



ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ



**Матеріали
Міжнародної наукової конференції**

**Івано-Франківськ
20-23 травня 2025 року**

Міністерство освіти і науки України
Прикарпатський національний університет ім. В. Стефаника
Представництво "Польська Академія Наук" в Києві
Вінницький національний технічний університет
Інститут прикладних проблем механіки і математики
ім. Я.С. Підстригача. НАН України
AGH науково-технологічний університет
ім. Ст.Сташіца, Польща
Інститут кібернетики ім. В.М.Глушкова НАН України
Харківський національний університет радіоелектроніки
Національний авіаційний університет
Національний університет «Львівська політехніка»
Фінансово-економічний інститут Таджикистану
Економічна академія "Д.А.Ценов", Болгарія
Штуттгартський університет, Німеччина
НДІ інтелектуальних комп'ютерних систем THEU та ІК НАН України
Інститут інженерів з електротехніки
та електроніки (IEEE), Українська секція
Громадська організація "Івано-Франківський ІТ кластер"

"ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ"

**матеріали
міжнародної науково-практичної конференції**

**20-23 травня 2025 року
Івано-Франківськ**

**"INFORMATION TECHNOLOGIES AND COMPUTER MODELLING"
proceedings
of the International Scientific Conference
2025, May, 20th to 23th
Ivano-Frankivsk**

Івано-Франківськ — 2025

УДК (004:004.2/004.9+007):33/37+51+621
ББК 22.17 32.81
І-74 Т

Науковий редактор: докт. техн. наук, проф. **Л.Б. Петришин** (ПНУ, AGH)

Матеріали статей опубліковані в авторській редакції

"Інформаційні технології та комп'ютерне моделювання"; матеріали статей Міжнародної науково-практичної конференції, м. Івано-Франківськ, 20-23 травня 2025 року. – Івано-Франківськ: п. Голіней О.М., 2025. –267с.

Збірка містить матеріали статей Міжнародної науково-практичної конференції з проблем інформаційних технологій в технічних системах, в соціумі, освіті, медицині, економіці та екології; теорії інформації, кодування та перетворення форми інформації; технологій цифрової обробки інформації; захисту інформації в інформаційно-телекомунікаційних системах; математичного та імітаційного моделювання систем.

УДК (004:004.2/004.9+007):33/37+51+621
ББК 22.17 32.81
І-74 Т

ISBN 978-617-8470-31-9

© ПНУ ім. В. Стефаника та автори, 2025

Зміст

1. Програмна система для аналізу медичних томографічних зображень із використанням SVM.....	3
Катерина Горішня, Ілля Головашенко, Володимир Кобзєв	
2. Розпізнавання військової техніки на супутникових знімках за допомогою ШІ.....	5
Віталій Витрикуш, Наталія Гузинець	
3. Архітектура та дизайн безсерверної системи для збору спеціалізованих даних.....	10
Олександр Демідов, Оксана Гонсьор	
4. База даних, як частина автоматизованої системи управління земельними ресурсами.....	12
Дрозд Василь, Мічута Ольга	
5. Оптимізація продуктивності корпоративних мереж за допомогою SD-WAN технологій.....	15
Жуков Роман, Юрченко Юрій,	
6. Analysis of war-related landscape fires around the Bucha-Irpin-Hostomel agglomeration using satellite monitoring data.....	17
Tetiana Ivanova, Ruslana Pashko, Rostyslav Bun	
7. CNN-ViT Hybrid Framework for Histopathological Breast Cancer Analysis.....	19
Oleksandr Papchenko, Borys Kuzikov	
8. Spatial Assessment of Thermal Anomalies in Ukraine Using Intelligent Data Analysis Methods.....	22
Svitlana Kuznichenko, Dmytro Ivanov	
9. Fractality Formation of Self-Organized Structures and their Initiation in the Education.....	26
Mykhaylo Mar'yan, Nataliya Yurkovych, Vladimir Seben	
10. Appreciative Inquiry (AI) method in the study of sustainable development of education quality improvement.....	29
Iryna Melnyk, Kateryna Kotsiubivska	
11. Development of a Chatbot for End-to-End Encrypted Messaging.....	32
Volodymyr Palahin, Olena Palahina, Oleksandr Protsenko, Oleksandr Ivchenko, Anatolii Bairak	
12. Модель оцінки ефективності електронного навчального процесу на основі психофізіологічних показників.....	35
Лебеза Андрій Васильович, Повхан Ігор Федорович, Сароз Віталій Ярославович	
Яковлев Владислав Олександрович	
13. Spatial analysis of consequences of war-related landscape fires in the Kharkiv region using satellite image processing methods and a cloud platform.....	41
Dmytro Pohorilets, Alina Puto, Yuliia Ivato, Rostyslav Bun	
14. Електронні навігаційні карти для безпеки судоходства.....	44
Наталія Пунченко	
15. Порівняльний аналіз оптимізації системи контрольних допусків при розпізнаванні інфраструктурних об'єктів.....	46
Максим Руденко, Микита Мироненко	
16. Метод агрегування експертних оцінок функціонального стану персоналу.....	50
Володимир Темніков, Андрій Темніков	
17. Підхід до моделювання проблемної області інтелектуальної навчальної системи.....	52
Олена Темнікова, Андрій Темніков	
18. Концепція програмного забезпечення цифрового кластера безпеки.....	54
Антон Турок	
19. Програмна система вивчення англійської мови з використанням штучного інтелекту для аналізу та навчання.....	56
Євдоким Федорчук, Мирослав Труняк	
20. Method of improving an interference-resistant for radiosystem with FHSS and dynamic channel state analysis.....	58
Dmytro Tsybulnykov, Shostko Igor	
21. Formalization of Deductive Rules for Syntactic-Semantic Transformations in a System for Ontology Construction from Textual Documents.....	61
Andrii Chorny, Dmytro Dosyn	
22. Modernization of the Video Surveillance System Network Using Software-Defined Networking and Network Function Virtualization Technologies.....	68
Oleksandr Shloma, Stanislav Korobka	

23. Investigation of the Remote Control Method of Autonomous Video Surveillance Dahua Cameras from the SpaceX Satellite Networks.....	71
Oleksandr Shloma, Stanislav Korobka	
24. Моделювання Методу Усереднення Несинхронних Сигналів на Прикладі ЕКГ.....	74
Леонід Файнзільберг, Ольга Сапон	
25. Розпаралелювання стиску зображень зі сканерів земної поверхні.....	79
Тарас Грицько, Валерій Глухов	
26. Комп'ютерна технологія захищеної передачі текстових повідомлень на основі процесів спотворення та відновлення зображень.....	82
Анастасія Маріненко, Сергій Вовк	
27. Wavelet Filtering of Colored Noise in an Image.....	87
Olena Osharovska, Andrii Doroshuk	
28. Одночасна апроксимація серіями типу вибірки у зважених просторах функцій.....	89
Метін Тургай	
29. Моделювання Каскадного Фільтру Приглушення Зосереджених Гармонічних Завад на Основі ДПФ.....	95
Леонід Файнзільберг, Владислав Самборський	
30. Modeling of a Cascade Filter for Suppression of Harmonic Interference Based on DFT.....	95
Leonid Fainzilberg, Vladislav Samborskyi	
31. Штучний інтелект та використання його можливостей для смарт-аналітики.....	98
Людмила Колечкіна, Софія Середа, Анна Мещерякова	
32. Апроксимація залежності опору термістора від температури.....	105
Роман Малахівський	
33. Портфелі алгоритмів для розв'язання задачі про найкоротше покриття множини.....	107
Сергієнко Іван, Шило Володимир, Рошин Валентина, Шило Петро, Боярчук Дмитро	
34. Automatic Grayscale Images Contrast Enhancement Based on Power Transformations.....	109
Lyudmila Akmetshina, Artyom Yegorov, Olexandra Nikishyna	
35. Три Моделі Створення Стереозображень За Сенсорними Даними БПЛА.....	112
Віталій Боюн, Людмила Возненко, Аніса Касім, Олександр Матвієнко	
36. Порівняльний аналіз NLP-бібліотек NLTK та spaCy.....	116
Дадиверін Віталій, Бісікало Олег	
37. Advancements in Agent-Based Modeling for Enhanced Transportation Network Simulation: Methodological Innovations and Practical Applications.....	119
Bohdan Dokhniak, Viktor Khavalko	
38. Особливості розрахунку спотворень сигналу в електронних системах.....	122
Ігор Заячук, Богдан Благітко	
39. Наївний метод на основі правил в аналізі емоційного забарвлення контенту українською мовою.....	125
Антон Ломовацький, Тарас Басюк	
40. Comparison of Entity Framework Core File Export Strategies Under Parallel Processing.....	127
Yaroslav Luchenko, Volodymyr Kobziev	
41. Апаратна оптимізація генеративних змагальних мереж: аналіз продуктивності та енергоефективності.....	129
Микола Максимів	
42. Вдосконалення методів моніторингу додатків в мікросервісній архітектурі.....	133
Олексій Мельник	
43. Underwater Images Preprocessing Techniques.....	136
Dmytro Moroz	
44. Climate Models and Temperature Forecast for Odesa.....	138
Yurii Illytskyi, Volodymyr Moroz	
45. Концептуальні підходи до адаптивного синтезу моделей для задач інтелектуального моніторингу.....	143
Володимир Остапук, Сергій Голуб	
46. The Method of Context-Aware Data Management in Customer Relationship Management Systems.....	145
Marian Pisotskyi	
47. Невизначеність в задачах штучного інтелекту та її вирішення самоналагоджувальними алгоритмами.....	147
Тимофієва Н.К.	

48.Розробка Архітектури Глибокого Навчання для Класифікації Дефектів Дорожнього Покриття.....	149
Є.С. Чернов, С.Ю.Борю	
49.Заземлене розуміння мови ШІ-моделями через втілену взаємодію та моделі світу.....	153
Олексій Шамов	
50.Predictive Maintenance for Agricultural Vehicles: Impact of GIS Data on LSTM-Based RUL Prediction.....	155
Anton Shykhmat, Zenoviy Veres	
51.Порівняння ефективності інструкцій для мовних моделей у контексті генерації зображень за допомогою GAN моделей.....	157
Володимир Якимів, Йосиф Піскозуб	
52.Практика аналізу витрат і вигравів кібербезпеки.....	160
Василь Горбачук, Максим Дунаєвський	
53.Методи Захисту Від Атак На Біометричні Системи Аутентифікації.....	162
Єлизавета Єжова	
54.Соціальна інженерія як частина тестування на проникнення.....	165
Анастасія Журавчак, Андріян Піскозуб	
55.Security Models for IoT Systems.....	168
Oleksiy Kovalenko, Natalia Karevina	
56.Comparative Analysis of Curves Performance of ElGamal Algorithm.....	170
Yurii Baryshev, Vladyslava Lanova	
57.Applying an intelligent disinformation search algorithm to a dataset of Ukrainian-language news.....	172
Olga Lozynska, Oksana Markiv, Victoria Vysotska	
58.Елементи Великого Порядку в Групових Кільцях, Заданих Скінченням Полем та Діедальною Групою. .	175
Роксолана Оберишин, Роман Попович	
59.Інтелектуальна система прогнозування внутрішніх інцидентів на основі даних SOCMINT: практична реалізація.....	177
Вадим Пантелєєв, Володимир Білодід	
60.Інтегрований підхід до прогнозування внутрішніх інцидентів на основі аналізу соціальних мереж та емоційно-часових характеристик.....	180
Вадим Пантелєєв, Володимир Білодід	
61.Масштабованість та продуктивність розподілених баз даних з використанням фрагментації даних у блокчейн-мережах.....	183
Петро Петрів, Іван Опірський	
62.Інтеграція LLM у технологію автоматизованого тестування безпеки веб-застосунків.....	188
Андрій Притула, Леонід Куперштейн	
63.Застосування моделі ShieldGemma для аналізу відео з мобільних пристроїв з метою виявлення потенційно небезпечних осіб.....	192
Тарас Фединашин, Партика Ольга	
64.Реалізація апаратних та програмних рішень для дослідження надійності роботи мікропроцесорних засобів в складі АСУ ТП комунальної сфери.....	195
Олександр Гедзь, Ольга Скрипнікова	
65.Інтерактивна карта індексів безпеки країн світу: розробка та моделювання.....	198
Олександр Палагін, Денис Симонов, Аніса Касім, Масуд Касім	
66.Підходи до побудови комп'ютерної системи розпізнавання запахів.....	201
Северин Рибка, Максим Попов, Severyn Rybka, Maksym Popov	
67.Застосування псевдообернених матриць для розв'язання задач теплопровідності.....	204
Білоус Максим, Варенюк Наталія, Тукалевська Нелля	
68.Genetic programming tool involving fractional-order operators.....	208
Vsevolod Bohaienko	
69.Spatial modeling of carbon dioxide fugitive emissions from coke production in Ukraine.....	210
Yuliia Ivato, Dmytro Pohorilets, Alina Puto, Rostyslav Bun	
70.Minimax Rational Approximations for the Hyperbolic Tangent Activation Function.....	212
Larysa Vakal, Yevhen Vakal	
71.Відновлення функції концентрації домішкових частинок за дискретними даними в області тіла.....	214
Богдан Гера	

72. Thermoelastic damping in a piezoelectric microbeam resonators with microstructure.....	216
Olha Hrytsyna, Maryan Hrytsyna	
73. Erroneous Parallel Gateways Detection in BPMN Models using Fuzzy Logic-based Techniques.....	218
Andrii Kopp, Dmytro Kudii	
74. Дослідження екстремальних експлуатаційних характеристик підземних сховищ газу в складі газотранспортної системи.....	220
Мирослав Притула, Зоя Притула, Назар Притула, Ольга Химко	
75. Greenhouse gas emissions from railway transport in Ukraine: Spatial modeling for 2015-2022.....	224
Alina Puto, Yuliia Ivato, Dmytro Pohorilets, Rostyslav Bun	
76. Homogenization and Modeling of Processes in Composite Materials with a Layered Structure.....	227
Gennadiy Sandrakov	
77. Про підхід до аналізу кібер-фізичних атак на розумні мережі на основі бі-матричних ігор.....	229
Володимир Г. Скобелев, Сергій В. Компан	
78. Mathematical Modeling and Optimization of Rooftop Solar Panel Placement in Urban Environments Using Genetic Algorithms.....	233
Petro Topylko, Artur Dankanych	
79. Taguchi's optimization of surface eddy current probes with rectangular orthogonal coils.....	237
Volodymyr Halchenko, Ruslana Trembovetska, Volodymyr Tychkov	
80. Математичне моделювання дифузії домішки у трифазному стохастично неоднорідному тілі із застосуванням діаграм Фейнмана.....	240
Юрій Чернуха	
81. Ймовірно-статистичний підхід до моделювання масоперенесення у випадково неоднорідному тілі за експериментальних даних на границі.....	242
Ольга Чернуха, Галина Білушак, Юрій Білушак, Анастасія Чучвара	
82. Approximation by Hermite-type exponential sampling series in logarithmic weighted spaces of functions.....	245
Sadettin Kursun	
83. Метод блокового шифрування на основі перетворень Уолша.....	249
Володимир Лужецький, Євгеній Кесарчук	
84. Математична Модель Фільтрації Газу з Використанням Похідних Дробових порядків.....	252
Ярослав П'янило, Назар Лопух, Ганна Лянце, Галина П'янило	
85. Похідні Дробових порядків в Математичному Моделюванні.....	256
Ярослав П'янило, Назар Лопух, Ганна Лянце, Галина П'янило	

Наукове видання

**"ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ
ТА
КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ"**

матеріали

**Міжнародної науково-практичної конференції
20-23 травня 2025 року
Івано-Франківськ**

**"INFORMATION TECHNOLOGIES
AND
COMPUTER MODELLING"**

**proceedings
of the International Scientific Conference
2025, May, 20st to 23th
Ivano-Frankivsk**

Науковий редактор: Л.Б. Петришин
Технічний редактор: М.О. Федоряк
Коректор: Ю.Ю. Іляш
Комп'ютерна верстка: О.М. Голіней

Прикарпатський національний університет
імені Василя Стефаника
76018, Івано-Франківськ, вул. Шевченка, 57,
ПНУ, адміністративний корпус

ISBN 978-617-8470-31-9

Для нотаток

Для нотаток

Development of a Chatbot for End-to-End Encrypted Messaging

Volodymyr Palahin, Olena Palahina

Department of Robotic and Telecommunication Systems
and Cybersecurity
Cherkasy State Technological University
Cherkasy, Ukraine
v.palahin@chdtu.edu.ua

Oleksandr Ivchenko

Department of Robotic and Telecommunication Systems
and Cybersecurity
Cherkasy State Technological University
Cherkasy, Ukraine
o.ivchenko@chdtu.edu.ua

Oleksandr Protsenko

Department of Robotic and Telecommunication Systems
and Cybersecurity
Cherkasy State Technological University
Cherkasy, Ukraine
o.protsenko@chdtu.edu.ua

Anatolii Bairak

Department of Robotic and Telecommunication Systems
and Cybersecurity
Cherkasy State Technological University
Cherkasy, Ukraine
a.bairak@chdtu.edu.ua

Розробка Чат Бота Для Обміну Повідомленнями Методом Наскрізного Шифрування

Володимир Палагін, Олена Палагіна

Кафедра робототехнічних і телекомунікаційних систем
та кібербезпеки
Черкаський державний технологічний університет
Черкаси, Україна
v.palahin@chdtu.edu.ua

Олександр Івченко

Кафедра робототехнічних і телекомунікаційних систем
та кібербезпеки
Черкаський державний технологічний університет
Черкаси, Україна
o.ivchenko@chdtu.edu.ua

Олександр Проценко

Кафедра робототехнічних і телекомунікаційних систем
та кібербезпеки
Черкаський державний технологічний університет
Черкаси, Україна
o.protsenko@chdtu.edu.ua

Анатолій Байрак

Кафедра робототехнічних і телекомунікаційних систем
та кібербезпеки
Черкаський державний технологічний університет
Черкаси, Україна
a.bairak@chdtu.edu.ua

Abstract — This paper describes the development of a chatbot that implements end-to-end encryption to ensure message confidentiality. Technologies such as React, Firebase, Elliptic Curve Cryptography (ECC), and CryptoJS contribute to the creation of a secure environment for information exchange. The study highlights the architectural and technical foundations of the chatbot, detailing encryption protocols and data flows to maintain interaction privacy. Through the examination of real-time data processing and user authentication strategies, the chatbot demonstrates an advanced approach to information protection, making it a reliable solution for privacy-sensitive applications

Анотація — В роботі описано процес розробки чат-бота, який реалізує наскрізне шифрування для забезпечення конфіденційності повідомлень. Використані технології, такі як React, Firebase, криптографія еліптичних кривих (ECC) та CryptoJS, сприяють створенню безпечного середовища для обміну інформацією. Дослідження висвітлює архітектурні та технічні основи чат-бота, детально описуючи протоколи шифрування і потоки даних для збереження конфіденційності взаємодій. Завдяки розгляду обробки даних у режимі реального часу та стратегій аутентифікації користувачів, чат-бот демонструє передовий підхід до захисту інформації, що робить його надійним рішенням для додатків, чутливих до конфіденційності

Ключові слова—чат-бот, наскрізне шифрування, React, Firebase, ECC, CryptoJS, інформаційна безпека

Keywords— chatbot, end-to-end encryption, React, Firebase, ECC, CryptoJS, information security

I. INTRODUCTION

In today's world, where information security is increasingly vital, end-to-end encrypted chatbots offer an effective solution for safeguarding data privacy. The development of digital communications has increased the need for reliable encryption methods that prevent unauthorized access to confidential information. This paper examines the implementation of a chatbot that uses end-to-end encryption and the technologies supporting this process. By integrating recognized cryptographic protocols and modern frameworks, the chatbot provides a secure data-sharing platform that addresses common vulnerabilities in online communications. [1], [2].

The chatbot's architecture includes a multi-layered approach to security, starting from user authentication and proceeding to encrypted message exchange. A key component is the use of Elliptic Curve Cryptography (ECC), which provides robust encryption with efficient performance, especially for devices with limited computing power [3]. ECC's low computational cost combined with a high level of security makes it ideal for this application, strengthening the chatbot's ability to maintain a secure communication channel without compromising speed. This research aims to show how a systematic approach to data flow security and encryption design can contribute to advancing the field of information security, addressing common challenges in digital privacy.

II. METHODOLOGY

To develop a reliable and secure end-to-end encrypted chatbot, we focused on integrating ECC and AES encryption in the React and Firebase environments. The study tests ECC's performance and security in real-time data processing, considering factors such as encryption speed and compatibility with Firebase's database structure. The methodology includes testing the efficiency of key generation, storage, and retrieval processes to ensure chat data protection.

By analyzing the flow of messages through encrypted channels and observing the React-based interface's responsiveness, the study assesses the system's ability to meet real-time encryption requirements. Additionally, Firebase's real-time data synchronization capabilities are tested to ensure consistent and secure message delivery across different devices. The following technologies were used in the work:

React - serves as the foundation for creating the user interface, simplifying the creation of a dynamic and interactive user experience. React's component architecture enables efficient state management and event handling, making it a popular choice among developers for building scalable applications. Its modular structure also simplifies debugging and maintenance, providing a seamless user experience;

Firebase - as a real-time database solution, Firebase ensures fast data storage and retrieval, essential for chat applications where message updates must be instant.

Firebase's built-in security features allow real-time data synchronization between different clients, ensuring secure storage and message transmission;

Elliptic Curve Cryptography (ECC) - The ECC algorithm provides a high level of data protection by generating a key pair for each user. The small size of ECC keys ensures a high level of security without significant resource consumption, making it suitable for real-time applications where speed is crucial;

CryptoJS - for message encryption and decryption, the CryptoJS library implements the AES algorithm, which is a widely accepted standard for information protection. AES provides reliable encryption with manageable key sizes, making it compatible with various devices.

Bot Architecture. User Authentication: The authentication process starts with verifying user data stored in the Firebase database. This step ensures that only authorized users have access to the chatbot. Upon successful login, users gain access to the encrypted messaging system. Authentication plays a critical role in maintaining a secure environment, preventing unauthorized access to the chat.

Key Generation and Storage: Users' encryption keys are stored in Firebase in encrypted form, allowing the bot to perform encryption and decryption directly on the user's device. Each user receives a unique private key, ensuring secure message encryption that can only be decrypted by the recipient.

Message Encryption: Before sending, the bot generates a shared secret key based on the ECC keys of the sender and receiver. This key is then used with the AES algorithm to encrypt the message, securing data during transmission. The message remains encrypted until it reaches the recipient, protecting it from interception.

Message Decryption: Upon receiving a message, the bot uses the shared secret to decrypt it, allowing the recipient to view the original text. This decryption process ensures that only the intended user can see the message content, preserving communication privacy.

III. RESULTS AND DISCUSSION

The proposed chatbot architecture successfully provides end-to-end encryption for message transmission. The dynamic React interface enables the handling of encrypted messages, and Firebase database integration ensures fast and reliable data access. The compact size of ECC keys provides strong encryption without significantly reducing performance, proving its feasibility for real-time applications.

During testing, the bot demonstrates robust encryption and decryption processes, with minimal data transmission delays, meeting the requirements of a fast chat interface. AES-based encryption further ensures that messages remain protected, and the integration of the CryptoJS library simplifies encryption, enabling secure communication even on mobile devices.

Moreover, the bot's architecture shows resilience against common security threats, such as man-in-the-middle attacks, as messages remain encrypted during transmission. This

resilience is critical for environments where message privacy is a priority.

IV. CONCLUSIONS

Developing an end-to-end encrypted chatbot illustrates the application of modern technologies to ensure information security. Through the use of React, Firebase, ECC, and CryptoJS, the chatbot emerges as a reliable tool for secure message exchange. Lightweight and efficient ECC-based encryption enhances protection while preserving performance, making it ideal for real-time communication. This research demonstrates the potential for integrating powerful cryptographic methods into a user-friendly interface, promoting secure digital interactions.

Future research may focus on expanding the chatbot with multi-factor authentication, such as biometric verification, which will further enhance security by combining various user identification factors. Integrating additional security layers will significantly improve protection against unauthorized access and reinforce the role of end-to-end encryption in information security.

REFERENCES

- [1] Yang, J., Chen, Y.-L., Por, L.Y., & Ku, C.S. (2023). A Systematic Literature Review of Information Security in Chatbots. *Applied Sciences*, 13(11), 6355
- [2] Kalyan Kumar, D., Shaguftha, M., Sujinth, P.V., Praveen Kumar, M.N., & Karthikeya, N. (2024). Implementing a Chatbot with End-To-End Encryption for Secure and Private Conversations. *International Journal for Modern Trends in Science and Technology*, 10(2), 130-136.
- [3] Hankerson, D., Menezes, A.J., Vanstone, S.: *Guide to Elliptic Curve Cryptography*. Springer, New York (2004). <https://doi.org/10.1007/b97644>.