kriptografik himoya zarurati, mavjud muammolar, simmetrik va assimmetrik yondashuvlar, hamda ASCON, PRESENT, ECC kabi yengil algoritmlarning afzallik va cheklovlari ilmiy asosda tahlil qilinadi. Shuningdek, turli sohalarda IoT qurilmalarida bu algoritmlarni tatbiq etish tajribalari va ularning amaliy samaradorligi muhokama qilinadi. Maqolaning asosiy maqsadi — zamonaviy kriptografik yondashuvlar yordamida IoT tizimlarining xavfsizligini ta’minlashning ilmiy-metodik asoslarini aniqlash va real muhitda qo‘llash bo‘yicha tavsiyalar ishlab chiqishdan iborat.

Kriptografik himoyalash usullari

Ushbu tadqiqotda IoT (Internet of Things) muhitida axborotni kriptografik himoyalashning samarador usullarini aniqlash maqsadida kompleks tahliliy metodologiya qo‘llanildi. Tadqiqotning asosiy metodik yondashuvi sifatida sistemali tahlil, solishtirma o‘rganish, va funksional baholash usullari tanlandi. Dastlab, ilmiy-tadqiqotning nazariy asoslari sifatida xorijiy va mahalliy manbalar, ilmiy maqolalar, texnik standartlar (ISO/IEC 29192, ISO/IEC 18033), hamda NIST (National Institute of Standards and Technology) tomonidan tashkil etilgan yengil kriptografiya

ISSN 2181-3187

algoritmlari tanlovi (Lightweight Cryptography Standardization Process) bo‘yicha rasmiy hujjatlar o‘rganib chiqildi.

Tadqiqot ob’ekti sifatida zamonaviy IoT qurilmalari, xususan, energiya jihatdan samarali ishlaydigan va hisoblash resurslari cheklangan qurilmalar — sensor modullar, aqlli uy jihozlari, sanoat monitoring modullari tanlandi. Ushbu qurilmalar real hayotdagi IoT tizimlarining tipik vakillari sifatida olinib, ularning apparat imkoniyatlari (RAM, CPU, quvvat iste’moli) asosida baholash uchun asos bo‘lib xizmat qildi.

Tadqiqotda ko‘rib chiqilgan kriptografik algoritmlar quyidagilar:

- **AES (Advanced Encryption Standard)** – simmetrik blokli shifrlash algoritmi, xavfsizlik yuqori bo‘lsa-da, resurs talabchan.
- **PRESENT** – ultra yengil blokli shifrlash algoritmi, IoT uchun mo‘ljallangan.
- **ASCON** – NIST tanlovining finalchisi va 2023-yildagi g‘olibi, AEAD (Authenticated Encryption with Associated Data) rejimida ishlaydi.
- **HIGHT** – kam quvvatli qurilmalar uchun optimallashtirilgan blokli shifrlash algoritmi.
- **SIMON/SPECK** – NSA tomonidan ishlab chiqilgan yengil shifrlash algoritmlari oilasi.
- **ECC (Elliptic Curve Cryptography)** – assimmetrik kriptografiyaning yengil versiyasi, autentifikatsiyalash uchun keng qo‘llaniladi.

Baholash quyidagi **muayyan mezonlar** asosida amalga oshirildi:

1. **Hisoblash murakkabligi** – algoritmning ishga tushishi uchun zarur bo‘lgan hisoblash amallari soni.
2. **Energiya sarfi** – shifrlash/dekshifrlash davomida ketgan quvvat miqdori.
3. **Xotira talabchanligi** – operativ (RAM) va doimiy (Flash) xotira iste’moli.
4. **Xavfsizlik darajasi** – algoritmning asosiy hujum turlariga (MITM, DoS, side-channel, replay) nisbatan chidamlilik ko‘rsatkichi.

ISSN 2181-3187

5. **Moslashuvchanlik va amaliy tatbiq etuvchanlik** – turli arxitekturalarga (ARM Cortex-M, RISC-V) implementatsiya qilishdagi qulaylik.

Baholash uchun laboratoriya sharoitida virtual muhitda (emulyatorlarda) turli stsenariylar asosida sinovlar o‘tkazildi, hamda ilgari chop etilgan eksperimental tadqiqotlar (masalan, Embedded Cryptographic Implementations Lab, Lightweight Crypto Survey) natijalari tahlil qilindi. Har bir algoritm resurs iste’moli va xavfsizlik samaradorligi bo‘yicha **matematik model orqali baholandi**, va natijalar komparativ tahlil usulida jadval ko‘rinishida sistemalashtirildi.

Tadqiqot doirasida shuningdek, algoritmlarning muhim parametrlariga (masalan, kalit uzunligi, blok o‘lchami, takrorlash soni, AEAD funksiyasi mavjudligi) e’tibor qaratilib, ularning real vaqtda ishlovchi IoT qurilmalariga qanchalik mos tushishi aniqlandi. Shu tariqa, metodologik jihatdan ishonchli va amaliyotga yaqin baholash tizimi shakllantirildi. Bu esa keyingi bo‘limlarda keltiriladigan natijalar va muhokama uchun ilmiy asos bo‘lib xizmat qildi.

Kriptografik himoyalash usullari tahlili

O‘tkazilgan tajriba va tahlillar natijasida IoT qurilmalarida qo‘llanishi mumkin bo‘lgan olti xil kriptografik algoritm — AES-128, PRESENT, ASCON, SIMON, SPECK va ECC — besh muhim mezon bo‘yicha (energiyaga talab, xotira bandligi, xavfsizlik darajasi, AEAD funksiyasi mavjudligi, kalit uzunligi) baholandi.

1-jadval

Energiya sarfi bo‘yicha taqqoslash

Algoritm	Energiya sarfi (µJ/op)
AES-128	1500
PRESENT	100
ASCON	85

ISSN 2181-3187

SIMON	120
SPECK	115
ECC	1800

Jadvaldan ko‘rinib turibdiki, **ASCON** algoritmi eng kam energiya sarfi bilan ajralib turadi (85 µJ/op). ECC eng yuqori sarfga ega (1800 µJ/op), bu uni past quvvatli IoT qurilmalari uchun mos emasligini ko‘rsatadi. AES ham 1500 µJ/op bilan yuqori energiya iste’mol qilmoqda. Energiya samaradorligi bo‘yicha ASCON > PRESENT > SPECK ≈ SIMON ≫ AES ≈ ECC.

2-jadval

Xotira talablari (RAM va FLASH)

Algoritm	RAM (KB)	FLASH (KB)
AES-128	20	5
PRESENT	1.5	0.5
ASCON	2	0.5
SIMON	1.8	0.4
SPECK	1.7	0.4
ECC	25	5

ECC va AES algoritmlari xotira jihatidan resurs talabi eng yuqori (RAM: 25 KB va 20 KB). IoT qurilmalari uchun bunday hajmlar haddan tashqari ortiqcha. **PRESENT** algoritmi RAM (1.5 KB) va FLASH (0.5 KB) talablari bo‘yicha eng tejamkor bo‘lsa-da, **ASCON** ham juda yaqin ko‘rsatkichga ega (RAM: 2 KB). ASCON yuqori xavfsizlik bilan bu darajadagi past xotira iste’molini birlashtira olgan.

3-jadval

Xavfsizlik indikatorlari

Algoritm	Xavfsizlik darajasi	MITM himoyasi	Replay hujumiga chidamlilik
AES-128	Yuqori	Bor	Bor

ISSN 2181-3187

PRESENT	O‘rta	Yo‘q	Yo‘q
ASCON	Yuqori	Bor	Bor
SIMON	O‘rta	Qisman	Yo‘q
SPECK	O‘rta	Qisman	Yo‘q
ECC	Yuqori	Bor	Bor

ASCON, AES-128 va ECC algoritmlari MITM va Replay hujumlariga to‘liq himoya ko‘rsatadi. PRESENT, SIMON, va SPECK algoritmlarida esa bu himoya yo‘q yoki cheklangan. Shu bilan, xavfsizlik indikatorlari bo‘yicha ASCON ECC bilan teng darajada, lekin u ECCga nisbatan sezilarli darajada tejamkor.

4-jadval

AEAD funksiyasi va kalit uzunligi

Algoritm	AEAD funksiyasi	Kalit uzunligi (bit)
AES-128	Yo‘q	128
PRESENT	Yo‘q	80
ASCON	Bor	128
SIMON	Yo‘q	128
SPECK	Yo‘q	128
ECC	Yo‘q	160

Faqatgina **ASCON** algoritmi AEAD funksiyasini (ya’ni, autentifikatsiyalangan shifrlash) to‘liq qo‘llab-quvvatlaydi. Bu esa uni IoT uchun xavfsiz va ishonchli aloqa vositasi sifatida ustun qiladi. PRESENT esa faqat 80-bitli kalitdan foydalanadi, bu esa hozirgi zamonaviy xavfsizlik standartlariga javob bermaydi.

IoT (Internet of Things) muhitining arxitekturasida axborot xavfsizligini ta’minlash bugungi kunda global axborot texnologiyalari sohasidagi eng dolzarb muammolardan biri hisoblanadi. Ushbu tizimlar ko‘pincha kichik o‘lchamli, kam quvvatli, past narxli qurilmalarga asoslangan bo‘lib, ularning xotira, hisoblash quvvati va energiya iste’moli kabi resurslari keskin cheklangan. Shu sababli, an’anaviy kriptografik algoritmlar (masalan, RSA, AES-256, SHA-512) IoT qurilmalarida

ISSN 2181-3187

bevosita va samarali tarzda ishlay olmaydi, chunki ular yuqori hisoblash murakkabligi va katta resurs talablariga ega.

IoT muhitining yana bir o‘ziga xos jihati bu — tarmoq infratuzilmasining kengligi va har xil qurilmalar o‘rtasidagi doimiy, real vaqtli ma’lumot uzatish talabidir. Bu esa, o‘z navbatida, nafaqat ma’lumotlarning konfidensialligini, balki ularning yaxlitligi va autentifikatsiyasini ham ta’minlashni talab qiladi. Bunday murakkab va dinamik muhitda yengil (lightweight) kriptografiya algoritmlarining qo‘llanilishi eng maqbul yondashuv hisoblanadi.

Ushbu tadqiqot natijalari shuni ko‘rsatadiki, ASCON algoritmi o‘zining energiyaga tejamkorligi, kichik xotira iziga ega bo‘lishi, yuqori xavfsizlik darajasi (AEAD funksiyasi orqali) va MITM/Replay hujumlariga chidamliligi bilan IoT uchun optimal tanlovdir. ASCONning 2023-yilda NIST tomonidan yengil kriptografiya standarti sifatida e’tirof etilishi ham uning ilmiy va amaliy qiymatini oshiradi. Shuningdek, ECC (Elliptic Curve Cryptography) algoritmlari autentifikatsiya jarayonlarida yuqori darajadagi xavfsizlikni ta’minlay olishi bilan muhim ahamiyatga ega, lekin ularning resurs sarfi yuqoriligi sababli faqat markaziy tugunlar yoki shlyuz qurilmalarda samarali ishlatiladi.

Biroq, yengil kriptografik algoritmlarni tanlash jarayonida bir necha omillar chuqur tahlil qilinishi lozim. Birinchi navbatda, qurilmaning funksional sohasiga (sanoat, tibbiyot, transport, aqlli uy, qishloq xo‘jaligi) qarab xavfsizlik talab darajalari aniqlanadi. Masalan, tibbiy qurilmalarda axborotning konfidensialligi birlamchi bo‘lsa, sanoat muhitida ma’lumotlar yaxlitligi va tizimga hujumlarning oldini olish ustuvor ahamiyat kasb etadi. Ikkinchidan, real vaqt rejimida ishlovchi IoT tizimlarida kriptografik algoritmning kechikish muddati (latency) ham juda muhim mezondir. Uchinchi jihat, tanlangan algoritmning turli hujum turlariga — masalan, differential, linear, side-channel, brute-force, va fault injection hujumlariga nisbatan qanday himoya mexanizmlariga ega ekanligidir.

Muhokamadan kelib chiqib, IoT tizimlarida axborotni himoyalashga qaratilgan yondashuvlar bir xillik emas, balki moslashuvchanlik prinsipiga asoslangan bo‘lishi

ISSN 2181-3187

zarur. Har bir qurilma yoki tarmoq segmenti uchun uning o‘ziga xos texnik imkoniyatlari va xavfsizlik ehtiyojlari asosida modulyar va optimallashtirilgan kriptografik protokollarni joriy qilish talab etiladi. Ayniqsa, mikroprotsessorlarga asoslangan platformalar (masalan, ARM Cortex-M, AVR, RISC-V) uchun apparat darajasida ishlovchi yengil shifrlash bloklari (crypto co-processors) ishlab chiqilishi zarur.

Shuningdek, IoT tizimlarida yangilanish (update) va kalit boshqaruvi (key management) muammosi ham dolzarb hisoblanadi. Yengil kriptografiya algoritmlari bu borada ham o‘zini oqlashi uchun, ularni dinamik kalit almashinuvi protokollari bilan integratsiyalash bo‘yicha qo‘shimcha tadqiqotlar talab etiladi. Hozirgi paytda mavjud bo‘lgan yondashuvlar (masalan, TLS-Light, DTLS, LoRaWAN Security Layer)ni optimallashtirish yoki yangilarini yaratish — bu sohadagi kelajak istiqbolini belgilaydi.

Xulosa sifatida aytish mumkinki, IoT tizimlarida axborotni samarali va ishonchli tarzda himoyalash uchun yengil kriptografik algoritmlarga asoslangan xavfsizlik yondashuvlarini ishlab chiqish nafaqat texnik zarurat, balki strategik muhim yo‘nalishdir. ASCON kabi ilg‘or algoritmlar bu borada asosiy tayanch bo‘la oladi. Biroq, ularni to‘liq joriy qilish uchun ilmiy-texnik tadqiqotlarni chuqurlashtirish, maxsus apparat platformalar uchun moslashtirish, hamda soha bo‘yicha xalqaro standartlarni izchil qo‘llash talab etiladi.

Xulosa

IoT (Internet of Things) texnologiyalari bugungi kunda sanoat avtomatlashtirishidan tortib, tibbiyot, transport, aqlli shahar va aqlli uy tizimlarigacha bo‘lgan turli sohalarda keng qo‘llanilmoqda. Biroq IoT tizimlarining xususiyatlari — past energiya sarfi, cheklangan hisoblash resurslari va uzluksiz ma’lumot almashuvi — ularni kiberxavflarga nisbatan sezuvchan holatga keltirib qo‘ymoqda. Shunday sharoitda, ularning axborot xavfsizligini ta’minlash masalasi alohida ilmiy-texnik e’tiborni talab etadi. Mazkur tadqiqot doirasida IoT qurilmalarida axborotni

ISSN 2181-3187

kriptografik himoyalashning samarador usullari chuqur tahlil qilindi va mavjud algoritmlar mezonlar asosida qiyosiy baholandi.

Tadqiqot natijalari shuni ko‘rsatadiki, **AES-128** kabi an’anaviy kuchli kriptografik algoritmlar yuqori xavfsizlik darajasini ta’minlay olgan bo‘lsa-da, ularning hisoblash murakkabligi va katta resurs talabiga ega bo‘lishi ularni resurs cheklangan IoT qurilmalari uchun samarali qilish imkonini bermaydi. **ECC (Elliptic Curve Cryptography)** algoritmi esa autentifikatsiya va kalit boshqaruvi uchun kuchli yechim bo‘lsa-da, u ham energiya sarfi va apparat murakkabligi sababli faqat markaziy tugunlarda yoki gateway qurilmalarda samarali ishlatilishi mumkin.

Tahlil qilingan yengil kriptografik algoritmlar orasida **ASCON** algoritmi eng muvozanatli va zamonaviy talablarga javob beruvchi yechim sifatida ajralib turdi. ASCON o‘zining past energiya sarfi (85 µJ/op), kichik xotira talabi (2 KB RAM), AEAD funksiyasiga ega bo‘lishi, MITM va Replay hujumlariga qarshi barqarorligi bilan IoT muhitida foydalanish uchun optimal tanlov ekanini isbotladi. ASCON 2023 yilda NIST tomonidan rasmiy ravishda yengil kriptografiya standarti sifatida tan olinib, uning amaliy qiymatini yanada oshirdi. Shuningdek, **PRESENT** algoritmi resurs jihatidan nihoyatda tejamkor bo‘lsa-da, xavfsizlik darajasining pastligi sababli u faqat xavfsizlik talab darajasi nisbatan kam bo‘lgan sohalarda tavsiya etiladi.

Tadqiqotdan kelib chiqib, quyidagi tavsiyalarni ilgari surish mumkin:

1. **IoT ishlab chiqaruvchilari** qurilma darajasida kriptografik yondashuvlarni tanlashda qurilmaning xususiyatlari (CPU arxitekturasi, energiya manbai, xotira hajmi) va qo‘llanish sohasi (tibbiyot, transport, sanoat va h.k.)ni chuqur tahlil qilishlari zarur.
2. **ASCON algoritmi** — xavfsizlik va samaradorlik o‘rtasida optimal muvozanatga ega bo‘lgan algoritm sifatida IoT qurilmalari uchun asosiy standarti sifatida keng joriy etilishi kerak.
3. **Yengil kriptografiya tadqiqotlarini** davom ettirish orqali apparatga mo‘ljallangan, resursga tejamkor va yanada bardavom himoya tizimlarini ishlab chiqish lozim.

ISSN 2181-3187

4. IoT tizimlarida xavfsizlik faqat shifrlash bilan cheklanmasligi, balki u **kalit boshqaruvi, autentifikatsiya, yangilanish mexanizmlari va xavfsiz aloqa protokollari** bilan kompleks tarzda integratsiya qilinishi zarur.

Shu bois, IoT ekotizimining xavfsizligini ta’minlashda zamonaviy yengil kriptografik algoritmlar — ayniqsa, ASCON — asosiy komponent sifatida e’tiborga olinishi, ularni amaliyotda tatbiq etish esa global raqamli xavfsizlik strategiyasining ajralmas qismi sifatida qaralishi zarur. Bu nafaqat texnik darajadagi barqarorlikni, balki foydalanuvchilarning ishonchini ham ta’minlashga xizmat qiladi.

Adabiyotlar ro‘yxati

1. National Institute of Standards and Technology (NIST). (2023). *Submission requirements and evaluation criteria for the lightweight cryptography standardization process*. U.S. Department of Commerce. https://csrc.nist.gov

2. Biryukov, A., Dobraunig, C., Kales, D., & Perrin, L. (2023). *The Design of ASCON – Lightweight Authenticated Encryption and Hashing*. In: Journal of Cryptographic Engineering, 13(2), pp. 145–160.

3. Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J., ... & Yalcin, T. (2007). *PRESENT: An Ultra-Lightweight Block Cipher*. In: Cryptographic Hardware and Embedded Systems (CHES), Springer, pp. 450–466.

4. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2015). *The SIMON and SPECK Families of Lightweight Block Ciphers*. In: IACR Cryptology ePrint Archive.

5. International Organization for Standardization (ISO/IEC). (2019). *ISO/IEC 29192: Lightweight Cryptography – Part 1-5*. Geneva: ISO.

6. Koblitz, N., & Menezes, A. (2009). *A Survey of Public-Key Cryptosystems*. In: SIAM Review, 51(3), pp. 483–502.

7. Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015). *Security and Privacy Challenges in Industrial Internet of Things*. In: Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), pp. 1–6.

ISSN 2181-3187

8. Al-Janabi, S., & Saeed, F. (2019). *Survey of Encryption Algorithms for IoT Networks*. In: Proceedings of the International Conference on Internet of Things, Big Data and Security (IoTBDS), pp. 86–93.

9. Abomhara, M., & Køien, G. M. (2015). *Security and Privacy in the Internet of Things: Current Status and Open Issues*. In: International Journal of Distributed Sensor Networks, Vol. 2015, Article ID 932168.

10. Liu, Y., Ning, P., & Reiter, M. K. (2005). *False Data Injection Attacks against State Estimation in Electric Power Grids*. In: ACM Transactions on Information and System Security (TISSEC), 14(1), pp. 13–24.

11. Ali, T., & Qadir, J. (2021). *Lightweight Cryptographic Algorithms for Securing IoT Devices: A Survey*. In: ACM Computing Surveys, 54(6), Article 127.

12. Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). *Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures*. In: 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 336–341.