

INNOVATION SCIENCE AND TECHNOLOGY



Scopus || Electronic journal specializing in Scopus

ISSUE 12



Acceptance of papers **December, 2025**



**Acceptance of
papers**

Published monthly



Topics

economics,
technology, social
sciences



ISSN 3060-5229

**EDITOR-IN-CHIEF:**

Mirzaliyev Sanjar Makhamatjon ugli

DEPUTY EDITOR-IN-CHIEF:

Makhmudov Nosir Makhmudovich
DSc., Prof., Academician

DEPUTY EDITOR-IN-CHIEF:

Ochilov Bobur Bakhtiyor ugli – Senior
lecturer at TSUI

THE SCIENTIFIC-POPULAR ELECTRONIC
JOURNAL **"INNOVATION SCIENCE AND
TECHNOLOGY"** HAS BEEN REGISTERED
UNDER THE NUMBER **C-5669633** BY THE
AGENCY FOR INFORMATION AND MASS
COMMUNICATIONS (AOKA) OF THE
REPUBLIC OF UZBEKISTAN, EFFECTIVE
FROM OCTOBER 9, 2024.

CONTACTS

Phone: **+998 50 737 87 88**

Website: <https://ist-journal.uz>

Email: innovationist2025@gmail.com

The scientific electronic journal "Innovation Science and Technology" has been included in the list of scientific publications recommended for the publication of main scientific results of dissertations for the award of PhD and DSc degrees in economics and technical sciences, in accordance with the Resolution No. 370 of the Presidium of the Higher Attestation Commission of the Republic of Uzbekistan, dated May 8, 2025.

Electronic publication, Issue 12. 613 pages.
Approved for publication on December, 2025.

Editorial board:

Sharipov Kongiratbay Avezimbetovich,
Doctor of Technical Sciences (DSc), Professor



Abdurakhmanova Gulnora Kalandarovna, Doctor of
Economic Sciences (DSc), Professor



Cham Tat Huei,
Doctor of Philosophy (PhD), Professor (Malaysia)



Muhammad Imran Sadiq
Doctor of Philosophy in Economics (PhD), Professor,
Malaysia



Ahmed Aziz Ismail
Doctor of Technical Sciences (DSc),
Professor (Egypt)



Lee Chin
Doctor of Philosophy in Economics (PhD), (Malaysia)



Asongu Simplicé
Doctor of Philosophy in Economics (PhD), Cameroon



Rui Dang
Doctor of Chemistry (DSc), Professor, China



Zahoor Ahmed
Doctor of Philosophy in Economics (PhD), Turkey



Shujaat Abbas
Doctor of Philosophy in Economics (PhD), Russia



Tina A Coffelt
Doctor of Philosophy in Educational Sciences (PhD),
USA



Abdikarimova Dinara Rustamxanovna
Doctor of Economic Sciences (DSc), Professor

Kurbonbekova Mohichehra Turobjonovna
Doctor of Economic Sciences (DSc), Professor

Alimardonov Ilkhom Muzrabshokovich
Doctor of Economic Sciences (DSc), Professor



Razakova Barno Sayfiyevna
Doctor of Philosophy in Economics (PhD)



Khasanov Sarvar Ulugbek ugli
Doctor of Philosophy in Economics (PhD)

CONTENTS

THE THEORETICAL FOUNDATIONS OF APPLYING TAX INCENTIVES FOR INVESTMENTS DIRECTED TOWARD HUMAN CAPITAL	14
Quliyev Begimqul Melikovich	
ECONOMETRIC MODELS OF CASHLESS SETTLEMENTS AMONG ECONOMIC ENTITIES.....	21
Ruzimuradov Shukhrat Khusanovich	
PROSPECTS FOR THE DEVELOPMENT OF TOURISM BRAND MARKETING IN MODERN CONDITIONS (UAE: DUBAI ON THE EXAMPLE OF A CITY).....	26
Ibodova Dilsora Ibodovna	
CREDIT DEFAULT SWAPS AS A WAY TO HEDGE AGAINST FORTHCOMING FUTURE UNCERTAINTIES IN THE DEBT MARKET OF UZBEKISTAN	31
Abduganiev Abdulaziz Alisher o'g'li	
SHOULD THE REGULATION OF THE E-COMMERCE MARKET IN THE REPUBLIC OF UZBEKISTAN BE CARRIED OUT BY THE NATIONAL AGENCY FOR PERSPECTIVE PROJECTS OR THE CENTRAL BANK?	39
Sadikov Aziz Mirsharapovich	
MECHANISM FOR IMPLEMENTING ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN THE OPERATIONS OF COMMERCIAL BANKS IN UZBEKISTAN.....	46
Bakhriddin Berdiyarov	
INNOVATIVE APPROACHES OF SMALL BUSINESSES IN THE INDUSTRY AND CONSTRUCTION SECTORS AND THEIR IMPACT ON EMPLOYMENT.....	53
Ergasheva Nigora Abdigapparovna	
AI-BASED NORMALIZATION METHODOLOGY FOR COLLECTING AND PROCESSING KPI INDICATORS.....	56
Shuhratov Mamurjon Shuhrat o'g'li	
REFORMS AND PROSPECTS FOR THE DEVELOPMENT OF THE PARTICIPATORY BUDGETING INITIATIVE IN UZBEKISTAN	63
Khamidov Khabibullo Hikmatulla ugli	
PROBLEMS OF THE INWARD PROCESSING CUSTOMS REGIME AND WAYS TO ELIMINATE THEM.....	70
Abdullaev Shakhzodbek	
FINANCIAL ANALYSIS OF SMALL BUSINESS AND PRIVATE ENTREPRENEURSHIP IN CONSTRUCTION	74
Musayeva Shoirazimovna	
MEASURES TO ENHANCE THE ROLE AND EFFECTIVENESS OF SMALL BUSINESS IN REGIONAL ECONOMIC DEVELOPMENT.....	80
Ergashev Jamshid Jamoliddinovich	
THEORETICAL AND METHODOLOGICAL FOUNDATIONS FOR IMPLEMENTING INNOVATIVE TECHNOLOGIES IN EDUCATION	84
Alijonova Marjonabonu Jaxongir qizi	
INDIA'S EXPERIENCE IN ENHANCING PUBLIC WELFARE THROUGH THE DEVELOPMENT OF ENTREPRENEURIAL ACTIVITY	88
Aripov Oybek Abdullayevich	
GREEN STRUCTURAL TRANSFORMATION IN UZBEKISTAN: GREEN FINANCE AND ECO-INNOVATION FOR SUSTAINABLE INDUSTRIAL AND AGRICULTURAL DEVELOPMENT.....	93
Egamberdiev Khumoyun	
AGRICULTURAL MANAGEMENT BASED ON INNOVATIVE TECHNOLOGIES AT THE INTERNATIONAL LEVEL: THE EXAMPLE OF UZBEKISTAN.....	101
Bustonov Komiljon Kumakovich	
ANALYSIS OF THE FINANCIAL CONDITION OF ENTERPRISES: ASSESSMENT OF EQUITY EFFICIENCY	110
Umurkul Shukhratovich Fayziev	

IMPROVING THE QUALITY OF ECONOMIC GROWTH THROUGH THE TRANSITION TO THE DIGITAL ECONOMY.....	118
Mamadaliyev Akmaljon	
МЕТОДЫ И МЕХАНИЗМЫ ИССЛЕДОВАНИЯ ПОТРЕБИТЕЛЬСКОГО ПОВЕДЕНИЯ НА ТУРИСТСКОМ РЫНКЕ.....	124
Нурматова Ситора Шавкатовна	
ANALYSIS OF INNOVATION ACTIVITIES.....	133
Alieva Elnara Ametovna	
METHODS AND MECHANISMS FOR STUDYING CONSUMER BEHAVIOR IN THE TOURISM MARKET.....	139
Nurmatova Sitora Shavkatovna	
ALGORITHMS AND METHODS FOR CALCULATING THE AREA OF A GASTRIC ULCER DEFECT USING MODERN MATHEMATICAL TECHNIQUES.....	145
Yusupov Ibrohimbek XXX, Abdusamatova Munira Sultonbek qizi	
UTILIZATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN ENTERPRISE MARKETING ACTIVITIES.....	151
Sadikov Shohrux Shukhratovich	
ENSURING THE FINANCIAL SUSTAINABILITY OF HIGHER EDUCATION INSTITUTIONS: STRATEGIC DIRECTIONS, GLOBAL TRENDS, AND POLICY IMPLICATIONS.....	156
Inomiddin Imomov	
THEORETICAL FOUNDATIONS OF THE STRUCTURE OF THE NATIONAL ECONOMY.....	161
Bustonov Mansurjon Mardonakulovich	
IMPORTANT CHARACTERISTICS OF THE DEVELOPMENT OF E-COMMERCE SERVICES.....	169
Jurakulov Shohruh Bahtiyorovich	
AGRICULTURE PROMOTION AND DEVELOPMENT IN MOUNTAIN AND MOUNTAIN REGIONS.....	173
Abdulxayeva Gulshan Maxmudovna	
IMPROVING MECHANISMS FOR ENHANCING ECONOMIC EFFICIENCY IN SERVICE ENTERPRISES.....	178
Seytimbetov Kabul Serimbetovich	
INTEGRATION OF INTELLIGENT CONTROL IN DRYING SYSTEMS: PROCESS OPTIMIZATION THROUGH SENSORS, ARTIFICIAL INTELLIGENCE, AND MODULAR DRYING.....	184
Yangiboyeva Raxbaroy Mashrabboy qizi	
THEORETICAL MODELS AND CONCEPTS OF ECONOMIC DEVELOPMENT IN THE ENERGY SECTOR.....	190
Nigmatullaeva Gulchekhra Nurullaevna	
STATISTICAL ANALYSIS OF REGIONAL ECONOMIC POTENTIAL (A CASE STUDY OF NAMANGAN REGION).....	196
Tursinbayev Azizbek Nabijon o'g'li, Sirojiddinov Kamoliddin Ikromiddinovich	
DIRECTIONS FOR DEVELOPING INVESTMENT AND EXPORT IN REMOTE SERVICE ENTERPRISES.....	203
Uzakov Ortik Shaymardanovich	
SPECIFIC FEATURES OF ENTREPRENEURSHIP IN INCREASING THE INCOME OF THE POPULATION IN THE REGION.....	207
Kuldasheva Maftuna Musurmon kizi	
KEY FACTORS OF ATTRACTING INVESTMENT THROUGH SUBSIDIES AND INVESTMENTS TO INCREASE AGRICULTURAL CROP PRODUCTION IN UZBEKISTAN.....	211
Mamatkulova Nadira Makkamovna	
RAQAMLI MARKETING VA INNOVATSION TEXNOLOGIYALAR ASOSIDA EKOTIZIM SAMARADORLIGINI OSHIRISH USULLARI.....	216
Sobirov Azizbek Avazbekovich	
WAYS TO IMPROVE THE STATISTICAL ASSESSMENT OF FRUIT AND VEGETABLE PRODUCTION PROCESSES AND EXPORT POTENTIAL IN THE REPUBLIC OF UZBEKISTAN.....	223
Anorboeva Bakhtijamol Daniyar kizi	

THE IMPACT OF DEGRADATION ON THE OPERATIONAL CHARACTERISTICS OF PHOTOVOLTAIC MODULES UNDER SHARPLY CONTINENTAL CLIMATIC CONDITIONS	229
Qurbanov Yunus Murtaza o'g'li	
INTEGRATED NEW MEDIA OPERATION MODEL FOR INTELLIGENT TALENT ASSESSMENT PLATFORMS: THE PATH OF QR CODE ACTIVATION AND CONTENT-DRIVEN ENGAGEMENT.....	235
Wang Biao	
METHODOLOGICAL FOUNDATIONS FOR SHAPING THE CREATIVE ACTIVITY OF YOUNGER PUPILS IN SOLVING MATHEMATICAL PROBLEMS	239
Dzhurakulova Adolat Khalmuratovna	
SOLIDWORKS-BASED MODELING OF AN AIR-BLOWING SYSTEM TO ENSURE HIGH-QUALITY FIBER REMOVAL FROM SAW TEETH	247
Mirzakarimov Mirsharoffiddin Mirzaabdurahimovich	
THEORETICAL STUDY OF TEMPERATURE AND THERMAL PHENOMENA IN MECHANICAL CUTTING OF WHITE CAST IRON.....	256
Allanazarov Akmal Abdulxaqovich	
THEORETICAL AND METHODOLOGICAL FOUNDATIONS OF SUSTAINABLE DEVELOPMENT OF THE REGIONAL ECONOMY	262
Turdiyev Ulug'bek Qayumovich	
THE INTERRELATIONSHIP BETWEEN MIGRATION AND THE INDUSTRIAL ECONOMY	266
Khusanbek Begmatov	
THE IMPACT OF ESG PRINCIPLES ON THE HOTEL INDUSTRY	271
Khusenova Mekhrangiz	
CURRENT STATUS OF INDUSTRIAL PRODUCTION AND SERVICES MARKET IN KASHKADARYA REGION.....	276
Norov Murodjon Makhmudovich	
DEVELOPMENT OF AN ARTIFICIAL INTELLIGENCE-BASED CYBERSECURITY SYSTEM FOR THE AUTOMATIC DETECTION OF FAKE FINANCIAL RECEIPTS, PHISHING URLS, AND MALICIOUS APK FILES.....	284
Shermatov Axlidin Sharobiddin o'g'li	
WAYS TO INCREASE REVENUES IN COMMERCIAL BANK OPERATIONS	287
Ostonaqulova Gulchehraxon Muhammadyoqub qizi	
РОЛЬ СВОБОДНЫХ ЭКОНОМИЧЕСКИХ ЗОН В РЕГИОНАЛЬНОМ РАЗВИТИИ И ЗАРУБЕЖНЫЙ ОПЫТ	301
Файзиева Ширин Шодмоновна	
RAQAMLI IQTISODIYOTGA O'TISH SHAROITIDA IQTISODIY O'SISH OMILLARINING TA'SIRINI BAHOLASH METODOLOGIYASI.....	307
Bustonov Mansurjon Mardonakulovich	
FINTECH TRENDS: NEW TOOLS FOR ATTRACTING FINANCING IN THE CONTEXT OF DIGITAL TRANSFORMATION	313
Madjitova Lolakhon Lazizovna	
CHALLENGES AND PROSPECTS FOR THE DEVELOPMENT OF E-COMMERCE IN UZBEKISTAN.....	317
Toshpulatov Akhror Tukhtamurod ugli	
STRATEGIC DETERMINANTS OF FOREIGN DIRECT INVESTMENT IN UZBEKISTAN	326
Rustamov Foziljon	
TYPES AND MEANS OF ADVERTISING IN THE FIELD OF TOURISM	335
Bahriyeva Zarina Nasimovna	
INTELLECTUALIZATION OF TECHNICAL MEANS FOR CONTROLLING TECHNOLOGICAL REFINING PROCESSES.....	340
Ruziyev Umidjon Abdimajitovich	
NECESSITY OF ENSURING AND INCREASING THE COMPETITIVENESS OF PLACEMENT MEANS	349
Sherkulov Dilshod Jurakulovich	
YASHIL IQTISODIYOT VA MOLIYAVIY INKLYUZIYANING O'ZARO BOG'LIQLIK NAZARIYALARI.....	354
Adashaliyev Baxtiyorjon Valisher o'g'li	

THE IMPORTANCE OF THE AUDIT OF LEASING OPERATIONS ON FARMS OF THE REPUBLIC OF UZBEKISTAN	359
Tursunov Ulugbek Sativoldievich	
METHODOLOGY DEVELOPMENT RETAIL MARKETING AND TRADING SYSTEM.....	365
Makhmatkulov Golibjon Kholmuminovich	
NECESSITY OF ENSURING AND INCREASING THE COMPETITIVENESS OF PLACEMENT MEANS	369
Sherkulov Dilshod Jurakulovich	
ENVIRONMENTAL FISCAL POLICY AS A DRIVER OF GREEN GROWTH AND EMPLOYMENT IN CENTRAL ASIA: EMPIRICAL EVIDENCE	374
Rakhmatova Zilola Yurevna	
ON THE ISSUE OF CALCULATING THE POWER REQUIRED TO HEAT THE EDGES OF THE PIPE BILLET TO THE WELDING TEMPERATURE.....	379
Zairkulov Elyor Yoqubjon o'g'li	
STATISTICAL ASSESSMENT OF REGIONAL ELECTRICITY GENERATION VOLUMES	385
Doliev Shokhabbos Kulmurat ugli	
ANALYSIS OF ICT APPLICATION IN UZBEKISTAN'S TOURISM BASED ON EMPIRICAL RESEARCH	389
Nazarov Khusanbek Avazbek ogli	
METHODOLOGY FOR FORECASTING AND ANALYZING MANAGEMENT ACCOUNTING INDICATORS AT AN ENTERPRISE	395
Minutdinova Liliya Tagirovna	
WELLNESS TOURISM AS AN ESSENTIAL COMPONENT OF HEALTH TOURISM	402
Tashtayeva Saida Kahharovna	
THE EXPERIENCE OF GERMANY IN DEVELOPING SMALL AND MEDIUM ENTERPRISES.....	409
Annaklichev Saxi Saparmuxamedovich	
ANALYSIS OF THE APPLICATION OF THE INTERNATIONAL STANDARD ON AUDITING "ANALYTICAL PROCEDURES" IN NATIONAL AUDIT ACTIVITIES	416
Tajekeev Ziyatdin Kobeyzinovich	
ORGANIZATIONAL AND ECONOMIC FOUNDATIONS OF GREEN ENTERPRISE DEVELOPMENT IN ENSURING REGIONAL ENVIRONMENTAL SAFETY	421
Khamidillo Odilov	
A REALIST-POSITIVIST FRAMEWORK FOR ANALYSING MERGERS AND ACQUISITIONS UNDER ECONOMIC POLICY UNCERTAINTY	429
Zakhidov Azizbek Rustamovich	
DEVELOPING MATHEMATICAL MODELS TO SIMULATE THE DYNAMIC BEHAVIOR OF SEPARATION PROCESSES, CONSIDERING THE IMPACT OF EXTERNAL FACTORS	436
Abdulleva Kamola Rustamovna	
THEORETICAL FOUNDATIONS OF IMPLEMENTING DIGITAL TECHNOLOGIES IN THE TRANSFORMATION OF BANKS.....	445
Umarova Malika Baxtiyarovna	
ON THE ISSUE OF RESEARCH AND DEVELOPMENT OF A SLAG-FORMING BASE FOR ELECTRODE COATINGS FOR WEAR-RESISTANT SURFACING.....	451
Sadikov Jaxongir Nasidjanovich	
MODELING OF HEAT FLOWS IN GAS-FIRED CHAMBER FURNACES.....	456
Rajabov Azamat Toirovich	
DEVELOPMENT OF A MIMO MODEL OF AZEOTROPIC DISTILLATION	462
Shamsutdinova Vinera Khafizovna	
THEORETICAL FOUNDATIONS OF THE INTERACTION OF A COTTON TUFT WITH A SCREW CONVEYOR AND A MESH SURFACE.....	468
Matyaqubova Jumagul Bakhtiyarovna	
FORECASTING LIQUIDITY AND SOLVENCY INDICATORS BASED ON ARTIFICIAL INTELLIGENCE	473
Zaynutdinov Ismoil Samariddin o'g'li	
MODELS FOR PREDICTING THE MANAGEMENT OF COMPLEX TECHNOLOGICAL PROCESSES AND PRODUCTIONS	477
Gulyamov Shukhrat Mannapovich	

WAYS TO ADJUST LAND RESOURCE USE MECHANISMS FOR FARMERS BASED ON THE EXPERIENCE OF FOREIGN COUNTRIES.....	482
Akhmatov Abutolibkhon Ochilkhon oglu	
STATE SUPPORT MECHANISMS FOR THE DEVELOPMENT OF THE MACHINE-BUILDING INDUSTRY	487
Xursandov Komiljon Makhmatkulovich	
EMPIRICAL ANALYSIS OF TOURISM FLOW FORECASTING IN CENTRAL ASIA BASED REGRESSION MODELS	491
Suratova Mokhirakhon Shavkat Kizi	
THE ROLE OF LOANS IN THE DEVELOPMENT OF THE REGIONAL ECONOMY.....	498
Meylikov Fazliddin Abduhalim o'g'li, Valiev Oybek Shukhrat ugli	
PROPAGATION OF SMALL MOTIONS IN A TWO-LAYER DISPERSE MEDIA FLOW.....	503
D. S. Yakhshibaev	
FURTHER IMPROVEMENT OF THE AUTOMATION SYSTEM OF ELECTRONIC SERVICES AND TOURIST PERMITS.....	511
Najmiddinov Sultan Nurali ugli	
THE NECESSITY OF DISCLOSING INFORMATION ON SELLING EXPENSES IN ACCOUNTING REPORTS OF PHARMACEUTICAL ENTERPRISES	516
Xudaynazarova Dilnoza Gafurovna	
INVESTMENT FINANCIAL MECHANISMS AND THEIR ROLE IN THE NATIONAL ECONOMY	521
Karjavova Khurshida Abdumalikovna	
WESTERN COUNTRIES' EXPERIENCES IN ENSURING THE FINANCIAL PERFORMANCE OF BANKING ACTIVITIES.....	526
Alimjanova Dilrabo Sobirjanovna	
MAIN FEATURES OF DIVIDEND POLICY IN COMMERCIAL BANKS.....	530
Aliyev G'ulomnozir Maxamatjonovich	
OPTIMIZATION OF THE DESIGN OF AN ENERGY- AND RESOURCE-EFFICIENT PRESSING DEVICE FOR CONVERTING DRIED LEAVES, FALLEN FOLIAGE, AND PLANT RESIDUES INTO LOCALLY PRODUCED ORGANIC FERTILIZERS.....	536
Toirova Nuriya Abdiyevna, Toirov Murtoza Shavkidinovich, Urinova Xulkar Shokirovna	
FUNDAMENTALS OF FORMING ACCOUNTING POLICIES FOR LEASING COMPANIES BASED ON INTERNATIONAL FINANCIAL REPORTING STANDARDS	540
Baxadirov Alisher Komilovich	
THE USE OF DUE DILIGENCE PROCEDURES TO ENSURE TRANSPARENCY OF FINANCIAL REPORTING IN JOINT-STOCK COMPANIES	545
Prokudina Kristina Aleksandrovna	
INTERNATIONAL EXPERIENCE: EXAMPLES OF HISTORICAL CITIES (FLORENCE, LVIV, GRANADA, AND OTHERS)	550
Radjabova Mavluda Ergash qizi	
APPLYING LINEAR PROGRAMMING TO ANALYZE THE STATE OF COMMODITY AND RAW MATERIAL RESOURCES IN INDUSTRIAL ENTERPRISES	554
Beknazarov Farxod Abduvaxidovich, Usmanov Shakhzod Shokhrukhovich	
INTEGRATED EDUCATION MODEL IN TEACHING WATER-SAVING IRRIGATION TECHNOLOGIES.....	561
Shokhimardanova Niginabonu Shavkatovna	
IMPACT OF INFLATIONARY PROCESSES ON PROBLEM LOANS.....	566
Tojiyev Sardor Dilmurod ugli	
DIRECTIONS FOR ORGANIZING EFFECTIVE MANAGEMENT IN GRAIN PRODUCT ENTERPRISES.....	572
Kurbanova Dildora Abduraxmanovna	
THE OIL AND GAS INDUSTRY AS A BACKBONE SECTOR OF UZBEKISTAN'S ECONOMY	576
Salomova Sarvinoz Salimovna	
BEHIND THE BENCH: THE CURRENT SITUATION OF PURCHASING LABORATORY EQUIPMENT IN UZBEKISTAN	581
Kabashev Tairjon	

ISSUES OF IMPROVING AGRICULTURAL INSURANCE IN UZBEKISTAN	586
Shennayev Xo'jayor Musurmanovich	
THE LENDING SYSTEM IN COMMERCIAL BANKS AND THE CAUSES OF NON-PERFORMING LOANS.....	590
Shokhista K. Kholiyorova, Marjona O. Barnoqulova	
INNOVATIVE FINANCIAL INSTRUMENTS FOR FINANCING RENEWABLE ENERGY AND GREEN PROJECTS: CONCEPTUAL FOUNDATIONS	595
F. Nishonov	
DATA TRANSMISSION CONFIDENTIALITY CHALLENGES IN THE INTERNET OF THINGS.....	604
Mardiyev Ulugbek	

DATA TRANSMISSION CONFIDENTIALITY CHALLENGES IN THE INTERNET OF THINGS

Mardiyev Ulugbek

Researcher at Department of Cryptology

Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Email: ulugbekmardiyev@gmail.com

Abstract: This article examines data transmission confidentiality challenges in Internet of Things (IoT) technologies within the framework of Industry 4.0. The rapid growth of IoT devices and the increasing volume of exchanged data have significantly intensified data security risks. The study focuses on data breach threats, the role of cryptographic techniques in ensuring confidentiality and integrity, and the importance of prime-number-based keys in asymmetric cryptosystems. In addition, the paper discusses probabilistic and deterministic primality testing algorithms and their implications for cryptographic stability in IoT environments.

Key words: Internet of Things (IoT), Industry 4.0, data confidentiality, cryptography, asymmetric encryption, prime numbers, information security.

Annotatsiya: Mazkur maqolada Industry 4.0 doirasida shakllanayotgan Narsalar Interneti (IoT) texnologiyalarida ma'lumotlarni uzatish jarayonida yuzaga keladigan maxfiylik muammolari tahlil qilinadi. IoT qurilmalarining jadal ko'payishi va ular orqali uzatiladigan ma'lumotlar hajmining oshishi axborot xavfsizligini ta'minlashni muhim masalaga aylantirmoqda. Tadqiqotda ma'lumotlar buzilishi xavflari, kriptografik himoya mexanizmlarining o'rni hamda assimetrik kriptotizimlarda tub sonlarga asoslangan kalitlarning ahamiyati yoritiladi. Shuningdek, tub sonlarni aniqlashda qo'llaniladigan ehtimollik va deterministik algoritmlar nuqtayi nazaridan xavfsizlik masalalari baholanadi.

Kalit so'zlar: Internet of Things (IoT), Industry 4.0, ma'lumotlar maxfiyligi, kriptografiya, assimetrik shifrlash, tub sonlar, axborot xavfsizligi.

Аннотация: В статье рассматриваются проблемы конфиденциальности передачи данных в технологиях Интернета вещей (IoT) в контексте Industry 4.0. Стремительный рост числа IoT-устройств и объемов передаваемых данных усиливает угрозы информационной безопасности. Особое внимание уделяется рискам утечек данных, применению криптографических методов для обеспечения конфиденциальности и целостности информации, а также значению простых чисел при формировании ключей в асимметричных криптосистемах. Дополнительно анализируются вероятностные и детерминированные алгоритмы проверки простоты чисел с точки зрения их влияния на устойчивость криптографических механизмов.

Ключевые слова: Интернет вещей (IoT), Industry 4.0, конфиденциальность данных, криптография, асимметричное шифрование, простые числа, информационная безопасность.

INTRODUCTION

As several emerging technologies converge to offer digital solutions, Industry 4.0 has been referred to as a new industrial stage. They cover four basic technologies: Internet of Things (IoT), cloud services, big data, and analytics. The next phase of communication is the Internet of Things (IoT). IoT allows for the seamless creation, receipt, and exchange of data between physical items. Different IoT applications concentrate on automating various processes in an effort to give inanimate physical things the ability to behave autonomously. As the number of IoT devices increases from year to year, so does the amount of data. Consequently, there is a rise in the frequency of data breaches as a result. Consequently, guaranteeing the security of data, particularly its

confidentiality, becomes crucial. Employing cryptographic techniques stands as the most effective approach to safeguarding information confidentiality and integrity. The stability of cryptographic algorithms depends on the key used. In asymmetric cryptosystems, the key value must be prime. Currently, there are both probabilistic and deterministic algorithms for checking numbers for probability, and in practice, more probabilistic algorithms are used. This article analyzes data privacy issues in IoT technology, which is part of Industry 4.0.

REVIEW OF LITERATURE ON THE SUBJECT

The rapid expansion of the Internet of Things within the Industry 4.0 paradigm has significantly increased concerns related to data transmission confidentiality and cybersecurity. Early comprehensive studies by Ahmad et al. in 2021 emphasize that IoT-based cloud computing environments are inherently vulnerable due to resource-constrained devices, heterogeneous architectures, and large-scale data exchange. Their survey highlights confidentiality, integrity, and authentication as the most critical security dimensions, stressing that traditional security mechanisms are often inadequate for IoT ecosystems.

Privacy preservation has become a central research focus as IoT systems increasingly support smart city infrastructures. Kumar et al. in 2021 propose a blockchain-based machine learning framework aimed at protecting user privacy in IoT-driven urban environments. Their findings demonstrate that decentralized architectures can reduce single points of failure while enhancing data confidentiality and trust. Similar conclusions are drawn by Fernández-Caramés and Fraga-Lamas in 2018, who provide a detailed review of blockchain applications in IoT and underline its potential to secure data exchange through cryptographic primitives and distributed consensus mechanisms. However, Nartey et al. in 2021 caution that scalability, latency, and computational overhead remain major obstacles to large-scale deployment.

Several studies address IoT security from an architectural and communication perspective. Salama et al. in 2023 present an overview of IoT and machine-to-machine communications, identifying insecure data transmission channels and weak encryption practices as persistent challenges. In domain-specific applications, Kantipudi et al. in 2021 examine remote patient monitoring systems and demonstrate that confidentiality breaches in healthcare IoT can have direct safety implications, reinforcing the need for robust cryptographic protection. Likewise, Alaghbari et al. in 2022 analyze complex event processing in data centers and show that cyber-physical security heavily depends on secure data streams and reliable encryption mechanisms.

Cryptographic strength in IoT systems is closely tied to the reliability of key generation and primality testing algorithms. Classical foundations of primality testing are discussed by Bressoud in 1989 and Buchmann and Müller in 1992, who outline deterministic and probabilistic approaches to number theory-based cryptosystems. Rabin's probabilistic algorithms, introduced in 1976, and the Solovay–Strassen test proposed in 1977 remain cornerstones of modern cryptographic practice due to their efficiency. Subsequent studies, including Baillie and Wagstaff in 1980 and Ishmukhametov et al. in 2020, analyze the behavior of pseudoprimes and witnesses, demonstrating that probabilistic methods, while efficient, require careful parameter selection to minimize false positives.

Recent research has focused on improving the reliability of primality testing for cryptographic applications. Pulatovna and Rasulovich in 2023 propose enhancements to the Miller–Rabin algorithm aimed at reducing the number of false witnesses, which is particularly relevant for asymmetric encryption in IoT devices with limited computational capacity. Frameworks for evaluating primality testing algorithms are further discussed by Duta et al. in 2015 and Westerdijk in 2021, offering comparative insights into algorithmic performance and security trade-offs. Foundational number theory works by Nagell in 2021 and Koukoulopoulos in 2020 provide the mathematical basis for understanding prime distribution, which underpins cryptographic key generation.

Overall, the literature demonstrates that ensuring data transmission confidentiality in IoT systems requires an integrated approach combining secure architectures, advanced cryptographic techniques, and reliable primality testing algorithms. While probabilistic methods dominate practical implementations due to their efficiency, ongoing improvements are essential to maintain cryptographic stability as IoT ecosystems continue to scale.

RESEARCH METHODOLOGY

This study employs a qualitative and analytical research methodology based on a systematic review of peer-reviewed scientific articles, conference proceedings, and authoritative monographs related to IoT security and cryptographic algorithms. Collected data are analyzed using comparative and logical analysis to identify confidentiality risks and evaluate the effectiveness of probabilistic and deterministic primality testing methods in IoT-oriented cryptographic systems.

ANALYSIS AND RESULTS

One of the key problems in the new industrial stage is the extremely complicated technical architecture of the production systems in the Industry 4.0 concept [1]. Industry 4.0 has been referred to as a new industrial stage. They cover four basic technologies: Internet of Things (IoT), cloud services, big data, and analytics. The rate at which physical objects in our environment are being connected to the Internet is accelerating. In 2020, there will be over 8.4 billion linked items worldwide, according to a recent Gartner estimate. By 2022, this figure is projected to increase to 20.4 billion [2]. There are expected to be 27 billion machine-to-machine (M2M) connections in 2024, up from about 5.6 billion in 2016 [3]. M2M connections are used in a wide range of applications, including smart grids, smart retail, smart agriculture, and smart cities and ecosystems [4]. The IoT's history, present, and future architecture are depicted in Figure 1 (Figure 1) [5].

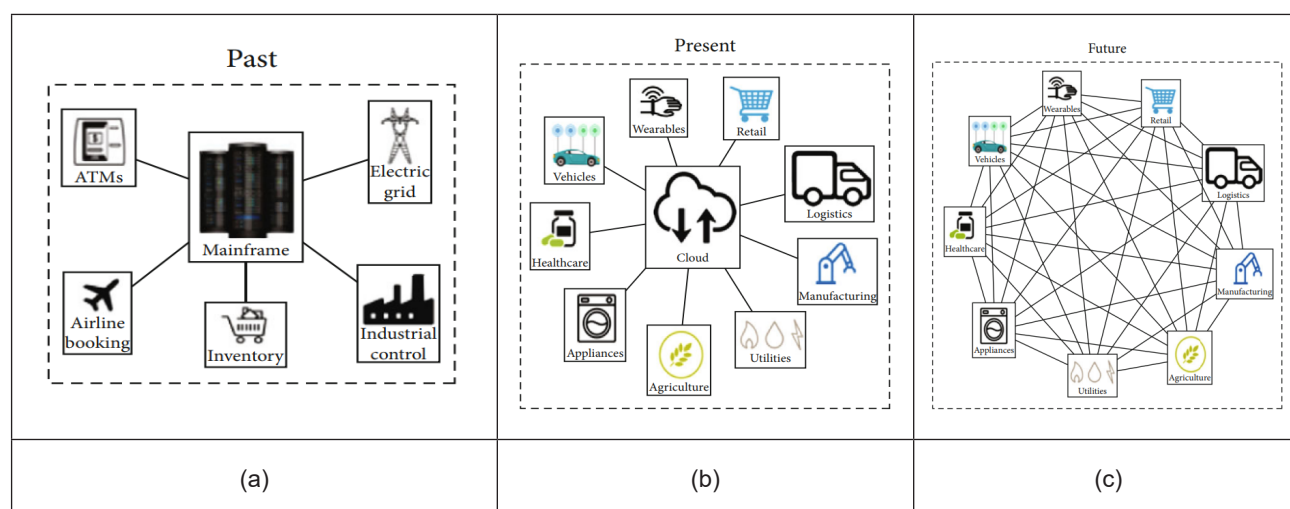


Figure 1. Past (a), present (b) and future (c) architecture of IoT

IoT devices give enemies easy access to consumer data by serving as a doorway for their entry into residential and commercial networks due to their cheap power and low security. Additionally, the IoT is becoming more than just physical items or things. There have been several instances where attempts have been made to successfully integrate IoT devices into the human body for the purpose of monitoring the health of different organs [6].

There are four key levels in every ecosystem or environment for the Internet of Things. In order to perceive the data or information needed to carry out various activities, numerous sensors and actuators are used in the first layer. Based on that, a communication network is utilized in the second layer to transfer the data acquired. The middleware layer, which is commonly utilized in the development of IoT applications, acts as a bridge connecting the network and application layers. Various IoT-based end-to-end applications, including smart grids, smart manufacturing, and smart transportation, are present on the fourth layer. Varieties of different technologies are used by each of these levels in an IoT application, which poses a number of problems and security risks. At these four strata, diverse technologies, apparatus, and applications are depicted in Figure 2 [7].

Privacy (confidentiality), trust (integrity, authentication), nonrepudiation (signature, access control), and availability are some of the most crucial security services needed in IoT. Protection from node capture, impersonation, data duplication, and forensic assaults is also necessary for specific situations. The majority of the in-demand security services may be achieved using cryptography.

A key is a replaceable component of a cipher that is used to encrypt a specific message, and this is one of the fundamental ideas in cryptography. Modern public-key cryptosystems produce keys using enormous primes, which can be several hundred or even a thousand bits and then distribute them to users. The creation of specialized software is necessary to execute mathematical operations on such numbers on regular computers and to construct quick methods for producing prime numbers. Modern security needs dictate that there be such a wide range of these numbers, therefore a deterministic approach will not be effective enough. Currently, techniques to produce numbers with a probability of at least $1 - 2^{-128}$ are employed for this purpose (Figure 2) [8].

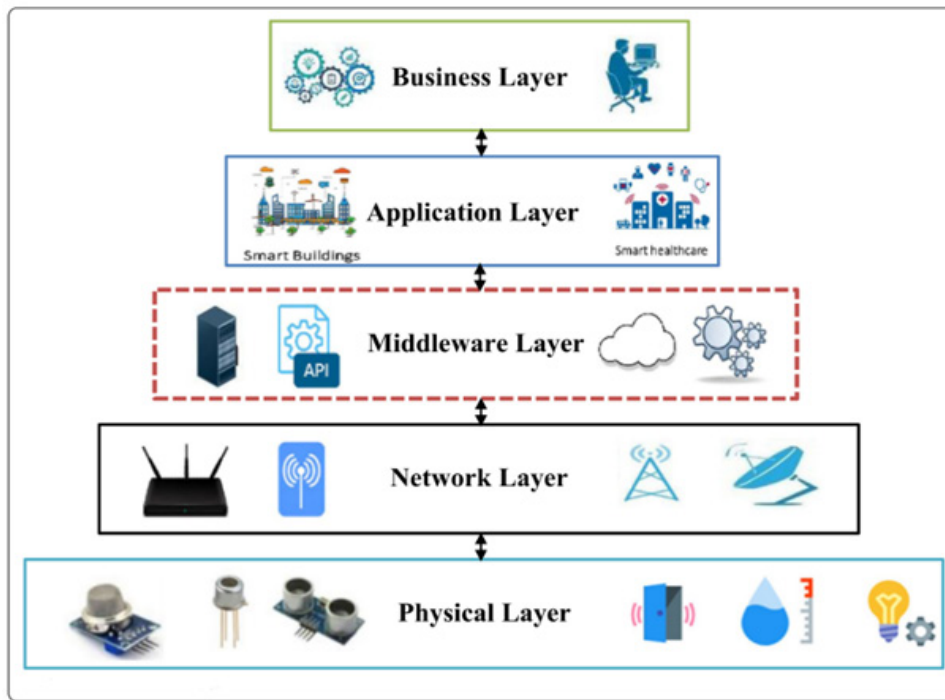


Figure 2. Layers in IoT system

Although prime numbers have long been studied, the greatest development of probabilistic testing has received in the second half of the 20^{th} century due to the need to generate large (a hundred or more decimal places) prime numbers for cryptosystems such as RSA.

In a set of natural numbers, the weight of prime numbers is considered sufficient to find them. For example, prime numbers up to 512 bits have a weight of about 10151. The probability that a randomly chosen number from a number close to n is a prime number is $1/(\ln n)$. Hence, the total number of prime numbers up to n is $n/(\ln n)$. Hence, the probability that two people choose the same large prime number is close to zero [9].

As noted above, the generation of prime numbers is one of the main stages of the design of cryptosystems with a transparent key, since they form the basis of the solver of modular arithmetic - the module. In general, the algorithms used to check numbers for primality are based on number theory concepts.

The classification of primality testing algorithms can be broadly divided into two groups: deterministic and randomized. Nevertheless, further research reveals that these algorithms can be more accurately categorized into four distinct groups [10]:

- Randomized Monte-Carlo primality tests.
- Randomized Las-Vegas primality tests.
- Deterministic primality tests.
- Heuristic primality tests.

Mathematicians have different ways to test if a number is a prime number based on its form. Basically, there are different kinds of tests to determine whether a number possesses special attributes or falls within the category of a regular number. Certain tests are specifically designed to determine the uniqueness or distinctive qualities of numbers, such as Lucas, Lucas-Lehmer, Pepin, and Proth, while others are for regular numbers like Fermat, Miller-Rabin, Solovay-Strassen, Baillie-PSW. Testing if a number is prime is easier if it can be written in a special way, rather than if it is just a regular number.

Indeed in spite of the fact that probabilistic tests are, in common, exceptionally productive, they don't guarantee 100% exactness of what comes about. At the inverse conclusion, are the deterministic tests, but their fundamental drawback is the truth that they can be in numerous circumstances illogical to execute. Their runtime is exponential (depends on the estimate of the number being tried) and the time fundamental to test the primality of a given number is greatly long.

The only deterministic primality test is minor division [11]. In this test, given an input number, N , it confirms in case any numbers m , from 2 to $(N - 1)$ isolates equitably N (there's no leftover portion). On the off

chance that N is separable by any m , the number is composite, else it is prime. The advantage of this test is the reality that it continuously returns a genuine reply. On the other hand, for expansive numbers, the calculation is unsatisfactorily moderate. Trial division takes $O(2^{n/2})$ operations to check on the off chance that an n -bit number is prime, which is exponential within the estimate of the input.

Probabilistic algorithms are more practical due to the sluggishness of deterministic tests, though they can falter in specific contexts. Balancing efficiency and result accuracy is essential. The Miller-Rabin algorithm emerges as the top-performing probabilistic primality test, while the LLR algorithm proves the most efficient among deterministic methods. Future endeavors aim to optimize these efficient tests, deploying them across parallel and distributed systems while identifying practical scenarios where they excel [12].

The AKS algorithm, although theoretically significant, is found to be inefficient in practical applications when compared to the practical superiority of the Miller-Rabin algorithm. The Miller-Rabin algorithm is recognized as one of the most extensively employed and efficient methods for testing primality in real-world scenarios. The probabilistic Solovay-Strassen and Miller-Rabin tests often require only a single test to determine compositeness. Overall, the practical performance of the Miller-Rabin algorithm stands out among the presented algorithms. The importance of large prime numbers in information security and introduces various primality testing algorithms, highlighting the efficiency of probabilistic algorithms over the AKS primality testing algorithm [13].

The smallest algorithm in this class is based on the Fermat theorem. This examination process is predicated on the theorem that prominent French mathematician Pierre Fermat put forward in the 17th century, often known as the "little Fermat theorem" [14].

Fermat's little theorem states that the equation $a^{n-1} \equiv 1 \pmod{n}$ holds if n is a prime number. Here, a is an arbitrary number and n is not divisible by a . To ascertain the primality of a given integer n , it is necessary and sufficient to satisfy the equation $a^{n-1} \equiv 1 \pmod{n}$. That is, for each a , n is a complex number if and only if $a^{n-1} \not\equiv 1 \pmod{n}$; otherwise, it is hard to say for sure, but the likelihood of the number grows. When a complex integer n is found to be a pseudo-prime based on a , the comparison $a^{n-1} \equiv 1 \pmod{n}$ is made.

When a number n is determined to be complex, however, and the comparison $a^{n-1} \equiv 1 \pmod{n}$ is not made, this is referred to as evidence of the number n 's complexity, and the preceding number a , which made the comparison, is referred to as a "false witness" of primality n .

Therefore, the number n is selected when a number is tested for primeness using the Fermat theorem. The greater the number a that fulfills the requirement, the greater the probability that n is prime. $a^{n-1} \equiv 1 \pmod{n}$. However, for any arbitrary number a , which is prime with n , the comparison holds for complex numbers n such that $a^{n-1} \equiv 1 \pmod{n}$. We refer to this as Carmichael numbers. The set of Carmichael numbers is an unbounded collection, with $n = 561 = 3 \cdot 11 \cdot 17$ being the lowest. Despite this, composite numbers can be found using the Fermat test [15]. This test's time complexity is $O(k \log n)^3$.

This class also includes the Solovay-Strassen test algorithm. The test can yield an inaccurate answer with a certain probability for complex numbers, but it always properly detects prime values. The test's primary benefit is that, in contrast to the Fermat test, it determines Carmichael's numbers as composite numbers.

The primary objective of the test is to examine a random subset of random numbers for a specified number of iterations, as opposed to evaluating every single number in the entire sequence.

The Carmichael numbers in this instance are defined by the Jacobi symbol.

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n} \quad (1)$$

The number of prime numbers is given by $\pi(n)$, where $\left(\frac{a}{n}\right)$ is a Legendre symbol.

We apply the Euler criterion in this test. It is widely recognized that if the Euler criterion's condition $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$ is satisfied for every witness of a prime number that is coprime to n (meaning they do not share a common divisor), then n is acknowledged as an odd prime number.

That is, in the $(n-1)/2$ row of the table of levels of prime numbers, the items 1 and -1 that are created in the column corresponding to the "prime witnesses" a and that are mutually simple with n are the focus of this algorithm [16].

In the algorithm, the main focus lies on the items 1 and -1 that are generated in the column corresponding to the "prime witnesses" a , which are mutually coprime with n . Specifically, these items are located in the row $(n-1)/2$ of the table that represents the levels of prime numbers.

However, according to primness, nonprime integers that meet the test's requirements are referred to as pseudoprime Euler numbers. This test has an estimated difficulty of $O(\log^3 p)$.

The Rabin-Miller test is an example of a probabilistic primality test that is constructed based on the reliable concept of pseudoprimality.

A popular test algorithm for public key cryptosystem design is presently Michael Rabin's, which was partially inspired by Jerry Miller's concepts. It is known that this approach is an effective way to test pseudo prime integers. The Miller-Rabin algorithm operates in polynomial time and has a time complexity of $O(k \log n)^3$.

It is predicated on the representation of $p-1$ in $2^s * r$, where r is an odd number and s is the number of times $p-1$ has been divided by 2 . The following definition serves as the foundation for the Rabin-Miller algorithm [17].

Definition. Assume that $p-1 = 2^s * r$, where r is an odd number, and that p is an odd composite integer. For every j , $0 \leq j \leq s-1$, $a^{2^j r} \not\equiv -1 \pmod{p}$, and $a^r \not\equiv 1 \pmod{p}$, a is referred to as a "strong witness" (composite) for p . In the absence of these conditions, p is referred to as the number of the "strong pseudo-prime" if $a^r \equiv 1 \pmod{p}$ for all $0 \leq j \leq s-1$, $a^{2^j r} \not\equiv -1 \pmod{p}$. For p , an integer a is referred to as a "strong liarwitness" number.

The Lucas test, developed by Lucas in 1891, is a technique used to ascertain the primality of numbers (not limited to just Mersenne and Fermat numbers). It employs probability-based calculations to determine the primality of these numbers.

The procedure states that an input value n is considered prime if, under certain conditions, there exists a such that, for each prime q , a divisor of $n-1$, $a^{n-1} \equiv 1 \pmod{n}$ and $a^{(n-1)/q} \not\equiv 1 \pmod{n}$. It is necessary to know the prime divisors of $n-1$ in order to use this algorithm. To date, no complex number has been found that does not pass a certain number of Rabin-Miller and Lucas tests. [18].

A probabilistic method called the Proth theorem is used to determine if a given sort of primality exists in a given integer. Typically, values in the format $k * 2^n + 1$ —where k is an odd integer such that $k < 2^n$ —are tested in this test. If for any integer a , the condition $a^{(p-1)/2} \equiv -1 \pmod{p}$ holds, then p is a prime number. Prot prime numbers are prime numbers of this kind. Prot's theorem allows one to rapidly ascertain if a given integer is prime or not. It takes a very long time, though, to determine whether a given integer is composite (every number from 2 to n must be checked). For the purpose of locating prime numbers inside a specific range, this algorithm is advised [19]. The Proth test has an $O((k \log k + \log n) \log n)$ temporal complexity.

Pocklington and Lammer created the Pocklington test, which establishes whether or not an incoming prime number may be recognized. An input number N is prime if and only if there exists an integer a such that $\gcd(a^{(N-1)/q} - 1, N) = 1$ and $a^{N-1} \equiv 1 \pmod{N}$ for every prime number q that is a divisor of number $N-1$. The prime divisors of $N-1$ must be known in order to use this technique (Table 1) [20].

Table 1. Here is a examination of probabilistic algorithms utilized for verifying the primality of numbers [21]

Tests	Benefits	Drawbacks	Complications
Fermat	- Highly straightforward to execute. - Base for many tests.	- Failure probability may reach 1. - Pseudoprime can pass the test.	$O(k \log n)^3$
Solovey Strassen	Pseudoprimes are successfully announced as composites.	- Euler pseudoprime can pass the test. - Computation of Jacobi symbol adds more computation overhead.	$O(k \log n)^3$
Miller-Rabin	- Fast & efficient. - Euler Pseudoprimes are successfully announced as composites.	Strong pseudoprimes can pass the test.	$O(k \log n)^3$
Pocklington	Very efficient if there is a factor $q > \sqrt{n-1}$	Prime factors of $n-1$ are required to be already known.	$O(\ln \ln n)$
Lucas	Valid for any generic or special form numbers.	- Prime factors of $n-1$ are required to be already known. - In the event of a worst-case scenario, the execution time can be significantly prolonged.	$O(p^2 \log_p n)$
Proth	Very fast and reliable test to decide about Proth number.	Working well only with Proth numbers.	$O((k \log k + \log n) \log n)$

CONCLUSIONS AND SUGGESTIONS

The convergence of emerging technologies in Industry 4.0, such as IoT, cloud services, big data, and analytics, has ushered in a new industrial stage. IoT plays a vital role in facilitating seamless data exchange among physical objects, leading to an exponential increase in data volume. Consequently, ensuring data security and confidentiality becomes crucial to mitigate the rising frequency of data breaches. Cryptographic methods emerge as the most effective approach to safeguard information integrity. Within cryptographic algorithms, prime numbers hold significant importance, especially in asymmetric cryptosystems. The analysis of probabilistic methods for testing number primality reveals that the Millner-Rabin algorithm serves as a reliable tool for verifying the primality of integers within IoT technology, a key component of Industry 4.0.

List of used literature:

- Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber security in IoT-based cloud computing: A comprehensive survey. *Electronics*, 11(1), 16.
- Kumar, P., Kumar, R., Srivastava, G., Gupta, G. P., Tripathi, R., Gadekallu, T. R., & Xiong, N. N. (2021). PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities. *IEEE Transactions on Network Science and Engineering*, 8(3), 2326-2341.
- Salama, R., Altrjman, C., & Al-Turjman, F. (2023). An overview of the Internet of Things (IoT) and Machine to Machine (M2M) Communications. *NEU Journal for Artificial Intelligence and Internet of Things*, 2(3).
- T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, pp. 32 979–33 001, 2018.
- Nartey, C., Tchao, E. T., Gadze, J. D., Keelson, E., Klogo, G. S., Kommey, B., & Diawuo, K. (2021). On blockchain and IoT integration platforms: current implementation challenges and future perspectives. *Wireless Communications and Mobile Computing*, 2021, 1-25.
- Kantipudi, M. P., Moses, C. J., Aluvalu, R., & Kumar, S. (2021). Remote patient monitoring using IoT, cloud computing and AI. *Hybrid Artificial Intelligence and IoT in Healthcare*, 51-74.
- Alaghbari, K. A., Saad, M. H. M., Hussain, A., & Alam, M. R. (2022). Complex event processing for physical and cyber security in datacentres-recent progress, challenges and recommendations. *Journal of Cloud Computing*, 11(1), 65.
- Pulatovna, O. A., & Rasulovich, U. M. (2023). A method for improving Milner-Rabin algorithm to reduce the number of false witnesses. *Texas Journal of Engineering and Technology*, 18, 63-70.
- Koukouloupoulos, D. (2020). The distribution of prime numbers. *American Mathematical Soc.*
- Ishmukhametov, S. T., Mubarakov, B. G., & Rubtsova, R. G. (2020). On the number of witnesses in the Miller–Rabin primality test. *Symmetry*, 12(6), 890.
- D. M. Bressoud, "Factorizations and primality testing", in SpringerVerlag, NY, 1989, pp. 21-22.
- Duta, C. L., Gheorghe, L., & Tapus, N. (2015, May). Framework for evaluation and comparison of primality testing algorithms. In *2015 20th International Conference on Control Systems and Computer Science* (pp. 483-490). IEEE.
- Westerdijk, L. (2021). Algorithms for Testing Primality (Bachelor's thesis).

14. Nagell, T. (2021). Introduction to number theory (Vol. 163). American Mathematical Soc.
15. Adleman L. M., Huang M. D. Algorithmic Number Theory First International Symposium, ANTS-I Ithaca, NY, USA, May 6–9, 1994 Proceedings //Conference proceedings ANTS. – 1994. – P. 292.
16. Robert, Solovay., Volker, Strassen. "A Fast Monte-Carlo Test for Primality." SIAM Journal on Computing, 6 (1977):84-85. doi: 10.1137/0206006
17. M. O. Rabin, "Probabilistic Algorithms", in Academic Press, Algorithms and Complexity, New Directions and Recent Results, 1976, pp. 21-24.
18. R. Baillie, S.W. Jr. Wagstaff, "Lucas Pseudoprimes", in Math. Comput. vol 35, 1980, pp. 1391-1417.
19. Grau J., Oller-Marcén A., Sadornil D. A primality test for $Kp^n + 1$ numbers //Mathematics of Computation. – 2015. – T. 84. – №. 291. – P. 505-512.
20. Buchmann, Johannes, and Volker Müller. "Primality testing." (1992).
21. Pulatovna O. A., Rasulovich U. M. A method for improving Milner-Rabin algorithm to reduce the number of false witnesses //Texas Journal of Engineering and Technology. – 2023. – T. 18. – P. 63-70.

Proofreader: Zokir ALIBEKOV

Layout and Designer: Oloviddin Sobir ugli

2025. № 12

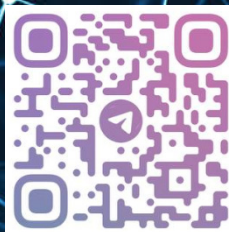
© When materials are reproduced, the INNOVATION SCIENCE AND TECHNOLOGY journal must be cited as the source. Authors are responsible for the accuracy of the information in materials and advertisements published in the journal. Editorial opinions may not always align with those of the authors. Submitted materials will not be returned to the editorial office.

To publish articles in this journal, you may submit articles, advertisements, stories, and other creative materials through the following links. Materials and advertisements are published on a paid basis.

You may subscribe to the journal at any time using the following details. Once subscribed, please send a screenshot or photo of your payment confirmation to our Telegram page @iqtisodiyot_77. Based on this, we will send the latest issue of the journal to your address each month.

“The journal “INNOVATION SCIENCE AND TECHNOLOGY” has been registered by the Agency for Information and Mass Communications under the Administration of the President of the Republic of Uzbekistan from 09.10.2024 under the registration number №390637. License number: C-5669633. PNFL: 30407832680027

Our address: Tashkent city, Yunusobod district, 19th block,
House 17.



Acceptance of articles

Published every
monthly



Directions

Social, economic, political,
technological, scientific



Scopus || Scientific electronic journal specializing in Scopus

CERTIFICATE NUMBER: №390637

**ORDER NUMBER ACCORDING TO
THE LICENSE REGISTER: C-5669633**

CONTACT:



Contact us
+998 50 737 87 88



Telegram channel
t.me/scopus_IST2100



Journal official website
<https://ist-journal.uz/index.php/IST>