MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE REPUBLIC OF KAZAKHSTAN

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН

KAZAKHSTAN

ХАЛЫҚАРАЛЫҚ УНИВЕРСИТЕТІ

INTERNATIONAL UNIVERSITY SINCE 2009

МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Published since 2020.
Volume 7. 3 (27). 2026
July–September

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

2020 жылдан бері шығарылады
Том 7. 3 (27). 2026
Шілде-Қыркүйек

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Издается с 2020 г.
Том 7. 3 (27). 2026
Июль-Сентябрь

Свидетельство о постановке на учет периодического печатного издания в Министерство информации и общественного развития Республики Казахстан № KZ82VPY00020475, выданное от 20.02.2020 г.

Зарегистрировано в Международном центре регистрации серийных изданий ISSN (ЮНЕСКО, Париж, Франция). ISSN 2708–2032 (print), ISSN 2708–2040 (online)

Журнал входит в Перечень научных изданий, рекомендуемых КОКНВО МНВО РК для публикации основных результатов научной деятельности.

EDITOR-IN-CHIEF:
Kateryna Kolesnikova — Doctor of Technical Sciences, professor, Vice-Rector for Research, International Information Technology University (Kazakhstan)

DEPUTY EDITOR-IN-CHIEF:
Madina Ipalakova — Candidate of Technical Sciences, associate professor, Director of the Research Department, International Information Technology University (Kazakhstan)

EDITORIAL BOARD:
Abdul Razak — PhD, professor, Department of Cybersecurity, International Information Technology University (Kazakhstan)
Lucio Tommaso De Paolis — Director of the R&D Department of the AVR Laboratory, Department of Engineering for Innovation, University of Salento (Italy)
Liz Bacon — Professor, Deputy Vice-Chancellor, Abertay University (United Kingdom)
Michele Pagano — PhD, Professor, University of Pisa (Italy)
Mukhtarbay Otelbayev — Doctor of Physical and Mathematical Sciences, professor, academician of the National Academy of Sciences of the Republic of Kazakhstan, professor of the Department of Mathematical and Computer Modeling, International Information Technology University (Kazakhstan)
Bolatbek Rysbaiuly — Doctor of Physical and Mathematical Sciences, professor, professor of the Department of Computing and Data Science, Astana IT University (Kazakhstan)
Yevgeniya Daineko — PhD, research professor, Department of Information Systems, International Information Technology University (Kazakhstan)
Nurzhan Duzbayev — PhD, associate professor, Vice-Rector for Digitalization and Innovation, International Information Technology University (Kazakhstan)
Bakhtgerei Sinchev — Doctor of Technical Sciences, professor, Department of Information Systems, International Information Technology University (Kazakhstan)
Nurgul Seilova — Candidate of Technical Sciences, Dean of the Faculty of Computer Technologies and Cybersecurity, International Information Technology University (Kazakhstan)
Ardak Mukhamediyeva — Candidate of Economic Sciences, Dean of the Faculty of Business, Media and Management, International Information Technology University (Kazakhstan)
Zamira Abdikalikova — PhD, associate professor, Head of the Department of Mathematical and Computer Modeling, International Information Technology University (Kazakhstan)
Yerlan Shildibekov — PhD, associate professor, Head of the Department of Economics and Business, International Information Technology University (Kazakhstan)
Damilya Yeskendirova — Candidate of Technical Sciences, associate professor, Head of the Department of Cybersecurity, International Information Technology University (Kazakhstan)
Aigul Niyazgulova — Candidate of Philological Sciences, Professor, Head of the Department of Media Communications and History of Kazakhstan, International Information Technology University (Kazakhstan)
Altai Aitmagambetov — Candidate of Technical Sciences, Professor, Department of Radio Engineering, Electronics and Telecommunications, International Information Technology University (Kazakhstan)
Yelena Bakhtiyarova — Candidate of Technical Sciences, associate professor, Head of the Department of Radio Engineering, Electronics and Telecommunications, International Information Technology University (Kazakhstan)
Kanibek Sansyzbay — PhD, research professor, Department of Cybersecurity, International Information Technology University (Kazakhstan)
Sakhybay Tynymbayev — Candidate of Technical Sciences, Professor, Research Professor, Department of Computer Engineering, International Information Technology University (Kazakhstan)
Ali Abd Almisreb — PhD, associate professor, Department of Cybersecurity, International Information Technology University (Kazakhstan)
Mohamed Ahmed Hamada — PhD, associate professor, Department of Information Systems, International Information Technology University (Kazakhstan)
Yang Im Chu — PhD, Professor, Gachon University (South Korea)
Tadeusz Wallas — PhD, Vice-Rector, Adam Mickiewicz University (Poland)
Orken Mamyrbayev — PhD, Deputy Director for Science, RSE Institute of Information and Computational Technologies, Committee for Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Kazakhstan)
Sergey Bushuyev — Doctor of Technical Sciences, professor, Director of the Ukrainian Project Management Association “UKRNET,” Head of the Department of Project Management, Kyiv National University of Construction and Architecture (Ukraine)
Svetlana Beloshitskaya — Doctor of Technical Sciences, professor, Department of Computing and Data Science, Astana IT University (Kazakhstan)

MANAGING EDITOR
Raushan Mrzabayeva — Master of Science, editor, International Information Technology University (Kazakhstan)

International Journal of Information and Communication Technologies
Periodicity: 4 times a year.
Languages: Kazakh, Russian, English
DOI prefix: 10.54309
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Thematic focus: "Information technology"; "Digital technologies in the development of socio-economic systems"; "Information security and communication technologies".
Distribution: Materials are distributed under the Creative Commons Attribution 4.0
Journal website: https://journal.iitu.edu.kz
Owner: International Information Technology University JSC (Almaty).
Copyright: © International Journal of Information and Communication Technologies, 2026

РЕДАКЦИЯ

БАС РЕДАКТОР:

Колесникова Катерина Викторовна — техника ғылымдарының докторы, профессор, Халықаралық ақпараттық технологиялар университетінің ғылыми-зерттеу қызметі жөніндегі проректор (Қазақстан)

БАС РЕДАКТОРДЫҢ ОРЫНБАСАРЫ:

Ипалакова Мадина Тулегеновна — техника ғылымдарының кандидаты, қауымдастырылған профессор, Халықаралық ақпараттық технологиялар университетінің ғылыми-зерттеу қызметі жөніндегі департамент директоры (Қазақстан)

РЕДАКЦИЯЛЫҚ АЛҚА:

Разак Абдул — PhD, Халықаралық ақпараттық технологиялар университеті киберқауіпсіздік кафедрасының профессоры (Қазақстан)

Лучио Томмазо де Паолис — Саленто Университеті (Италия) инновация және технологиялық инжиниринг департаменті AVR зертханасының зерттеу және әзірлеу бөлімінің директоры

Лиз Бэкон — профессор, Абертей Университеті (Ұлыбритания) вице-канцлерінің орынбасары

Микеле Пагано — PhD, Пиза Университетінің (Италия) профессоры

Өтелбаев Мухтарбай Өтелбайұлы — физика-математика ғылымдарының докторы, профессор, ҚР ҰҒА академигі, Халықаралық ақпараттық технологиялар университеті математика және компьютерлік модельдеу кафедрасының профессоры (Қазақстан)

Рысбайулы Болатбек — физика-математика ғылымдарының докторы, профессор, Есептеу және деректер ғылымдары департаментінің профессоры, Astana IT University (Казахстан)

Дайнеко Евгения Александровна — PhD, Халықаралық ақпараттық технологиялар университеті ақпараттық жүйелер кафедрасының профессор-зерттеушісі (Қазақстан)

Дузбаев Нуржан Токкужаевич — PhD, қауымдастырылған профессор, Халықаралық ақпараттық технологиялар университеті цифрландыру және инновациялар жөніндегі проректор (Қазақстан)

Синчев Бахтгерей Куспанович — техника ғылымдарының докторы, профессор, Халықаралық ақпараттық технологиялар университеті ақпараттық жүйелер кафедрасының профессоры (Қазақстан)

Сейлова Нургуль Абадуллаевна — техника ғылымдарының докторы, Халықаралық ақпараттық технологиялар университеті компьютерлік технологиялар және киберқауіпсіздік факультетінің деканы (Қазақстан)

Мухамедиева Ардак Габитовна — экономика ғылымдарының кандидаты, Халықаралық ақпараттық технологиялар университеті бизнеса медиа және басқару факультетінің деканы (Қазақстан)

Абдикаликова Замира Турсынбаевна — PhD, қауымдастырылған профессор, Халықаралық ақпараттық технологиялар университеті математика және компьютерлік модельдеу кафедрасының меңгерушісі (Қазақстан)

Шильдибеков Ерлан Жаржанович — PhD, қауымдастырылған профессор, Халықаралық ақпараттық технологиялар университеті экономика және бизнес кафедрасының меңгерушісі (Қазақстан)

Дамеля Максутовна Ескендирова — техника ғылымдарының кандидаты, қауымдастырылған профессор, Халықаралық ақпараттық технологиялар университеті киберқауіпсіздік кафедрасының меңгерушісі (Қазақстан)

Ниязгулова Айгуль Аскарбековна — филология ғылымдарының кандидаты, доцент, профессор, Халықаралық ақпараттық технологиялар университеті медиакоммуникация және Қазақстан тарихы кафедрасының меңгерушісі (Қазақстан)

Айтмагамбетов Алтай Зуфарович — техника ғылымдарының кандидаты, Халықаралық ақпараттық технологиялар университеті радиотехника, электроника және телекоммуникация кафедрасының профессоры (Қазақстан)

Бахтиярова Елена Ажибековна — техника ғылымдарының кандидаты, қауымдастырылған профессор, Халықаралық ақпараттық технологиялар университеті радиотехника, электроника және телекоммуникация кафедрасының меңгерушісі (Қазақстан)

Канибек Сансызбай — PhD, қауымдастырылған профессор, Халықаралық ақпараттық технологиялар университеті киберқауіпсіздік кафедрасының профессор-зерттеушісі (Қазақстан)

Тынымбаев Сахибай — техника ғылымдарының кандидаты, профессор, Халықаралық ақпараттық технологиялар университеті компьютерлік инженерия кафедрасының профессор-зерттеушісі (Қазақстан)

Алмисреб Али Абд — PhD, Халықаралық ақпараттық технологиялар университеті киберқауіпсіздік кафедрасының қауымдастырылған профессоры (Қазақстан)

Мохамед Ахмед Хамада — PhD, Халықаралық ақпараттық технологиялар университеті ақпараттық жүйелер кафедрасының қауымдастырылған профессоры (Қазақстан)

Янг Им Чу — PhD, Гачон университетінің профессоры (Оңтүстік Корея)

Тадеуш Валлас – PhD, Адам Мицкевич атындағы (Польша) университеттің проректоры

Мамырбаев Оркен Жумажанович — PhD, ҚР ҒЖБМ Ғылым комитеті ақпараттық және есептеу технологиялары институты ӨМК директорының ғылым жөніндегі орынбасары (Қазақстан)

Бушуев Сергей Дмитриевич — техника ғылымдарының докторы, профессор, Украинаның "УКРНЕТ" жобаларды басқару қауымдастығының директоры, Киев ұлттық құрылыс және сәулет университеті жобаларды басқару кафедрасының меңгерушісі (Украина)

Белощицкая Светлана Васильевна — техника ғылымдарының докторы, доцент, Astana IT University есептеу және деректер ғылымы кафедрасының профессоры (Қазақстан)

ЖАУАПТЫ РЕДАКТОР:

Мрзабаева Раушан Жалиевна — магистр, Халықаралық ақпараттық технологиялар университетінің редакторы (Қазақстан)

Халықаралық ақпараттық және коммуникациялық технологиялар журналы
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Префикс DOI: 10.54309
Мерзімділігі: жылына 4 рет.
Басылым тілі: қазақ, орыс, ағылшын.
Тақырып бағыты: "Ақпараттық технологиялар"; "Ақпараттық қауіпсіздік және коммуникациялық технологиялар"; "Әлеуметтік-экономикалық жүйелерді дамытудағы цифрлық технология".
Журнал сайты: https://journal.iitu.edu.kz
Тарату: материалдар Creative Commons Attribution 4.0 лицензиясы бойынша таратылады
Меншік иесі: АҚ «Халықаралық ақпараттық технологиялар университеті» (Алматы қ.).
Авторлық құқық: © Халықаралық ақпараттық және коммуникациялық технологиялар журналы, 2026

РЕДАКЦИЯ

ГЛАВНЫЙ РЕДАКТОР:

Колесникова Катерина Викторовна — доктор технических наук, профессор, проректор по научно-исследовательской деятельности Международного университета информационных технологий (Казахстан)

ЗАМЕСТИТЕЛЬ ГЛАВНОГО РЕДАКТОРА:

Ипалакова Мадина Тулегеновна — кандидат технических наук, ассоциированный профессор, директор департамента по научно-исследовательской деятельности Международного университета информационных технологий (Казахстан)

РЕДАКЦИОННАЯ КОЛЛЕГИЯ:

Разак Абдул — PhD, профессор кафедры кибербезопасности Международного университета информационных технологий (Казахстан)

Лучио Томмазо де Паолис — директор отдела исследований и разработок лаборатории AVR департамента инноваций и технологического инжиниринга Университета Саленто (Италия)

Лиз Бэкон — профессор, заместитель вице-канцлера Университета Абертей (Великобритания)

Микеле Пагано — PhD, профессор Университета Пизы (Италия)

Отелбаев Мухтарбай Отелбайулы — доктор физико-математических наук, профессор, академик НАН РК, профессор кафедры математического и компьютерного моделирования Международного университета информационных технологий (Казахстан)

Рысбайулы Болатбек — доктор физико-математических наук, профессор, профессор Astana IT University (Казахстан)

Дайнеко Евгения Александровна — PhD, профессор-исследователь кафедры информационных систем Международного университета информационных технологий (Казахстан)

Дузбаев Нуржан Токкужаевич — PhD, ассоциированный профессор, проректор по цифровизации и инновациям Международного университета информационных технологий (Казахстан)

Синчев Бахтгерей Куспанович — доктор технических наук, профессор, профессор кафедры информационных систем Международного университета информационных технологий (Казахстан)

Сейлова Нургуль Абадуллаевна — кандидат технических наук, декан факультета компьютерных технологий и кибербезопасности Международного университета информационных технологий (Казахстан)

Мухамедиева Ардак Габитовна — кандидат экономических наук, декан факультета бизнеса медиа и управления Международного университета информационных технологий (Казахстан)

Абдикаликова Замира Турсынбаевна — PhD, ассоциированный профессор, заведующая кафедрой математического и компьютерного моделирования Международного университета информационных технологий (Казахстан)

Шильдибеков Ерлан Жаржанович — PhD, ассоциированный профессор, заведующий кафедрой экономики и бизнеса Международного университета информационных технологий (Казахстан)

Дамеля Максутовна Ескендирова — кандидат технических наук, ассоциированный профессор, заведующая кафедрой кибербезопасности Международного университета информационных технологий (Казахстан)

Ниязгулова Айгуль Аскарбековна — кандидат филологических наук, доцент, профессор, заведующая кафедрой медиакоммуникаций и истории Казахстана Международного университета информационных технологий (Казахстан)

Айтмагамбетов Алтай Зуфарович — кандидат технических наук, профессор кафедры радиотехники, электроники и телекоммуникаций Международного университета информационных технологий (Казахстан)

Бахтиярова Елена Ажибековна — кандидат технических наук, ассоциированный профессор, заведующая кафедрой радиотехники, электроники и телекоммуникаций Международного университета информационных технологий (Казахстан)

Канибек Сансызбай – PhD, ассоциированный профессор, профессор-исследователь кафедры кибербезопасности, Международного университета информационных технологий (Казахстан)

Тынымбаев Сахибай – кандидат технических наук, профессор, профессор-исследователь кафедры компьютерной инженерии, Международного университета информационных технологий (Казахстан)

Алмисреб Али Абд — PhD, ассоциированный профессор кафедры кибербезопасности Международного университета информационных технологий (Казахстан)

Мохамед Ахмед Хамада — PhD, ассоциированный профессор кафедры информационных систем Международного университета информационных технологий (Казахстан)

Янг Им Чу — PhD, профессор университета Гачон (Южная Корея)

Тадеуш Валлас – PhD, проректор университета имен Адама Мицкевича (Польша)

Мамырбаев Оркен Жумажанович — PhD, заместитель директора по науке РГП Института информационных и вычислительных технологий Комитета науки МНВО РК (Казахстан)

Бушуев Сергей Дмитриевич — доктор технических наук, профессор, директор Украинской ассоциации управления проектами «УКРНЕТ», заведующий кафедрой управления проектами Киевского национального университета строительства и архитектуры (Украина)

Белощицкая Светлана Васильевна — доктор технических наук, доцент, профессор кафедры вычислений и науки о данных Astana IT University (Казахстан)

ОТВЕТСТВЕННЫЙ РЕДАКТОР:

Мрзабаева Раушан Жалиевна — магистр, редактор Международного университета информационных технологий (Казахстан)

Международный журнал информационных и коммуникационных технологий
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Префикс DOI: 10.54309
Периодичность: 4 выпусков в год.
Язык издания: казахский, русский, английский.
Тематическая направленность: "Информационные технологии"; "Информационная безопасность и коммуникационные технологии"; "Цифровые технологии в развитии социо-экономических систем".
Сайт журнала: https://journal.iitu.edu.kz
Распространение: материалы распространяются по лицензии Creative Commons Attribution 4.0
Собственник: АО «Международный университет информационных технологий» (г. Алматы).
Авторские права: © Международный журнал информационных и коммуникационных технологий, 2026

CONTENTS

DIGITAL TECHNOLOGIES IN THE DEVELOPMENT OF SOCIO-ECONOMIC SYSTEMS

A Adalbek, S.Ye. Kerimkhulle, K.D. Kuliev, O. Mekesh, Zh.Zh. Khamitova
DEVELOPMENT OF RESULT-ORIENTED DATA SMOOTHING MODELS AND ANALYSIS OF THEIR EFFECTIVENESS 11
A.T. Iskakova, G.E. Kurmankulova, K. Gromaszek, K.O. Togzhanova, R.S. Algozhayeva
APPLICATION OF MACHINE LEARNING AND DEEP LEARNING FOR PREDICTIVE PLANNING AND RESOURCE EFFICIENCY IN PRODUCTION SYSTEMS 30
A.B. Kassymova, R.K. Uskenbayeva, Zh.A. Sydykov, D. Omirzak, S. Kalibekov
ARCHITECTURE OF AN INTELLIGENT CHATBOT FOR SMART CITY: AI-BASED RECEIVING, ANALYSIS AND ROUTING OF CITIZEN REQUESTS 46
O.M. Olzhayev, B.S. Omarov, A. Suliman
YOLO-CBAM: A LIGHTWEIGHT NEURAL NETWORK MODEL WITH INTEGRATED ATTENTION MECHANISM FOR ROAD DAMAGE ANALYSIS 66
K. Yermagambetova, A. Sarsekeyeva, Y. Akhlassov
OVERCOMING FRAGMENTATION IN THE CLASSIFICATION OF DIGITAL CULTURAL HERITAGE: AN INTEGRATIVE MULTIDIMENSIONAL MODEL 78

INFORMATION TECHNOLOGY

D. Abzhanova, S. Sharipova
ARCHITECTURE AND PRACTICAL IMPLEMENTATION OF A DIGITAL PLATFORM FOR MONITORING AND DATA EXCHANGE ON TRANSBOUNDARY WATER RESOURCES IN THE ZHAMBYL REGION 101
A. Aitanuly, O.A. Ussatova
ENHANCING TWO-FACTOR AUTHENTICATION FOR CLOUD HEALTHCARE SECURITY: THE ROLE OF DEEP LEARNING 122
O. Alseitov, O. Kuchanskyi
PHYSICS-INFORMED HYBRID LEARNING FOR HOURLY POWER-PLANT EMISSIONS: A MULTI-POLLUTANT BENCHMARK WITH UNCERTAINTY AND TRANSFER 141
A.M. Akhmetova, D.O. Baizhanova, Zh.N. Alisheva, B.A. Shaimov
ADAPTIVE OUTPUT ROUTER FOR NATURAL LANGUAGE MODELS CONSIDERING KEY PERFORMANCE INDICATORS 160
A.K. Aitim
AUTOMATIC AND SEMI-AUTOMATIC ANNOTATION OF KAZAKH TEXT CORPORA 180
Z.E. Balabayev, S.V. Biloshchytska
HANDWRITTEN TEXT RECOGNITION FOR CHAGATAI MANUSCRIPTS: COMPARING CRNN TRAINING FROM SCRATCH AND TRANSFORMER-BASED TRANSFER LEARNING 198
D.B. Baumuratova, T.K. Zhukabayeva, K.A. Abdrakhmanov, Z. Ahmad, A.A. Seitov
A NEURO-DIGITAL LEARNING MODEL FOR AI DRIVEN DIGITAL TRANSFORMATION IN HIGHER EDUCATION 219
T. Daoyun, G.A. Amirkhanova, Fu Yanwei, Y. Faruzkyzy
MULTIMODAL SEMANTIC MANIPULATION IN FAKE VIDEOS AND ITS INFLUENCE MECHANISM ON USERS' PERCEIVED TRUST 241
Zh. Doumchariyev, J. Tussupov, A. Akynbekova, M. Khassanova, M. Kassim
ENSEMBLE AND HYBRID LEARNING FOR DIGITAL TWIN MILK CLASSIFICATION 258
K.Z. Igibayev, A.Kh. Kozbakova, O. Auelbekov , T. Merembayev, K. Yessentayev
STUDY OF A DYNAMIC MIXING DEVICE IN A BIOREACTOR USING IOT TECHNOLOGIES 279
A.N. Ismukanova, G. Kochshanova, D.V. Pleskachev, Zh. Sarsenbayeva, P. Schmidt
AUTOMATED CLASSIFICATION OF SCIENTIFIC DATA USING ARTIFICIAL INTELLIGENCE: A COMPARATIVE ANALYSIS OF TRANSFORMER ARCHITECTURES AND HYBRID APPROACHES 306
T. Zh. Kamalov, Ali Abd. Almisreb, Mohammed A. Saleh
INVESTIGATION OF HYBRID QUANTUM-CLASSICAL ALGORITHMS FOR MACHINE LEARNING 323
B. Karimkyzy, K.G. Karasenko, N.A. Alisherov, N.M. Muratbek, A. Karim

KEY PUBLICATIONS OF 2021–2025 ON ARTIFICIAL INTELLIGENCE METHODS IN THE MANUFACTURING AND DIAGNOSTICS OF MEDICAL DEVICES FOR GLYCEMIC MONITORING: A THEMATIC ANALYTICAL REVIEW 338
S.K. Kumyzbaeva, K.E. Baglanbaev, K.S. Sarkyt, M.Zh. Konyrova
THREE-PHASE TRAINING OF INTELLIGENT ENERGY MANAGEMENT FOR A HYBRID ENERGY SYSTEM WITH A CLIMATE-AWARE STATE REPRESENTATION 357
N.E. Karabayev, S.K. Serikbayeva, E. Benkhelif, B. Tassuov
RESEARCH ON THE ROBUSTNESS OF ENSEMBLE MACHINE LEARNING MODELS TO ADVERSARIAL ATTACKS IN INTRUSION DETECTION SYSTEMS FOR IOT NETWORKS 369
M. Nurtas, G. Kapyshev
A METHODOLOGICAL FRAMEWORK FOR THE PREPROCESSING AND INTEGRATION OF GEOSPATIAL AND GEOPHYSICAL DATA FOR MINERAL PROSPECTIVITY PREDICTION USING MACHINE LEARNING 392
A. Neftissov, A. Biloshchytskyi, I. Kazambayev, A. Medetkhan, L. Kirichenko
ENERGY EFFICIENT MICROCLIMATE STABILIZATION FOR SEALED ARCHIVAL STORAGE ENCLOSURES 405
A.Zh. Omurtayeva, U.T. Makhazhanova, A.K. Adilova, Sh.K. Yelezhanova, J. Kultan
AN ADAPTIVE NEURAL-FUZZY MODEL FOR ASSESSING INVESTMENT RISKS IN THE AGRI-INDUSTRIAL COMPLEX: ODERNISATION OF THE DECISION-SUPPORT ARCHITECTURE THROUGH THE INTEGRATION OF MACHINE LEARNING 421
N. Shazhdekeyeva, A. Mukhanbetkaliyeva, A. Abdigaliyeva, A. Zhanekeshova, L. Nurgaliyeva
COMPARATIVE ANALYSIS OF MATHEMATICAL MODELS OF COLLABORATIVE FILTERING IN THE DEVELOPMENT OF A MOVIE RECOMMENDER SYSTEM 445
S. Sharmukhanbet, G. Turmukhanova, O. Findik, V. Makhatova, M. Rakhmetov
AN INTELLIGENT PIPELINE DEFECT DETECTION SYSTEM USING AN IN-PIPE ROBOT 461

INFORMATION SECURITY AND COMMUNICATIONTECHNOLOGIES

S.Z. Daruish, A.U. Utegenova, A.U. Kalizhanova, Zh.Zh. Zhumabekova
MACHINE LEARNING FOR POLLUTION CLASSIFICATION IN ROCKET BOOSTER IMPACT AREAS 480
S.N. Issabayeva, A.K. Rysbayeva, Zh.B. Ibrayeva, N.R. Mussabekov, N.Sh. Akimzhan
MACHINE LEARNING-BASED CYBERATTACK DETECTION IN OT-NETWORKS: A COMPARATIVE ANALYSIS OF NETWORK ANOMALY CLASSIFICATION METHODS 495
G. Shangytbayeva, A.N. Amanov, M.K. Issenova, G.E. Berikkhanova, K.O. Shakerkhan
INFORMATION SECURITY IN GOVERNMENT CLOUD SERVICES: RISK ASSESSMENT AND PROTECTION STRATEGIES 512
Ye. N. Tursynbek, N. Albanbay, D. Djenouri
OPTIMISATION OF COMMUNICATION COSTS IN TWO-TIER FEDERATED LEARNING FOR CYBERATTACK DETECTION IN IOT NETWORKS 529
A. Tastemirov, S.B. Mukhanov, S.T. Amanzholova, B. Aldosh
A COMPARATIVE EVALUATION OF MACHINE LEARNING MODELS FOR ACTIVE DIRECTORY THREAT DETECTION: FEATURE-LEAKAGE CONTROL AND CROSS-SCENARIO VALIDATION ON WINDOWS SECURITY EVENT LOGS 545

МАЗМҰНЫ
ӘЛЕУМЕТТІК-ЭКОНОМИКАЛЫҚ ЖҮЙЕЛЕРДІ ДАМЫТУДАҒЫ ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАР

А Адалбек, С.Е. Керімқұл, К.Д. Кулиев, О. Мекеш, Ж.Ж. Хамитова
ДЕРЕКТЕРДІҢ НӘТИЖЕ БАҒДАРЛАНҒАН ТЕГІСТЕУ МОДЕЛЬДЕРІН ӘЗІРЛЕУ ЖӘНЕ ОЛАРДЫҢ ТИІМДІЛІГІН ТАЛДАУ 11
А.Т. Искакова, Г.Е. Курманкулова, Конрад Громашек, К.О. Тогжанова, Р.С. Алгожаева
ӨНДІРІС ЖҮЙЕЛЕРІНДЕ БОЛЖАМДЫ ЖОСПАРЛАУ ЖӘНЕ РЕСУРСТАРДЫ ҮНЕМДЕУ ҮШІН МАШИНАЛЫҚ ЖӘНЕ ТЕРЕҢ ОҚЫТУДЫ ҚОЛДАНУ 30
А.Б. Касымова, Р.К. Ускенбаева, Ж.А. Сыдыков, Д. Өмірзақ, С. Калибеков
SMART CITY ҮШІН ИНТЕЛЛЕКТУАЛДЫ ЧАТ-БОТ АРХИТЕКТУРАСЫ: АЗАМАТТАРДЫҢ

ӨТІНІШТЕРІН ЖАСАНДЫ ИНТЕЛЛЕКТ НЕГІЗІНДЕ ҚАБЫЛДАУ, ТАЛДАУ ЖӘНЕ БАҒЫТТАУ 46
О.М. Олжаев, Б.С. Омаров, A.Suliman
YOLO-CBAM: ЖОЛДЫҢ ЗАҚЫМДАНУЫН ТАЛДАУҒА АРНАЛҒАН ИНТЕГРАЦИЯЛАНҒАН ЗЕЙІН МЕХАНИЗМІ БАР ЖЕҢІЛ САЛМАҚТЫ НЕЙРОНДЫҚ ЖЕЛІ МОДЕЛІ 66
К. Ермагамбетова, А. Сарсекеева, Е. Ахласов
ЦИФРЛЫҚ МӘДЕНИ МҰРАНЫ ЖІКТЕУДЕГІ ФРАГМЕНТАЦИЯНЫ ЕҢСЕРУ: ИНТЕГРАТИВТІ КӨПӨЛШЕМДІ МОДЕЛЬ 78

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР

Д.Е. Абжанова, С.Е. Шарипова
ЖАМБЫЛ ӨҢІРІНІҢ ТРАНСШЕКАРАЛЫҚ СУ РЕСУРСТАРЫН МОНИТОРИНГТЕУ ЖӘНЕ ДЕРЕКТЕР АЛМАСУҒА АРНАЛҒАН ЦИФРЛЫҚ ПЛАТФОРМАНЫҢ АРХИТЕКТУРАСЫ МЕН ПРАКТИКАЛЫҚ ІСКЕ АСЫРЫЛУЫ 101
А.Айтанұлы, О.А. Усатова
БҰЛТТЫ МЕДИЦИНАЛЫҚ ЖҮЙЕЛЕРДЕ ЕКІ ФАКТОРЛЫ АУТЕНТИФИКАЦИЯНЫ ЖАҚСАРТУ: ТЕРЕҢ ОҚЫТУ ӘДІСТЕРІНІҢ ҚОЛДАНУ МҮМКІНДІКТЕРІ 122
О. Альсеитов, О. Кучанский
ЭЛЕКТР СТАНЦИЯЛАРЫНЫҢ САҒАТТЫҚ ШЫҒАРЫНДЫЛАРЫН ФИЗИКАЛЫҚ ЗАҢДЫЛЫҚТАРДЫ ЕСКЕРЕТІН ГИБРИДТІ ОҚЫТУ: БЕЛГІСІЗДІК ПЕН ТАСЫМАЛДАУДЫ ЕСКЕРЕТІН КӨПЛАСТАУЫШТЫ БЕНЧМАРК 141
А.М. Ахметова, Д.О. Байжанова, Ж.Н. Алишева, Б.А. Шаймов
КРІ КӨРСЕТКІШТЕРІН ЕСКЕРЕ ОТЫРЫП, ТАБИҒИ ТІЛ МОДЕЛЬДЕРІНЕ АРНАЛҒАН ШЫҒЫС МАРШРУТТАУЫНЫҢ АДАПТИВТІ ЖҮЙЕСІ 160
Ә.Қ. Әйтім
ҚАЗАҚ МӘТІНДІК КОРПУСТАРЫН АВТОМАТТЫ ЖӘНЕ ЖАРТЫЛАЙ АВТОМАТТЫ АННОТАЦИЯЛАУ 180
Ж.Е. Балабаев, С.В. Белощицкая
ШАҒАТАЙ ҚОЛЖАЗБАЛАРЫНЫҢ МӘТІНІН ТАНУ: CRNN-ДІ НӨЛДЕН БАСТАП ОҚЫТУ МЕН ТРАНСФОРМЕР НЕГІЗІНДЕГІ ТРАНСФЕРЛІК ОҚЫТУДЫ САЛЫСТЫРУ 198
Д.Б. Баумуратова, Т.К. Жукабаева, К.А. Абдрахманов, З. Ахмад, А.А. Сеитов
ЖОҒАРЫ БІЛІМ БЕРУДЕ AI НЕГІЗДЕЛГЕН ЦИФРЛЫҚ ТРАНСФОРМАЦИЯҒА АРНАЛҒАН НЕЙРО-ЦИФРЛЫҚ ОҚЫТУ МОДЕЛІ 219
Т. Даоюн, Г. Амирханова, Фу Яньвэй, Е. Фарузқызы
ФЕЙК ВИДЕОЛАРДАҒЫ МУЛЬТИМОДАЛЬДЫ СЕМАНТИКАЛЫҚ МАНИПУЛЯЦИЯНЫҢ ПАЙДАЛАНУШЫЛАРДЫҢ ҚАБЫЛДАЙТЫН СЕНІМІНЕ ӘСЕР ЕТУ МЕХАНИЗМІ 241
Ж. Доумчариева, Д. Тусупов, А. Акынбекова, М. Хасанова, М. Кассим
ЦИФРЛЫҚ ЕГІЗДЕГІ СҮТ САПАСЫН АНСАМБЛЬДІК ЖӘНЕ ГИБРИДТІ ОҚЫТУ АРҚЫЛЫ ЖІКТЕУ 258
Қ.З. Игибаев, А.Х. Козбакова, О. Әуелбеков, Т. Мерембаев, Қ. Есентаев
БИОРЕАКТОРДА IoT ТЕХНОЛОГИЯЛАРЫН ПАЙДАЛАНА ОТЫРЫП ДИНАМИКАЛЫҚ АРАЛАСТЫРУ ҚҰРЫЛҒЫСЫН ЗЕРТТЕУ 279
А.Н. Исмуканова, Г.Кощанова, Д.В. Плескачев, Ж.Сарсенбаева, П. Шмидт
ЖАСАНДЫ ИНТЕЛЛЕКТ НЕГІЗІНДЕ ҒЫЛЫМИ ДЕРЕКТЕРДІ АВТОМАТТЫ ТҮРДЕ ЖІКТЕУ: ТРАНСФОРМЕР АРХИТЕКТУРАЛАРЫ МЕН ГИБРИДТІ ТӘСІЛДЕРДІҢ САЛЫСТЫРМАЛЫ ТАЛДАУЫ 306
Т.Ж. Камалов, Али Абд. Альмисреб, Мохаммед А. Салех
МАШИНАЛЫҚ ОҚЫТУҒА АРНАЛҒАН ГИБРИДТІ КВАНТТЫҚ-КЛАССИКАЛЫҚ АЛГОРИТМДЕРІН ЗЕРТТЕУ 323
Б. Кәрімқызы, К.Г. Карасенко, Н.А. Әлішеров, Н.М. Мұратбек, А. Кәрім
2021–2025 ЖЫЛДАР АРАЛЫҒЫНДАҒЫ ГЛИКЕМИЯЛЫҚ МОНИТОРИНГКЕ АРНАЛҒАН МЕДИЦИНАЛЫҚ ҚҰРЫЛҒЫЛАРДЫ ӨНДІРУ ЖӘНЕ ДИАГНОСТИКАЛАУДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕКТ ӘДІСТЕРІ БОЙЫНША НЕГІЗГІ ЖАРИЯЛАНЫМДАР 338
С. К. Кумызбаева, К.Е. Багланбаев, К.С. Саркыт, М. Конырова
КҮЙ-ЖАЙДЫ КЛИМАТҚА СЕЗІМТАЛ ҰСЫНУМЕН ГИБРИДТІ ЭНЕРГОЖҮЙЕНІҢ ИНТЕЛЛЕКТУАЛДЫ ЭНЕРГОМЕНЕДЖМЕНТІН ҮШФАЗАЛЫ ОҚЫТУ 357
Н.Е. Қарабаев, С.К. Серикбаева, Е. Бенкхелифа, Б. Тасуов

IOT-ЖЕЛІЛЕРІНДЕГІ БАСЫП КІРУДІ АНЫҚТАУЖҮЙЕЛЕРІНДЕ МАШИНАЛЫҚ ОҚЫТУДЫҢ АНСАМБЛЬДІ КҮЛГІЛЕРІНІҢ БӘСЕКЕЛЕС ШАБУЫЛДАРҒА ТӨЗІМДІЛІГІН ЗЕРТТЕУ 369
М. Нұртас, Ғ. Капышев
МАШИНАЛЫҚ ОҚЫТУДЫ ҚОЛДАНА ОТЫРЫП, ПАЙДАЛЫ ҚАЗБАЛАРДЫҢ ПЕРСПЕКТИВАЛЫЛЫҒЫН БОЛЖАУ ҮШІН ГЕОКЕҢІСТІКТІК ЖӘНЕ ГЕОФИЗИКАЛЫҚ ДЕРЕКТЕРДІ АЛДЫН АЛА ӨҢДЕУ ЖӘНЕ БІРІКТІРУДІҢ ӘДІСТЕМЕЛІК НЕГІЗІ 392
А. Нефтиссов, А. Билощицкий, И. Казамбаев, А. Медетхан, Л. Кириченко
ГЕРМЕТИКАЛЫҚ АРХИВТІК САҚТАУ ҚАПТАМАЛАРЫНДА МИКРОКЛИМАТТЫ ЭНЕРГИЯ ТИІМДІЛІГІН ЕСКЕРЕ ОТЫРЫП ТҰРАҚТАНДЫРУ 405
Ә.Ж. Омуртаева, У.Т. Махажанова, А.К. Адилова, Ш.К. Ележанова, Я. Култан
АГРОӨНЕРКӘСІПТІК КЕШЕНДЕГІ ИНВЕСТИЦИЯЛЫҚ ТӘУЕКЕЛДЕРДІ БАҒАЛАУҒА АРНАЛҒАН БЕЙІМДЕЛГІШ НЕЙРОНДЫҚ-БҰЛДЫР МОДЕЛЬ: МАШИНАЛЫҚ ОҚЫТУДЫ ИНТЕГРАЦИЯЛАУ АРҚЫЛЫ ШЕШІМ ҚАБЫЛДАУДЫ ҚОЛДАУ СӘУЛЕТІН ЖАҢҒЫРТУ 421
Н. Шаждекеева, А. Мұханбетқалиева, А. Әбдіғалиева, А. Жанекешова, Л. Нұрғалиева
ФИЛЬМДЕРДІ ҰСЫНУ ЖҮЙЕСІН ҚҰРУ КЕЗІНДЕГІ КОЛЛАБОРАТИВТІК СҮЗГІЛЕУДІҢ МАТЕМАТИКАЛЫҚ МОДЕЛЬДЕРІН САЛЫСТЫРМАЛЫ ТАЛДАУ 445
С. Шармұханбет, Г. Тұрмұханова, О. Финдик, В. Махатова, М. Рахметов
ҚҰБЫРІШІЛІК РОБОТТЫ ПАЙДАЛАНУ АРҚЫЛЫ ҚҰБЫР АҚАУЛАРЫН АНЫҚТАУДЫҢ ЗИЯТКЕРЛІК ЖҮЙЕСІ 461

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАРҒА АРНАЛҒАН

С.З. Дәруіш, А.У. Утегенова, А.У. Калижанова, Ж.Ж. Жумабекова
ЗЫМЫРАН ТАСЫМАЛДАУШЫЛАРДЫҢ ҚҰЛАУ АЙМАҚТАРЫНЫҢ ЛАСТАНУЫН МАШИНАЛЫҚ ОҚЫТУМЕН ЖІКТЕУ 480
С.Н. Исабаева, А.К. Рысбаева, Ж.Б. Ибраева, Н.Р. Муссабеков, Н.Ш. Акимжан
МАШИНАЛЫҚ ОҚЫТУ НЕГІЗІНДЕ ОТ-ЖЕЛІЛЕРІНДЕГІ КИБЕРШАБУЫЛДАРДЫ АНЫҚТАУ: ЖЕЛІЛІК АНОМАЛИЯЛАРДЫ ЖІКТЕУ ӘДІСТЕРІНІҢ САЛЫСТЫРМАЛЫ ТАЛДАУЫ 495
Г.А. Шангытбаева, А.Н. Аманов, М.К. Исенова, Г.Е. Берикханова, Қ.О. Шакерхан
МЕМЛЕКЕТТІК ОРГАНДАРДЫҢ БҰЛТТЫ СЕРВИСТЕРІНДЕГІ АҚПАРАТТЫҚ ҚАУІПСІЗДІК: ТӘУЕКЕЛДЕРДІ БАҒАЛАУ ЖӘНЕ ҚОРҒАУ СТРАТЕГИЯЛАРЫ 512
Е.Н. Турсынбек, Н. Албанбай, Д. Дженоури
IOT ЖЕЛІЛЕРІНДЕ КИБЕРШАБУЫЛДАРДЫ АНЫҚТАУ ҮШІН ЕКІ ДЕҢГЕЙЛІ ФЕДЕРАЦИЯЛАНҒАН ОҚЫТУДАҒЫ БАЙЛАНЫС ШЫҒЫНДАРЫН ОҢТАЙЛАНДЫРУ 529
А. Тастемиров, С.Т. Аманжолова, Б. Алдош, С.Б. Муханов
ACTIVE DIRECTORY ЖҮЙЕСІНДЕ ҚАУІПТЕРДІ АНЫҚТАУ ҮШІН МАШИНАЛЫҚ ОҚЫТУ МОДЕЛЬДЕРІН САЛЫСТЫРМАЛЫ БАҒАЛАУ: WINDOWS ҚАУІПСІЗДІК ОҚИҒАЛАРЫ ЖУРНАЛДАРЫНДА БЕЛГІ ЖЫЛЫСТАУЫН БАҚЫЛАУ ЖӘНЕ КРОСС-СЦЕНАРЛЫҚ ВАЛИДАЦИЯ 545

СОДЕРЖАНИЕ
ЦИФРОВЫЕ ТЕХНОЛОГИИ В РАЗВИТИИСОЦИО-ЭКОНОМИЧЕСКИХ СИСТЕМ

А Адалбек, С.Е. Керимкулов, К.Д. Кулиев, О. Мекеш, Ж.Ж. Хамитова
РАЗРАБОТКА РЕЗУЛЬТАТИВНО-ОРИЕНТИРОВАННЫХ МОДЕЛЕЙ СГЛАЖИВАНИЯ ДАННЫХ И АНАЛИЗ ИХ ЭФФЕКТИВНОСТИ 11
А.Т. Искакова, Г.Е. Курманкулова, К. Громашек, К.О. Тогжанова, Р.С. Алгожаева
ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО И ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ ПРОГНОЗНОГО ПЛАНИРОВАНИЯ И РЕСУРСОСБЕРЕЖЕНИЯ В ПРОИЗВОДСТВЕННЫХ СИСТЕМАХ 30
А.Б. Касымова, Р.К. Ускенбаева, Ж.А.Сыдыков, Д. Омирзак, С. Калибеков
АРХИТЕКТУРА ИНТЕЛЛЕКТУАЛЬНОГО ЧАТ-БОТА ДЛЯ SMART CITY: ПРИЁМ, АНАЛИЗ И МАРШРУТИЗАЦИЯ ОБРАЩЕНИЙ ГРАЖДАН НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА 46
О.М. Олжаев, Б.С. Омаров, A.Suliman
YOLO-CBAM: ЛЕГКОВЕСНАЯ НЕЙРОСЕТЕВАЯ МОДЕЛЬ С ИНТЕГРИРОВАННЫМ МЕХАНИЗМОМ ВНИМАНИЯ ДЛЯ АНАЛИЗА ДОРОЖНЫХ ПОВРЕЖДЕНИЙ 66
К. Ермагамбетова, А. Сарсекеева, Е. Ахласов
ПРЕОДОЛЕНИЕ ФРАГМЕНТАЦИИ В КЛАССИФИКАЦИИ ЦИФРОВОГО КУЛЬТУРНОГО НАСЛЕДИЯ:

ИНТЕГРАТИВНАЯ МНОГОМЕРНАЯ МОДЕЛЬ 78

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Д.Е. Абжанова, С.Е. Шарипова
АРХИТЕКТУРА И ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ ЦИФРОВОЙ ПЛАТФОРМЫ МОНИТОРИНГА И ОБМЕНА ДАННЫМИ О ТРАНСГРАНИЧНЫХ ВОДНЫХ РЕСУРСАХ ЖАМБЫЛСКОГО РЕГИОНА 101
А. Айтанулы, О.А. Усатова
СОВЕРШЕНСТВОВАНИЕ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЛАЧНЫХ МЕДИЦИНСКИХ СИСТЕМ: ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ 122
О. Альсеитов, О. Кучанский
ФИЗИЧЕСКИ ИНФОРМИРОВАННОЕ ГИБРИДНОЕ ОБУЧЕНИЕ ДЛЯ ПОЧАСОВОГО ПРОГНОЗИРОВАНИЯ ВЫБРОСОВ ЭЛЕКТРОСТАНЦИЙ: МНОГОКОМПОНЕНТНЫЙ БЕНЧМАРК С ОЦЕНКОЙ НЕОПРЕДЕЛЁННОСТИ И ПЕРЕНОСИМОСТЬЮ МОДЕЛЕЙ 141
А.М. Ахметова, Д.О. Байжанова, Ж.Н. Алишева, Б.А. Шаймов
АДАПТИВНЫЙ МАРШРУТИЗАТОР ВЫВОДА С УЧЕТОМ КЛЮЧЕВЫХ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ ДЛЯ МОДЕЛЕЙ ЕСТЕСТВЕННОГО ЯЗЫКА 160
Ә.Қ. Әйтім
АВТОМАТИЧЕСКАЯ И ПОЛУАВТОМАТИЧЕСКАЯ АННОТАЦИЯ КАЗАХСКИХ ТЕКСТОВЫХ КОРПУСОВ 180
Ж.Е. Балабаев, С.В. Белощицкая
РАСПОЗНАВАНИЕ РУКОПИСНОГО ТЕКСТА ШАГАТАЙСКИХ РУКОПИСЕЙ: СРАВНЕНИЕ ОБУЧЕНИЯ CRNN С НУЛЯ И ТРАНСФЕРНОГО ОБУЧЕНИЯ НА БАЗЕ ТРАНСФОРМЕРОВ 198
Д.Б. Баумуратова, Т.К. Жукабаева, К.А. Абдрахманов, З. Ахмад, А.А. Сеитов
НЕЙРО-ЦИФРОВАЯ МОДЕЛЬ ОБУЧЕНИЯ ДЛЯ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ С ПОМОЩЬЮ AI 219
Т. Даоюн, Г. Амирханова, Фу Яньвэй, Е. Фарузкызы
МЕХАНИЗМ ВЛИЯНИЯ МУЛЬТИМОДАЛЬНОЙ СЕМАНТИЧЕСКОЙ МАНИПУЛЯЦИИ В ФЕЙКОВЫХ ВИДЕО НА ВОСПРИНИМАЕМОЕ ДОВЕРИЕ ПОЛЬЗОВАТЕЛЕЙ 241
Ж. Доумчариева, Д. Тусупов, А. Акынбекова, М. Хасанова, М. Кассим
КЛАССИФИКАЦИЯ КАЧЕСТВА МОЛОКА В ЦИФРОВОМ ДВОЙНИКЕ АНСАМБЛЕВЫМИ И ГИБРИДНЫМИ МЕТОДАМИ 258
К.З. Игибаев, А.Х. Козбакова, О. Ауелбеков, Т. Мерембаев, К. Есентаев
ИССЛЕДОВАНИЕ УСТРОЙСТВА ДИНАМИЧЕСКОГО ПЕРЕМЕШИВАНИЯ В БИОРЕАКТОРЕ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ IoT 279
А. Н. Исмуканова, Г.Кощанова, Д.В. Плескачев, Ж.Сарсенбаева, П. Шмидт
АВТОМАТИЗИРОВАННАЯ КЛАССИФИКАЦИЯ НАУЧНЫХ ДАННЫХ НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТРАНСФОРМЕРНЫХ АРХИТЕКТУР И ГИБРИДНЫХ МЕТОДОВ 306
Т.Ж. Камалов, Али Абд. Альмисреб, Мохаммед А. Салех
ИССЛЕДОВАНИЕ ГИБРИДНЫХ КВАНТОВО-КЛАССИЧЕСКИХ АЛГОРИТМОВ ДЛЯ МАШИННОГО ОБУЧЕНИЯ 323
Б. Каримкызы, К.Г. Карасенко, Н.А. Алишеров, Н.М. Муратбек, А. Карим
КЛЮЧЕВЫЕ ПУБЛИКАЦИИ 2021–2025 ГОДОВ ПО МЕТОДАМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОИЗВОДСТВЕ И ДИАГНОСТИКЕ МЕДИЦИНСКИХ ИЗДЕЛИЙ ДЛЯ ГЛИКЕМИЧЕСКОГО МОНИТОРИНГА 338
С.К. Кумызбаева, К.Е. Багланбаев, К.С. Сарқыт, М.Ж. Конырова
ТРЁХФАЗОВОЕ ОБУЧЕНИЕ ИНТЕЛЛЕКТУАЛЬНОГО ЭНЕРГОМЕНЕДЖМЕНТА ГИБРИДНОЙ ЭНЕРГОСИСТЕМЫ С КЛИМАТО-ОСВЕДОМЛЁННЫМ ПРЕДСТАВЛЕНИЕМ СОСТОЯНИЯ 357
Н.Е. Қарабаев, С.К. Серикбаева, Е. Бенкхелифа, Б. Тасуов
ИССЛЕДОВАНИЕ УСТОЙЧИВОСТИ АНСАМБЛЕВЫХ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ К СОСТЯЗАТЕЛЬНЫМ АТАКАМ В СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ IOT-СЕТЕЙ 369
М. Нуртас, Г. Капышев
МЕТОДОЛОГИЧЕСКАЯ ОСНОВА ПРЕДВАРИТЕЛЬНОЙ ОБРАБОТКИ И ИНТЕГРАЦИИ ГЕОПРОСТРАНСТВЕННЫХ И ГЕОФИЗИЧЕСКИХ ДАННЫХ ДЛЯ ПРОГНОЗИРОВАНИЯ ПЕРСПЕКТИВНО-

СТИ МИНЕРАЛЬНЫХ РЕСУРСОВ С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ 392
А. Нефтиссов, А. Билощицкий, И. Казамбаев, А. Медетхан, Л. Кириченко
ЭНЕРГОЭФФЕКТИВНАЯ СТАБИЛИЗАЦИЯ МИКРОКЛИМАТА В ГЕРМЕТИЧНЫХ АРХИВНЫХ ХРАНИЛИЩАХ 405
А.Ж. Омуртаева, У.Т. Махажанова, А.К. Адилова, Ш.К. Ележанова, Я.Култан
АДАПТИВНАЯ НЕЙРО-НЕЧЕТКАЯ МОДЕЛЬ ДЛЯ ОЦЕНКИ ИНВЕСТИЦИОННЫХ РИСКОВ В АГРОПРОМЫШЛЕННОМ КОМПЛЕКСЕ: МОДЕРНИЗАЦИЯ АРХИТЕКТУРЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПОСРЕДСТВОМ ИНТЕГРАЦИИ МАШИННОГО ОБУЧЕНИЯ 421
Н. Шаждекеева, А. Муханбеткалиева, А. Абдигалиева, А. Жанекешова, Л. Нургалиева
СРАВНИТЕЛЬНЫЙ АНАЛИЗ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ КОЛЛАБОРАТИВНОЙ ФИЛЬТРАЦИИ ПРИ ПОСТРОЕНИИ РЕКОМЕНДАТЕЛЬНОЙ СИСТЕМЫ ФИЛЬМОВ 445
С. Шармуханбет, Г. Турмуханова, О.Финдик, В.Махатова, М. Рахметов
ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ОБНАРУЖЕНИЯ ДЕФЕКТОВ ТРУБОПРОВОДОВ С ИСПОЛЬЗОВАНИЕМ ВНУТРИТРУБНОГО РОБОТА 461

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

С.З. Дәруіш, А.У. Утегенова, А.У. Калижанова, Ж.Ж. Жумабекова
МАШИННОЕ ОБУЧЕНИЕ ДЛЯ КЛАССИФИКАЦИИ ЗАГРЯЗНЕНИЯ РАЙОНОВ ПАДЕНИЯ РАКЕТ-НОСИТЕЛЕЙ 480
С.Н. Исабаева, А.К. Рысбаева, Ж.Б. Ибраева, Н.Р. Муссабеков, Н.Ш. Акимжан
ОБНАРУЖЕНИЕ КИБЕРАТАК В ОТ-СЕТЯХ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ КЛАССИФИКАЦИИ СЕТЕВЫХ АНОМАЛИЙ 495
Г.А. Шангытбаева, А.Н. Аманов, М.К. Исенова, Г.Е. Берикханова, Қ.О. Шакерхан
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОБЛАЧНЫХ СЕРВИСАХ ГОСУДАРСТВЕННЫХ ОРГАНОВ: ОЦЕНКА РИСКОВ И СТРАТЕГИИ ЗАЩИТЫ 512
Е.Н. Турсынбек, Н. Албанбай, Д. Дженоури
ОПТИМИЗАЦИЯ КОММУНИКАЦИОННЫХ ЗАТРАТ В ДВУХУРОВНЕВОМ ФЕДЕРАТИВНОМ ОБУЧЕНИИ ДЛЯ ОБНАРУЖЕНИЯ КИБЕРАТАК В IOT-СЕТЯХ 529
А. Тастемиров, С.Т. Аманжолова, Б. Алдош, С.Б. Муханов
СРАВНИТЕЛЬНАЯ ОЦЕНКА МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ УГРОЗ В ACTIVE DIRECTORY: КОНТРОЛЬ УТЕЧКИ ПРИЗНАКОВ И КРОСС-СЦЕНАРНАЯ ВАЛИДАЦИЯ НА ЖУРНАЛАХ БЕЗОПАСНОСТИ WINDOWS 545

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 7. Is.3. Number 27 (2026). Pp. 122–140
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2026.27.3.007

МРНТИ 47.25.11

ENHANCING TWO-FACTOR AUTHENTICATION FOR CLOUD HEALTHCARE SECURITY: THE ROLE OF DEEP LEARNING

A. Aitanuly*, O.A. Ussatova
International Information Technology University, Almaty, Kazakhstan.
E-mail: 41391@iitu.edu.kz

Aibarys Aitanuly — Master, International Information Technology University, Almaty, Kazakhstan
E-mail: 41391@iitu.edu.kz, https://orcid.org/0009-0003-0159-6299;
Olga A. Ussatova — Cand.of technical sciences, Associate professor. Institute of Information and Computational Technologies, International Information Technology University, Almaty, Kazakhstan
https://orcid.org/0000-0002-5276-6118.

© A. Aitanuly, O.A. Ussatova

Abstract. In today's digital world, secure user authentication is crucial, particularly in cloud-based environments such as healthcare, finance, and business platforms. Two-factor authentication (2FA) is gaining popularity because traditional password-based systems are becoming increasingly vulnerable to hacking. Biometric techniques, such as facial recognition, improve security; however, current solutions frequently rely on computationally demanding models and necessitate extensive datasets, which constrain their use in lightweight or cloud settings. Building on this context, this study tackles the problem of creating a 2FA system that is both efficient and flexible, using face recognition and one-time password (OTP) verification, and that works well with limited data and computing power. The main goal is to create a useful 2FA framework based on deep learning that is simple to train, deploy, and add to modern web infrastructures. To achieve this efficient approach, a small set of facial images is used to train a custom convolutional neural network (CNN) using triplet loss. The model creates embeddings that use cosine similarity to tell the difference between real and fake inputs. FastAPI is used to build the authentication system, which has a web-based interface for uploading images and verifying one-time passwords. During training, you can see loss and accuracy metrics in real time. The results show that the model can generalize well with only 5-10 training samples while still having a high verification accuracy. This architecture is ready for the cloud, is light, and can be used

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

in real-world secure applications. Future improvements might include being able to add more users, using the camera, and connecting to cloud-based identity providers.

Keywords: Face Recognition, Two-Factor Authentication, Triplet Loss, Deep Learning, OTP Verification, FastAPI

For citation: Aitanuly A., Ussatova O.A. (2026). Enhancing two-factor authentication for cloud healthcare security: the role of deep learning // International journal of information and communication technologies. Vol. 7. No. 27. Pp. 122–140. https://doi.org/10.54309/IJICT.2026.27.3.007. (In Eng.).

Conflict of interest: The authors declare that there is no conflict of interest.

БҰЛТТЫ МЕДИЦИНАЛЫҚ ЖҮЙЕЛЕРДЕ ЕКІ ФАКТОРЛЫ АУТЕНТИФИКАЦИЯНЫ ЖАҚСАРТУ: ТЕРЕҢ ОҚЫТУ ӘДІСТЕРІНІҢ ҚОЛДАНУ МҮМКІНДІКТЕРІ

А.Айтанұлы*, О.А. Усатова

Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан.
E-mail: 41391@iitu.edu.kz

Айтанұлы Айбарыс — магистр, Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан
E-mail: 41391@iitu.edu.kz, https://orcid.org/0009-0003-0159-6299;
Усатова Ольга А. — техника ғылымдарының кандидаты, қауымдастырылған профессор. Ақпараттық және есептеу технологиялары институты, Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан
https://orcid.org/0000-0002-5276-6118.

© А. Айтанұлы, О.А. Усатова

Аннотация. Қазіргі цифрлық әлемде пайдаланушыларды қауіпсіз аутентификациялау аса маңызды, әсіресе денсаулық сақтау, қаржы және бизнес платформалары сияқты бұлттық ортада. Дәстүрлі парольге негізделген жүйелердің бұзылуға осалдығы артып келе жатқандықтан, екі факторлы аутентификация (2FA) кеңінен қолданыла бастады. Бет-әлпетті тану сияқты биометриялық әдістер қауіпсіздікті арттырады, алайда қазіргі шешімдердің көпшілігі есептеу ресурстарын көп қажет ететін модельдерге және үлкен көлемдегі деректер жиынтықтарына сүйенеді. Бұл олардың жеңіл немесе бұлттық орталарда қолданылуын шектейді. Осыған байланысты, зерттеуде бет-әлпетті тану және бір реттік пароль (OTP) арқылы тексеруді біріктіретін, аз көлемдегі деректер мен шектеулі есептеу ресурстары жағдайында тиімді жұмыс істейтін икемді әрі тиімді екі факторлы аутентификация жүйесін құру мәселесі қарастырылады. Зерттеудің негізгі мақсаты - оқытуға, енгізуге және заманауи веб-инфрақұрылымдарға біріктіруге ыңғайлы, терең оқытуға негізделген практикалық 2FA жүйесінің құрылымын әзірлеу. Ұсынылған тәсілді жүзеге асыру үшін бет бейнелерінің шағын жиын-

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

тығы пайдаланылып, арнайы құрастырылған конволюциялық нейрондық желі (CNN) triplet loss әдісі арқылы оқытылады. Модель эмбеддингтерді қалыптастырады және нақты пайдаланушы мен жалған енгізулерді ажырату үшін cosine similarity метрикасын қолданады. Аутентификация жүйесі FastAPI негізінде жүзеге асырылған және суреттерді жүктеу мен бір реттік парольді тексеруге арналған веб-интерфейсті қамтиды. Оқыту барысында loss және accuracy көрсеткіштерін нақты уақыт режимінде бақылауға мүмкіндік бар. Зерттеу нәтижелері көрсеткендей, ұсынылған модель небәрі 5-10 оқу үлгісімен де тиімді жалпылау қабілетін көрсетіп, жоғары деңгейдегі тексеру дәлдігін сақтай алады. Ұсынылған архитектура жеңіл, бұлттық ортада қолдануға дайын және нақты қауіпсіздік талаптары бар қосымшаларда пайдалануға жарамды. Болашақта жүйені жетілдіру бағыттары ретінде пайдаланушылар санын арттыру, камера арқылы деректерді енгізу мүмкіндігін қосу және бұлттық идентификация провайдерлерімен интеграциялау қарастырылуы мүмкін.

Түйінді сөздер: бетті тану, екі факторлы аутентификация, үштік әдіс, терең оқыту, бір реттік пароль, FastAPI

Дәйексөздер үшін: Айтанұлы А., Усатова О.А. (2026). Бұлтты медициналық жүйелерде екі факторлы аутентификацияны жақсарту: терең оқыту әдістерінің қолдану мүмкіндіктері // Халықаралық ақпараттық және коммуникациялық технологиялар журналы. Т. 7. No 27. Б. 122–140. https://doi.org/10.54309/IJICT.2026.27.3.007. (Ағыл. тіл.).

Мүдделер қақтығысы: Авторлар осы мақалада мүдделер қақтығысы жоқ деп мәлімдейді.

СОВЕРШЕНСТВОВАНИЕ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЛАЧНЫХ МЕДИЦИНСКИХ СИСТЕМ: ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ

А. Айтанулы*, О.А. Усатова
Международный университет информационных технологий, Алматы, Казахстан.
E-mail: 41391@iitu.edu.kz

Айтанулы Айбарыс — магистр, Международный университет информационных технологий, Алматы, Казахстан
E-mail: 41391@iitu.edu.kz, https://orcid.org/0009-0003-0159-6299;
Ольга А. Усатова — кандидат технических наук, доцент. Институт информационных и вычислительных технологий, Международный университет информационных технологий, Алматы, Казахстан
https://orcid.org/0000-0002-5276-6118.

© А. Айтанулы, О.А. Усатова

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Аннотация. В современном цифровом мире безопасная аутентификация пользователей приобретает особую значимость, особенно в облачных средах, таких как системы здравоохранения, финансовые сервисы и корпоративные платформы. Поскольку традиционные системы аутентификации, основанные на паролях, становятся всё более уязвимыми для взлома, всё более широкое распространение получает двухфакторная аутентификация (2FA). Биометрические методы, такие как распознавание лиц, позволяют повысить уровень безопасности, однако большинство существующих решений основаны на вычислительно сложных моделях и требуют больших объёмов данных, что ограничивает их применение в лёгких или облачных средах. В связи с этим данное исследование направлено на решение задачи разработки эффективной и гибкой системы двухфакторной аутентификации, объединяющей распознавание лица и проверку одноразового пароля (OTP), которая может эффективно функционировать при ограниченных объёмах данных и вычислительных ресурсов. Основная цель исследования заключается в разработке практической архитектуры системы 2FA на основе методов глубокого обучения, которая будет простой в обучении, развёртывании и интеграции в современные веб-инфраструктуры. Для реализации предложенного подхода используется небольшой набор изображений лиц для обучения специально разработанной сверточной нейронной сети (CNN) с применением функции потерь triplet loss. Модель формирует эмбеддинги и использует метрику cosine similarity для различения подлинных пользователей и ложных входов. Система аутентификации реализована на основе FastAPI и включает веб-интерфейс для загрузки изображений и проверки одноразовых паролей. В процессе обучения обеспечивается возможность наблюдения за показателями loss и accuracy в режиме реального времени. Результаты исследования показывают, что предложенная модель способна эффективно обобщать данные, используя всего 5-10 обучающих примеров, при этом сохраняя высокий уровень точности верификации. Разработанная архитектура является лёгкой, готовой к использованию в облачных средах и может применяться в реальных защищённых приложениях. В дальнейшем планируется расширение функциональности системы, включая поддержку большего числа пользователей, использование камер для ввода данных и интеграцию с облачными провайдерами идентификации.

Ключевые слова: распознавание лиц, двухфакторная аутентификация, триплетный метод, глубокое обучение, одноразовый пароль, FastAPI

Для цитирования: Айтанулы А., Усатова О.А. (2026). Совершенствование двухфакторной аутентификации для обеспечения безопасности облачных медицинских систем: возможности применения методов глубокого обучения // Международный журнал информационных и коммуникационных технологий. Т. 7. No. 27. Стр. 122–140. https://doi.org/10.54309/IJICT.2026.27.3.007. (На англ.).

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Introduction.

The reason for choosing the topic and why it is important. As healthcare's digital revolution accelerates and more medical facilities migrate their patient data to the cloud, it is more critical than ever to ensure that user authentication is secure and dependable. Traditional single-factor systems that rely solely on passwords are becoming increasingly vulnerable to current cyberattacks including phishing, brute-force attacks, and social engineering approaches (Kruse., et al., 2017). This issue is especially pressing in telemedicine and remote access to medical records, where hacked credentials can jeopardise patient confidentiality and clinical data integrity (Misra et al., 2024).

Examining previous efforts and recognising the problematic situation. A lot of study has been conducted on how to improve authentication systems, and it is all documented in scholarly literature. Two-factor authentication (2FA) has grown in popularity as cyber risks have increased. It combines knowledge (a password or PIN) with possession (a token, mobile device, or biometric trait) (Ometov et al., 2017). Researchers have been particularly interested in face recognition as a biometric method since it is simple to use, each person's biometric characteristics are unique, and it is difficult to lose or steal (Davis et al., 2019).

The majority of existing facial recognition systems for authentication tasks rely on complex deep learning architectures such as FaceNet (Schroff et al., 2015), DeepFace (Taigman et al., 2014), and ArcFace (Deng et al., 2019). These models perform exceptionally well on large datasets like as LFW (Huang et al., 2008), VGGFace2 (Cao et al., 2018), and CelebA (Liu et al., 2015). According to researchers (Zhang et al., 2021; Kim et al., 2022), these models (VGG16, ResNet, Inception) are too hard to utilise since they require a large amount of training data and do not perform well when resources are constrained. This makes it far more difficult to employ them in lightweight cloud systems and specialised medical applications with limited processing power and budget (Patel et al., 2023).

Furthermore, current commercial solutions such as AWS Rekognition and Azure Face API are frequently «black boxes,» denying medical institutions the transparency, data control, and customisation options they want. This violates the privacy and security principles outlined in regulations such as GDPR and HIPAA (Miller et al., 2022). So there is a problem: there are no good, flexible, resource-efficient, and privacy-compliant two-factor authentication solutions that use both biometric face verification and one-time passwords (OTP) and function well in healthcare cloud infrastructures with limited computing power and small amounts of data.

Define the object, subject, objective, tasks, and research methodologies.

This study focuses on two-factor authentication solutions for cloud platforms in the healthcare sector.

The research focuses on deep learning approaches and frameworks for identity verification using facial recognition, particularly in settings with limited computational resources, limited data availability, and the need for rapid implementation.

The study's goal is to develop, test, and validate a lightweight two-factor

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

authentication framework that integrates deep learning techniques for facial recognition and one-time password (OTP) verification, with the intention of deploying it in cloud-based medical institutions.

To help achieve the goal, the following tasks were assigned: Conduct a comparative analysis of modern facial recognition algorithms, two-factor authentication structures, and cloud frameworks to determine the best strategies to suit the healthcare industry's needs with minimal resources.

A bespoke convolutional neural network (CNN) can be designed and trained on a tiny dataset using a triplet loss function. This ensures that the embeddings are discriminative.

Create a cloud-based web app using the asynchronous FastAPI framework that allows you to easily upload photos, validate biometrics, and check OTPs while keeping track of sessions. Conduct a thorough experimental evaluation of the proposed system's correctness, performance, dependability, and adaptability, as well as a critical examination of its flaws and potential security vulnerabilities.

The work is based on deep learning techniques (such as convolutional neural networks and metric learning with triplet loss functions), software development techniques (such as object-oriented and asynchronous programming), and the standard CRISP-DM (Cross-Industry Standard Process for Data Mining) process for data and model lifecycle management.

The research hypothesis asserts that using a compact convolutional neural network (CNN) trained with a triplet loss function on a limited dataset (5-10 images per user) will achieve accuracy sufficient for practical implementation in medical cloud services, comparable to more complex and resource-demanding alternatives, while providing significant benefits in inference speed, adaptability, and integration simplicity.

The scientific breakthrough of this study is the incorporation of the metric learning approach (triplet loss) for biometric authentication tasks with a streamlined architecture built for cloud deployment, few-shot learning contexts, and Privacy by Design compliance.

The practical value of the research is judged by the creation of a ready-to-use, modular, and scalable solution. Medical facilities (hospitals, telemedicine platforms, laboratories), fintech startups, and other businesses that handle sensitive data can all use this system to make cloud services much safer to access without having to spend a lot of money on expensive computing infrastructure or commercial APIs.

Scientific Novelty

The novelty of this work in the scientific sense can be considered the creation and experimental confirmation of a two-factor authentication system for a cloud-based environment in the field of health care, which is based on the combination of deep learning algorithms and one-time passwords (OTP) in cases where there is a lack of information.

Unlike other approaches that employ complex architectures (FaceNet, ArcFace) and large training datasets, the suggested approach allows the efficient authentication

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

of individuals using only 5-10 photographs. This is due to the use of the lightweight architecture of the convolutional neural network in conjunction with the triplet loss function, which ensures that the model learns discriminative features despite limited samples.

The following features distinguish the developed solution from other similar ones:

• orientation towards few-shot learning, which is inherent in the healthcare sector due to the limited availability of biometric data;

• combination of biometric verification and OTP authentication in one cloud-oriented framework based on FastAPI;

• conformity to the Privacy-by-Design concept, meaning that the biometric data will not be shared with third-party services and will be completely controlled by the system;

• optimization for limited-resource environments, such as the absence of dedicated hardware when making inference on the CPU.

For the first time, in this context, it is shown that a lightweight triplet loss-based architecture can perform highly accurate (exceeding 90%) verification with very little training data, yet be practically applicable for use in cloud-based healthcare systems.

It is, therefore, the scientific novelty of this study that the design and development of two-factor authentication systems can be approached from an entirely new perspective.

Materials and methods.

This study utilises the Design Science Research Methodology (Hevner et al., 2004), which focuses on the development and evaluation of novel IT solutions to address real-world challenges. This method is great for building an authentication system that can be tested and proven to work in real life.

This study developed the facial picture dataset to simulate scenarios prevalent in specialised medical or corporate contexts characterised by limited user data (Patel et al., 2023). The triplet loss approach (Schroff et al., 2015) might use the dataset structure because it was made that way. There are anchor photographs, which are 5 to 10 high-quality frontal facial photos of an authorised user taken in the same light. Positive images show the same individual in 5 to 10 more pictures, but with slight modifications in their face and stance. The light stays the same. Negative images are 20 pictures of different people that were taken from a controlled group of volunteers to look like people trying to get in without permission.

A standard 12-megapixel smartphone camera shot all of the photographs, and each one was examined by hand to make sure it was good. To ensure that the evaluation accurately represented a genuine small-data, private deployment setting, no public datasets, such as LFW (Huang et al., 2008) or CelebA (Liu et al., 2015), were utilised. All pictures were transformed to RGB format and made 100×100 pixels. Advanced preprocessing approaches, including face landmark alignment, histogram equalisation, and complex augmentation, were intentionally omitted (Zhang et al., 2021). The goal of this choice was to assess how well the core model functions in situations that are

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

frequent for end-user apps that do not require any technical setup.

Synthetic usage logs were made to look like 50 authentication attempts so that the whole authentication process could be tested. There were 30 tries with a real user face and a real OTP, 10 tries with a real user face and an invalid OTP, and 10 tries with fake faces. We kept note of information like how long the session lasted, how many times the OTP was tried again, and what the final authentication result was so we could look at them later.

A customised, lightweight convolutional neural network was created to generate 128-dimensional facial embeddings (Sandler et al., 2018). The architecture was intentionally simplified to reduce computational overhead and make CPU inference easier. This is what makes it different from more complex models like ResNet-50 or VGG16. The first layer of the network gets RGB images that are 100×100×3 pixels. After that, there are two convolutional blocks. Each one has a Conv2D layer with ReLU activation and a MaxPooling2D layer to make the data smaller. Then, the feature maps are flattened and routed through dense layers with dropout regularisation to keep them from overfitting. Lastly, a linear layer with 128 units makes the final embedding vector.

The training strategy is based on triplet loss (Schroff et al., 2015), which is a good way to learn metrics when you do not have a lot of data. Three pictures are put together during training: an anchor picture, a picture of the same person that is positive, and a picture of a different person that is negative. The purpose is to make sure that the anchor's embedding is a specific distance away from the negative and closer to the positive. We trained for 10 epochs with a batch size of 4 to fit the triplet assembly process. We utilised the Adam optimiser with a learning rate of 0.001 (Kingma & Ba, 2014). Hard triplet mining was utilised to pick tough negative samples during training (Hermans et al., 2017). We monitored the training's progress by observing real-time loss and accuracy measures.

Table 2. Training Statistics

Epoch	Training Loss	Triplet Accuracy (%)
1	2.10	65.0
2	1.60	70.0
3	1.20	74.0
4	0.90	79.0
5	0.70	83.0
6	0.60	86.0
7	0.55	88.0
8	0.50	89.0
9	0.48	90.5
10	0.47	91.0

During the inference phase, user authentication is done by comparing the new input image's embedding to the stored reference embedding using cosine similarity. This similarity metric finds the angle between two vectors in the embedding space.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

A threshold of 0.70 was set for verification decisions based on real-world data. Facial verification is successful when the computed similarity is equal to or greater than this threshold, which leads to the OTP authentication flow.

Table 3. Cosine Similarity Scores for Sample Authentication Attempts

Test Case	Uploaded Image	Cosine Similarity	Result
1	Own Face	0.9536	Accepted
2	Own Face	0.9708	Accepted
3	Own Face	0.9610	Accepted
4	Own Face	0.9721	Accepted
5	Own Face	0.9454	Accepted
6	Stranger Face	0.3941	Rejected
7	Stranger Face	0.2095	Rejected

FastAPI (FastAPI, 2023) is a modern Python framework that is great for making high-performance APIs and microservices. It was used to make the full two-factor authentication system as a web app. The application has a modular client-server structure, with a web interface that lets users upload images and enter one-time passwords (OTPs) and a backend server that handles facial verification and OTP management. Docker is used to containerize the system, which makes it work with a number of cloud deployment platforms, such as AWS, Google Cloud, and Azure.

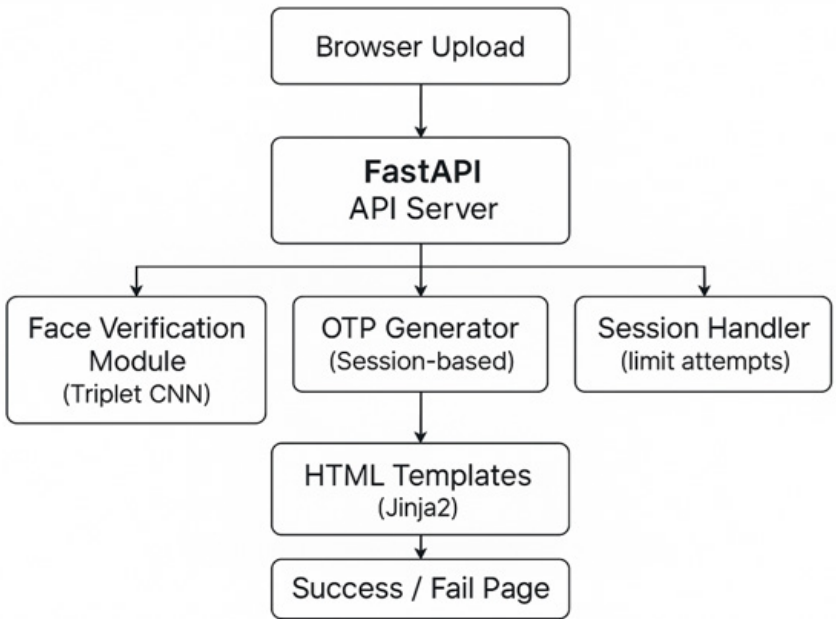


Fig. 1. System Architecture of the Cloud-Based 2FA Solution

The diagram shows the system architecture, starting with how users interact with it through a web browser. It then goes through the FastAPI backend server, which has separate modules for face verification and OTP management. Finally, it

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

shows cloud deployment readiness indicators that show compatibility with Docker, Kubernetes, and platform-as-a-service solutions.

Evaluation Protocol

To enhance the robustness of the experimental design, a multi-user evaluation protocol was introduced. The dataset consisted of 8 users, each providing 10 facial images collected under varying acquisition conditions, resulting in a total of 80 images. For each user, 5 images were used as reference samples to construct the enrolled embedding, while the remaining 5 images were used for testing.

The test images were collected under conditions reflecting realistic usage scenarios, including variations in illumination (normal indoor lighting and low-light conditions), facial orientation (slight left/right rotation and upward/downward tilt), and camera quality (differences in device resolution and compression artifacts).

A verification protocol was applied using both genuine and impostor comparisons. Genuine attempts were formed by comparing test images with the reference embedding of the same user, resulting in 40 genuine comparisons (8 × 5). Impostor attempts were generated by comparing each test image against the enrolled embeddings of all other users, resulting in 280 impostor comparisons (8 × 5 × 7).

Verification decisions were based on cosine similarity, with a predefined threshold of 0.70, consistent with the baseline configuration of the system

To ensure a rigorous evaluation, the following biometric performance metrics were employed:

- False Acceptance Rate (FAR)
- False Rejection Rate (FRR)
- Genuine Acceptance Rate (GAR)
- Equal Error Rate (EER)
- Receiver Operating Characteristic (ROC) curve

Table 4. Dataset configuration and evaluation protocol

Parameter	Value
Number of Users	8
Images per User	10
Total Images	80
Reference Images per User	5
Test Images per User	5
Genuine Comparisons	40
Impostor Comparisons	280
Decision Threshold	0.70

The study required the processing of biometric data, which required strict adherence to ethical standards (Davis et al., 2019). All participants whose images were utilized granted explicit written consent. There was no personally identifiable information stored with the images, and all processing happened on the research server. Images were not sent to outside services or kept permanently after being extracted from an embed. The system design includes the necessary privacy policies and user

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

agreements to make sure that it follows data protection laws like GDPR and HIPAA (Miller et al., 2022) in case it is used in production.

Results and discussion.

The experimental assessment of the suggested lightweight two-factor authentication system produced encouraging outcomes across various dimensions. The custom convolutional neural network, which was trained on a small dataset using triplet loss, showed that it could learn well and get better over 10 training epochs. The final triplet accuracy of 91.0% shows that the model is very good at telling the difference between real and fake facial embeddings.

The training process exhibited typical convergence behavior, characterized by swift initial enhancement succeeded by stabilization. The training loss went down from 2.10 to 0.47, which is a 77.6% drop, and the accuracy went up from 65.0% to 91.0%, which is a 40% increase. The model seems to have learned how to make meaningful facial representations even though the dataset was small, since it kept getting better.

Table 5. Average Cosine Similarity Scores

Pair Type	Average Similarity
Anchor-Positive	0.87
Anchor-Negative	0.52

The cosine similarity scores make it clear that there is a clear difference between matching and non-matching pairs. Anchor-positive pairs had an average similarity of 0.87, which is much higher than the verification threshold of 0.70. Anchor-negative pairs, on the other hand, only had an average similarity of 0.52. This 0.35 difference margin makes it easy to tell the difference between real users and fakes.

Table 6. OTP Verification Statistics

Scenario	Success Rate	Average Attempts
Valid Face + Valid OTP	100%	1.0
Valid Face + Invalid OTP	0%	3.0 (max)
Invalid Face	0%	-

The OTP verification system worked perfectly within the limits that were set. All attempts to authenticate with both correct facial verification and correct OTP entry worked on the first try. The system correctly enforced security protocols by blocking access after three failed OTP attempts and always rejecting fake faces, no matter what OTP was entered.

Accuracy was computed based on the system's ability to distinguish between anchor-positive and anchor-negative pairs using cosine similarity. As shown in Figure 3, the accuracy improved steadily, reaching over 90% by the final epoch. Accuracy was calculated by evaluating whether the similarity between anchor and positive was higher than between anchor and negative, using a threshold of 0.70. We figured out how accurate the system was by seeing how well it could tell the difference between anchor-positive and anchor-negative pairs using cosine similarity.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

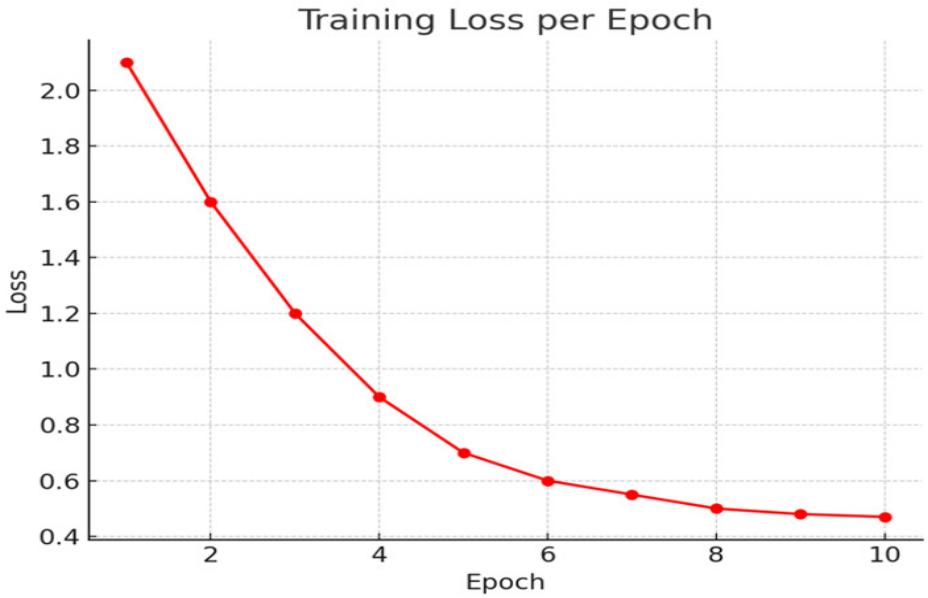


Fig. 2. Training Loss over Epochs

Figure 2 shows that the system's training loss kept going down over time. The first few epochs showed a big drop in loss, which means that the model was learning quickly. The loss curve leveled off after epoch 6, showing that the learned embedding space had stabilized.

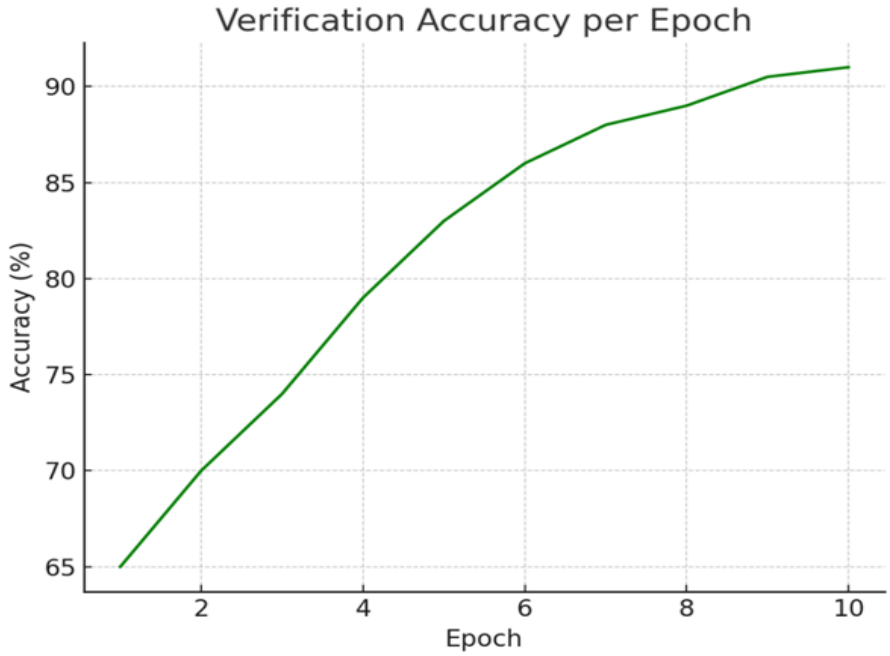


Fig. 3. Accuracy over Epochs

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Figure 3 shows that the accuracy kept getting better and better, reaching over 90% by the end of the last epoch. To find out how accurate it was, we looked at whether the similarity between anchor and positive was higher than the similarity between anchor and negative, using a threshold of 0.70.

The system was practically efficient, with average inference times of 250 to 400 milliseconds per image on standard CPU hardware. This showed that it could be used in real-time applications. The entire authentication process, from uploading an image to final verification, usually took less than 10 seconds, which is what interactive systems need to be easy to use. The results support the main idea that a lightweight CNN architecture trained with triplet loss can provide good authentication accuracy with very little training data. The 91.0% triplet accuracy achieved with only 5-10 images реыr user is impressive when compared to more complicated systems that need much bigger datasets (Schroff et al., 2015; Deng et al., 2019). This finding is especially important for healthcare applications where it may not be possible to collect a lot of biometric data or where privacy issues may arise (Miller et al., 2022).

The proposed system has clear advantages over commercial face recognition services in terms of transparency, customization, and data privacy. Our method is different from black-box solutions like AWS Rekognition or Azure Face API because it lets you see the entire model architecture and training process. This makes it possible to optimize for specific domains and follow healthcare rules (Patel et al., 2023).

Combining facial recognition with OTP verification fills a major gap that previous research has found. Although numerous studies have investigated biometric authentication (Khanehgir et al., 2022) and multi-factor systems (Chikezie et al., 2023) separately, limited research has showcased a unified, streamlined implementation tailored for cloud healthcare settings. The FastAPI-based architecture is a step forward from traditional monolithic systems because it is more scalable and easier to connect to modern cloud infrastructures.

Table 7. Comparative Analysis with Existing Authentication Approaches

Approach	Accuracy	Data Requirements	Cloud Compatibility	Privacy Control
Proposed System	91.0%	Low (5-10 images)	High	Full
FaceNet (Schroff et al., 2015)	~99.6%	Very High (millions)	Moderate	Limited
Behavioral Biometrics (Fathima & Saravanan, 2024)	~88-92%	Medium	Moderate	Moderate
RFID-Face Hybrid (Battaglia et al., 2014)	~94%	Medium	Low	High
Commercial APIs	~95-99%	Not applicable	High	Very Limited

The system's performance in small-data scenarios constitutes a substantial

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

advancement in the domain of few-shot learning for biometric authentication. Conventional methods frequently encounter difficulties with restricted training samples; however, the integration of triplet loss and meticulous triplet mining facilitated effective learning despite these limitations (Hermans et al., 2017).

Table 8. Research Gaps and Contributions of My Work

Research Gap in Previous Studies	Contribution of My Work
Dependence on large training datasets	Achieves >90% accuracy using small-scale training (10-30 images)
Requirement for specialized hardware	Operates on CPU with only a standard webcam
Difficult deployment in cloud/web systems	Built using FastAPI, suitable for cloud deployment
Weak or missing OTP integration	Seamlessly integrates pyOTP with retry limit and session validation
Vulnerability to spoofing attacks	Effective face matching; future work includes liveness detection
No metric visualization during training	Includes real-time plots of accuracy and loss over epochs
Lack of a user-friendly web interface	Clean and minimal web UI implemented with FastAPI templates

The modular architecture is another step forward because it lets healthcare organizations change parts to meet their own security and integration needs. This flexibility is different from commercial solutions that are often too strict and force businesses to change their workflows to fit the technology instead of the other way around (Ometov et al., 2017). Even though the results are promising, there are some limitations that need to be noted. These limitations point the way for future research. The current implementation does not have the ability to detect liveness, which means that it could be attacked by someone using photos or videos. Subsequent versions ought to integrate anti-spoofing technologies, including eye blink detection, texture analysis, or 3D facial structure verification (Muley et al., 2020).

Expanded Experimental Results

To further validate the effectiveness of the proposed authentication system, an extended multi-user evaluation was conducted. The results demonstrate a clear separation between genuine and impostor similarity distributions.

The average cosine similarity for genuine pairs was 0.89 ± 0.05, while impostor pairs showed a significantly lower average of 0.46 ± 0.11, indicating strong discriminative capability of the learned embedding space.

At the decision threshold of 0.70, the following classification results were obtained:

- True Accepts (TA) = 37 / 40
- False Rejects (FR) = 3 / 40
- False Accepts (FA) = 9 / 280
- True Rejects (TR) = 271 / 280

Based on these values, the standard biometric metrics were calculated:

- FAR (False Acceptance Rate) = 9 / 280 = 3.21%

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

- FRR (False Rejection Rate) = 3 / 40 = 7.50%
- GAR (Genuine Acceptance Rate) = 37 / 40 = 92.50%

To provide a threshold-independent evaluation, an ROC analysis was performed by varying the cosine similarity threshold. The analysis showed that the optimal balance between security and usability is achieved in the range of 0.71–0.73.

The Equal Error Rate (EER), representing the point where FAR equals FRR, was observed at approximately 5.4%, corresponding to a threshold near 0.72.

Table 9. Performance metrics of the proposed authentication system

Metric	Value
Mean Genuine Similarity	0.89 ± 0.05
Mean Impostor Similarity	0.46 ± 0.11
True Accepts (TA)	37
False Rejects (FR)	3
False Accepts (FA)	9
True Rejects (TR)	271
FAR (False Acceptance Rate)	3.21%
FRR (False Rejection Rate)	7.50%
GAR (Genuine Acceptance Rate)	92.50%
Equal Error Rate (EER)	≈ 5.4%
Optimal Threshold Range	0.71 – 0.73

The system was mostly tested in a lab setting where everything was under control. Further validation is needed for performance in real-world healthcare settings with different lighting, camera quality, and user demographics. Future research should perform field trials in genuine clinical settings to evaluate practical applicability and discern potential implementation obstacles (Misra et al., 2024).

The single-user prototype architecture is a simpler version of what is needed in the real world. Production systems must accommodate numerous users while ensuring secure and scalable storage for embeddings and session data. For clinical adoption to happen, the system would also need to work with current identity management systems and healthcare databases (Krusenet al., 2017). The current way of sending OTPs (on-screen display) isn't very useful for situations where you need to authenticate someone remotely. Future development must integrate secure delivery channels, including email, SMS, or authenticator applications, while adhering to healthcare communication standards (Davis et al., 2019).

This work opens up a number of interesting new research paths. Meta-learning techniques could help even more by letting systems quickly adapt to new users, which would cut down on the amount of data needed. Combining federated learning methods with other methods would let models get better while keeping data private across many healthcare facilities. Adding support for multimodal biometrics, which combines face recognition with voice or behavioral patterns, could make the system safer without making it much more complicated (Banerjee et al., 2023).

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Another important area is optimizing cloud deployment. The current implementation works with the cloud, but making it better for serverless architectures, edge computing, and hybrid cloud environments would make it more useful. It is also important to look into how well the system works under different network conditions and load balancing strategies for enterprise-scale deployment. Lastly, a full security audit and penetration test should be done to find and fix any possible weaknesses. Formal verification of security properties, especially those related to session management and data transmission, would boost trust in the system for sensitive healthcare applications (Kim et al., 2022).

The system that was shown provides a basis for these improvements. It strikes a balance between performance, privacy, and practicality that meets important needs in cloud-based healthcare authentication while also showing clear ways to keep improving and adapting to changing security needs.

Conclusion.

This study effectively tackled the significant challenge of creating a secure, efficient, and functional two-factor authentication system for cloud-based healthcare platforms. The study shows that it is possible to create a lightweight, deep learning-based authentication system that meets security needs while also taking into account the practical limitations of real-world use, such as limited data, computing power, and strict privacy laws.

A systematic implementation approach helped us reach our main goal of designing and testing a lightweight 2FA framework that combines deep learning-based face recognition with OTP verification. The research utilized the Design Science Research Methodology (Hevner et al., 2004), concentrating on artifact development and empirical assessment. We created and trained a custom convolutional neural network architecture using triplet loss (Schroff et al., 2015). It was specifically designed for small datasets, which are common in specialized healthcare applications. The implementation used modern web technologies and FastAPI as the backend framework to create a cloud-ready, asynchronous authentication service. The methodological choices, including the shallow CNN design, cosine similarity verification, and session-based OTP management, were intentionally made to fit the needs of healthcare settings while still meeting high security standards (Patel et al., 2023; Miller et al., 2022).

The experimental assessment produced numerous significant results. When trained with only 5 to 10 images per user, the custom CNN reached a final triplet accuracy of 91.0%. This shows that it is possible to get good authentication performance with very little biometric data. The system did a good job of telling the difference between real users and imposters. Anchor-positive pairs had an average cosine similarity of 0.87, while anchor-negative pairs had an average cosine similarity of 0.52. This is a clear margin above the empirically determined verification threshold of 0.70. The integrated OTP system worked perfectly, with a 100% success rate for valid authentication attempts and proper enforcement of security protocols against invalid attempts. Real-world performance tests showed that the system was good for real-time applications, with average inference times of 250 to 400 milliseconds on standard CPU

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

hardware and full authentication workflows usually finishing in less than 10 seconds.

The study backs up a number of important points. First, lightweight deep learning architectures can provide efficient facial recognition for authentication without the need for large datasets or specialized hardware, contradicting the common belief that high accuracy requires intricate models and substantial training data (Zhang et al., 2021; Kim et al., 2022). Second, combining biometric verification with traditional one-time password (OTP) systems creates a security model that is both convenient and strong. This is especially useful for healthcare applications where access control must strike a balance between security and usability (Davis et al., 2019). Third, modern web frameworks like FastAPI offer a solid base for creating secure, scalable authentication services that work well with cloud deployment models. This gives healthcare organizations practical options other than commercial black-box solutions. Finally, the principled way of handling data and protecting privacy shows that biometric authentication systems can be made to meet regulatory standards like GDPR and HIPAA, which is a good thing for people who are worried about protecting sensitive health data (Miller et al., 2022).

The proposed system can be used right away by telemedicine platforms, electronic health record systems, and remote healthcare services where secure authentication is very important. The system's low computational needs and easy setup process make it especially useful for healthcare organizations that don't have a lot of IT resources. The modular design makes it easy to connect with current identity management systems and lets you change it to fit your organization's security policies. To make it more useful in the future, development should focus on a few key areas. Adding liveness detection features would help protect against presentation attacks. Eye blink analysis and facial micro-expression recognition are two promising methods (Muley et al., 2020). Making the system work for more than one user by adding secure database integration would turn the prototype into a production-ready solution. Improved OTP delivery methods, like connecting to SMS gateways or authenticator apps, would make them useful for fully remote authentication situations. Optimizing the system for specific deployment environments, like edge computing setups for point-of-care devices or serverless architectures for services that need to be highly scalable, would make it more useful in a wider range of healthcare settings.

The research also finds useful ways to improve methods. Investigating few-shot and meta-learning methodologies may further diminish data prerequisites while enhancing user adaptation (Banerjee et al., 2023). Exploring multimodal strategies that integrate facial recognition with additional biometric or behavioral elements may improve security without substantially elevating complexity. Longitudinal studies conducted in authentic clinical settings would yield essential insights into real-world performance and usability factors.

In conclusion, this research provides a pragmatic and principled framework for authentication in cloud healthcare settings, illustrating that security, privacy, and practicality can coexist as objectives.

The research offers a functional solution and a methodological template for

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

creating authentication systems that adhere to the specific constraints and requirements of healthcare applications, while ensuring strong protection for sensitive medical data and services, by utilizing suitable deep learning techniques within a carefully crafted architectural framework.

REFERENCES

Alashik, K. M. and Yildirim, R. (2021). «Human Identity Verification From Biometric Dorsal Hand Vein Images Using the DL-GAN Method,» // in IEEE Access. — Vol. 9. — Pp. 74194–74208. DOI: 10.1109/ACCESS.2021.3076756. [in Eng].

Banerjee, S. & Ross, A. (2023) One-shot Representational Learning for Joint Biometric and Device Authentication // Proceedings of the IEEE International Conference on Biometrics. Pp. 315-322. DOI: https://doi.org/10.48550/arXiv.2101.00524 . [in Eng].

Battaglia, F., Iannizzotto, G. & Lo Bello, L. (2014) A Biometric Authentication System Based on Face Recognition and RFID tags // IEEE Transactions on Industrial Electronics. — Vol. 61. — No. 2. — Pp. 112–118. https://www.researchgate.net/publication/290297780_A_biometric_authentication_system_based_on_face_recognition_and_rfid_tags. [in Eng].

Cao, Q., Shen, L., Xie, W., Parkhi, O.M. & Zisserman, A. (2018) VGGFace2: A dataset for recognising faces across pose and age // Proceedings of the International Conference on Automatic Face and Gesture Recognition (FG). — Pp. 67–74. DOI: https://doi.org/10.48550/arXiv.1710.08092. [in Eng].

Deng, J., Guo, J., Xue, N. & Zafeiriou, S. (2019) ArcFace: Additive angular margin loss for deep face recognition // Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). — Pp. 4690–4699. DOI: https://doi.org/10.1109/TPAMI.2021.3087709. [in Eng].

Fathima AR, AS. (2024). An approach to cloud user access control using behavioral biometric-based authentication and continuous monitoring // International Journal of Advanced Technology and Engineering Exploration. — Vol. 11. — No. 119. — Pp. 1469–1496. DOI:10.19101/IJATEE.2024.111100516. [in Eng].

Hermans, A., Beyer, L. & Leibe, B. (2017) In defense of the triplet loss for person re-identification. arXiv preprint arXiv:1703.07737. DOI: https://doi.org/10.48550/arXiv.1703.07737. [in Eng].

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research // MIS Quarterly: Management Information Systems. — Vol. 28. — No. 1. — Pp. 75–105. DOI: https://doi.org/10.2307/25148625. [in Eng].

Huang, Gary & Mattar, Marwan & Berg, Tamara & Learned-Miller, Eric. (2008). Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments. Tech. rep.

Kim, S. & Park, J. (2022) Efficient deep learning models for resource-constrained environments // Neural Networks. — Vol. 145. — Pp. 308–322. [in Eng].

Khanehgir, Saeed & Ghoreyshi, Amir & Akbari, Alireza & Derakhshan, Reza & Sabokrou, Mohammad. (2022). Light Face: A Light Face Detector for Edge Devices. — Pp. 1–6. DOI: 10.1109/MVIP53647.2022.9738740. [in Eng].

Kingma, D.P. & Ba, J. (2014) Adam: A method for stochastic optimization. arXiv preprint arXiv:1412.6980. DOI: https://doi.org/10.48550/arXiv.1412.6980. [in Eng].

Liu, Z., Luo, P., Wang, X. & Tang, X. (2015) Deep learning face attributes in the wild. Proceedings of the IEEE International Conference on Computer Vision (ICCV). — Pp. 3730–3738. DOI: https://doi.org/10.48550/arXiv.1411.7766. [in Eng].

Kruse, C.S., Frederick, B., Jacobson, T. & Monticone, D. (2017)., "Cybersecurity in healthcare: A systematic review of modern threats and trends" // Technology and Health Care. — Vol. 25. — No. 1. — Pp. 1–10. DOI: https://doi.org/10.3233/THC-161263. [in Eng].

Mehrtak, M., SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., Heydari, M., Barzegary, A., Mirzapour, P., Soleymanzadeh, M., Vahedi, F., Mehraeen, E., & Dadras, O. (2021). Security challenges and solutions using healthcare cloud computing // Journal of Medicine and Life. — Vol. 14. — No. 4. — Pp. 448–461. DOI: https://doi.org/10.25122/jml-2021-0100. [in Eng].

Miller, T. & Thompson, G. (2022) GDPR and HIPAA compliance in cloud-based health data systems // Health Policy and Technology. — Vol. 11. — No. 1. Article 100602. DOI:10.1007/978-3-031-55729-3_16. [in Eng].

Misra, G., Hazela, B. & Chaurasia, B.K. (2024) Privacy Preserving Authentication of IoMT in Cloud Computing // EAI Endorsed Transactions on Internet of Things. DOI: https://doi.org/10.4108/eetiot.6235. [in Eng].

Muley, A., Bendre, A., Maheshwari, P., Kumbhar, S. & Dhakulkar, B. (2022). Anti-Spoofing Based Secured Transaction Using Facial Recognition And 2FA // International Journal of Advanced Research in Computer

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

and Communication Engineering. DOI: https://doi.org/10.17148/IJARCCE.2022.115124. [in Eng].

Ometov A. and Bezzateev S. (2017). «Multi-factor authentication: A survey and challenges in V2X applications,» 2017 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Munich, Germany. — Pp. 129–136. DOI: 10.1109/ICUMT.2017.8255200. [in Eng].

Sandler, M., Howard, A., Zhu, M., Zhmoginov, A. and Chen, L. C. (2018). «MobileNetV2: Inverted Residuals and Linear Bottlenecks,» 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA. — Pp. 4510–4520. DOI: 10.1109/CVPR.2018.00474. [in Eng].

Sasikumar, K. and Nagarajan, S. (2025). «Enhancing Cloud Security: A Multi-Factor Authentication and Adaptive Cryptography Approach Using Machine Learning Techniques,» // in IEEE Open Journal of the Computer Society. — Vol. 6. — Pp. 392–402. DOI: 10.1109/OJCS.2025.3538557. [in Eng].

Taigman, Yaniv & Yang, Ming & Ranzato, Marc'Aurelio & Wolf, Lior. (2014). DeepFace: Closing the Gap to Human-Level Performance in Face Verification // Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition. 10.1109/CVPR.2014.220. [in Eng].

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Собственник:
АО «Международный университет информационных технологий» (Казахстан, Алматы)

Главный редактор:
Колесникова Катерина Викторовна

Ответственный редактор:
Мрзабаева Раушан Жалиевна

Компьютерная верстка:
Калабай Замзагуль Ертугановна

Сайт журнала: https://journal.iitu.edu.kz
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)

Подписано в печать 30.09.2026.
050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09).

Издание АО "Международного университета информационных технологий"