



# ICORIS2022

The 4<sup>th</sup> International Conference on  
Cybernetics and Intelligent System

Kampus  
Merdeka

## UNIVERSITAS POTENSI UTAMA



2022 4th International Conference on Cybernetics and Intelligent System (ICORIS) | 978-1-6654-5395-0/22/\$31.00 ©2022 IEEE | DOI: 10.1109/ICORIS56080.2022.10031444

# 04<sup>th</sup> ICORIS INTERNATIONAL CONFERENCE

**Conference ON**  
**08-09** OCTOBER  
**2022**  
VENUE: HOTEL KHAS PARAPAT, LAKE TOBA  
NORTH SUMATERA - INDONESIA

**HOST**



**CO-HOST**



**SUPPORTED BY**



# **2022 Fourth International Conference on Cybernetics and Intelligent Systems (ICORIS)**

Medan, Indonesia

(Hybrid Conference)

October 08<sup>th</sup>-09<sup>th</sup>, 2022

**Part Number: CFP22BWC-ART**  
**ISBN: 978-1-6654-5395-0**

# 2022 Fourth International Conference on Cybernetics and Intelligent Systems (ICORIS)

Medan, Indonesia (Virtual)

Phone: +6281263411368

Email: [icoris2022@potensi-utama.ac.id](mailto:icoris2022@potensi-utama.ac.id)

Website: <http://icoris.org/>

October 08<sup>th</sup>-09<sup>th</sup>, 2022

**Part Number: CFP22BWC-ART**  
**ISBN: 978-1-6654-5395-0**

# 2022 Fourth International Conference on Cybernetics and Intelligent Systems (ICORIS)

Copyright ©2022 by the Institute of Electrical and Electronics Engineers, Inc. All rights reserved.

## **Copyright and Reprint Permission**

Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law, for private use of patrons, those articles in this volume that carry a code at the bottom of the first page, provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

Other copying, reprint, or reproduction requests should be addressed to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331.

ISBN: 978-1-6654-5395-0

Additional copies of this publication are available from

Curran Associates, Inc.

57 Morehouse Lane

Red Hook, NY 12571 USA

+1 845 758 0400

+1 845 758 2633 (FAX)

# PREFACE

Assalaamu ‘alaykum warahmatullahi wabarakaatuh,



After three successful sessions of ICORIS's conference, we are proud to present the fourth edition of ICORIS. We believe that ICORIS 2022 is an excellent and exceptional opportunity which enables researchers to present and discuss the latest innovations, results and developments in their research topics. This years' theme is "Build a trusted infrastructure system with blockchain technologies for society 5.0". The conference is expected to strengthen collaboration and provide a forum for academicians, professionals and researchers to discuss and exchange their research results, innovative ideas, and experiences to advance the field of Information Technology, Information Systems and Electronic Engineering in the modern world. The event will incorporate extensive discussions and consist of additional workshops, guest speaker sessions, and scintillating social events that will help our future leaders develop networks and transform their ideas into actions.

The ICORIS 2022 is in the general area of communication and information technology. It provides a forum for presenting and discussing the latest innovations, results, and developments in IT Management & organizations, IT Applications, Cyber & IT Security, and ICT. We present several tracks that are separated into nine thematic areas, each ICORIS 2022 track is a carefully curated selection of sessions and activities focused on an important current or emerging issue. There is 282 papers submission and only 106 papers are accepted to be presented in this Conference. The accepted papers will be presented in one of the regular sessions and will be published in the conference proceedings volume. All accepted papers are submitted to IEEEExplore. IEEE Conference Number: #56380.

On behalf of the ICORIS 2022 committee, we wish to extend our warm welcome and would like to thank all Keynote Speakers, Reviewers, Authors, and Committees, for their effort, guidance, contribution and valuable support.

Wa billahi taufiq wal hidaayah.

Wallahul muwaffiq ila aqwamit-tharieq.

Wasalaamu ‘alaykum warahmatullahi wabarakaatuh.

Husni Teja Sukmana, Ph.D

# THE COMMITTEE OF ICORIS 2022

## STEERING COMMITTEE

1. Dr. Y. Johny W. Soetikno, SE.,MM. ( Universitas Dipa Makassar, Indonesia)
2. Marthen Sengkey, PhD (Universitas Klabat)
3. Dr. Dadang Hermawan (ITB STIKOM Bali)
4. Dr. Ir. Djoko Soetarno, D.E.A (Binus University)
5. Prof. Dr. M. Suyanto, MM. (AMIKOM Yogyakarta)
6. Prof. Dr. Ir. Harjanto Prabowo, M.M. (Rektor Universitas Bina Nusantara)
7. Prof. Dr. Ir. Edi Noersasongko, M.Kom (Universitas Dian Nuswantoro Semarang)
8. Dr. Sandy Kosasi, MM., M.Kom. (STMIK Pontianak)
9. Dr. Rika Rosnelly, S.Kom., M.Kom. (Universitas Potensi Utama)
10. Restu Adi wiyono, M.Sc., M.Kom. (STMIK Tasikmalaya)
11. Dr. Po Abas Sunarya, M.Si. (STMIK Raharja)
12. Dr Berlilana , M.Kom ( Univ Amikom Purwokerto, Indonesia)
13. Dr Anthony Anggrawan, M.T., PhD ( Univ Bumigora Mataram, Indonesia)
14. Mus Aidah, S.Pd., MM. (STMIK Adhi Guna Palu)
15. Djuniharto, S.Kom., M.Kom( stmik PGRI, banyuwangi, Indonesia)
16. Dr. Hj. Rosiyati Mh Thamrin, SE., MM. (STMIK Sepuluh Nopember Jayapura)
17. M Hari Purwiantoro, S.Kom., M.Kom( STMIK AMIKOM Surakarta, Indonesia)
18. Muchammad Naseer, M.Kom (STT Bandung, Indonesia)
19. Benedictus Effendy, ST., MT ( STMIK Palcomtec Palembang, Indonesia)
20. Dr. Hadi Santoso, S.Kom., M.Kom.( Institut Sains dan Bisnis ATMALUHUR, Indonesia)
21. Suardi B Haruna, S.Si.,M.Si (STMIK PROFESIONAL, Makasar, Indonesia)
22. Bob Subhan Riza, S.T, M.Kom ( Universitas Potensi Utama, Medan, Indonesia)

## PROGRAM COMMITTEE

1. Prof. Riyanarto Sarno, Ph.D. (Institut Teknologi Sepuluh Nopember (ITS)), Indonesia
2. Prof. Pitoyo Hartono (Chukyo University, Toyota), Japan
3. Prof. Harold Boley (Faculty of Computer Science, University of New Brunswick, NB), Canada
4. Prof. Eko Sedyono, PhD (Universitas Satya Wacana, Indonesia)
5. Prof. Agus Buono ( IPB University, Indonesia)
6. Prof. Joko Lianto Buliali, Msc, Phd ( Institut Teknologi Sepuluh Nopember(ITS)), Indonesia
7. Prof. Ir. Arif Djunaidy M.Sc., Ph.D. (Institut Teknologi Sepuluh Nopember (ITS)), Indonesia
8. Prof. Dr.rer.nat. Achmad Benny Mutiara, Q.N, Ssi, Skom ( Universitas Gunadarma), Indonesia

9. Prof. Sri Hartati, M.Sc., Ph.D. (IndoCEIS/UGM)
10. Prof. Dr. Muhammad Zarlis (Universitas Sumatera Utara), Indonesia.
11. Prof. Dr Eri Prasetyo Wibowo, SSI, MMSI ( Universitas Gunadarma), Indonesia
12. Rafał Dreżewski, Ph.D. (AGH University of Science and Technology), Poland
13. Assoc. Prof. Huynh Thi Thanh Binh (Hanoi University of Science and Technology (HUST)), Viet Nam
14. Prof. Dr. Mustafa Bin Mat Deris (Universiti Tun Hussein Onn Malaysia (UTHM)), Malaysia
15. Assoc. Prof. Somnuk Phon-Amnuaisuk (Universiti Teknologi Brunei), Brunei Darussalam
16. Amil Ahmad Ilham, ST.,MIT, PhD( Universitas Hasanuddin), Indonesia
17. Daniel Oranova, S.Kom., M.Sc.PD.Eng. (Institut Teknologi Sepuluh Nopember (ITS)), Indonesia
18. Arief Setyanto, S.Si., M.T., Ph.D. (AMIKOM Yogyakarta), Indonesia
19. Dr. Ir. Untung Rahardja, M.T.I.,MM. ( Universitas Raharja), Indonesia
20. Andrew Tanny Liem, PhD (Universitas Klabat), Indonesia
21. Husni Teja Sukmana, PhD (Universitas Islam Negeri Syarif Hidayatullah), Indonesia
22. Dr Evi Triandini ( ITB Stikom Bali, Indonesia)
23. Dr Kusrini ( Univ Amikom Yogyakarta, Indonesia)

## Technical Program Committee (TPC)

Chair : Husni Teja Sukmana, Ph.D (UIN Syarif Hidayatullah Jakarta, Indonesia)

C0-Chair : Prof. Dr. Teddy Surya Gunawan (Universitas Potensi Utama, Indonesia)

## Organizing Committee

1. Program Chair : Husni Teja Sukmana, PhD. (IEEE Member : 93016632)
2. Co Program Chair : Helmi Kurniawan, M.Kom
3. Publication Chair : Prof. Dr. Teddy Surya Gunawan (IEEE Member : 8286407700 )
4. Secretary : Ratih Puspasari, M.kom
5. Treasurer : Linda Wahyuni M.Kom

## Editing Team

Husni Teja Sukmana, Ph.D

Edy Victor Haryanto, M.Kom

M. Sadikin, M.Kom

Fujiati, M.Kom

Alfa Saleh, M.Kom

Khairani Puspita, M.Kom

# TABLE CONTENT

FRONT MATTER	ii-iv
PREFACE	v
COMMITTEES	vi-vii
TABLE OF CONTENT	viii-xxi

1	Id_Paper_2 The Evaluation Model Of The Travel Application As The Impact Of The Covid-19 Pandemic And Its Adaptation Simulation Wahyu sardjono, Astari Retnowardhani,	1 - 5
2	Id_Paper_4 Banyan: Generating Micro, Small, And Mediumenterprises Through Augmented Reality Regina Carmelita Kristofani, Yudhistya Ayu Kusumawati, Mardhatillah Shanti	6 - 12
3	Id_Paper_9 Workev: Development And Evaluation Of A Web Based Electronic Human Resource Management Using Delphi Method Niccosan , Ray Tommy, Christian Kurniawan, Brilly Andro Makalew	13 - 18
4	Id_Paper_13 Systematic Literature Review On Machine Learning Predictive Models For Indoor Climate In Smart Solar Dryer Dome Karli Eka Setiawan, Gregorius Natanael Elwirehardja ,Bens Pardamean	19 - 25
5	Id_Paper_20 Web Development Of Direct-To-Consumer Genetics Testing Kians Azizatikarna, Deby Erina Parung, Dian Amirullah, Alam Ahmad Hidayat, Tjeng Wawan Cenggoro, Arif Budiarto, Simon, Bens Pardamean	26 - 31
6	Id_Paper_21 Digitizing Farmers' Land Data Collection Systems In Indonesia With The Use Of Tani Millenial Apps Mohammad Prasanto Bimantio, Dian Pratama Putra, Teddy Suparyanto, Amallia Ferhat, Nanda Satya Nugraha, Alam Ahmad Hidayat, Bens Pardamean	32 - 36



	Id_Paper_22	
7	<b>A Diversity Inventory Monitoring System Of Riparian Vegetation</b> Dian Pratama Putra, Nanda Satya Nugraha, Teddy Suparyanto, Alam Ahmad Hidayat, Digdo Sudigyo, Bens Pardamean	37 - 42
	Id_Paper_26	
8	<b>Systematic Literature Review: Machine Learning Prediction Model For Covid-19 Spreading</b> Faulinda Ely Nastiti, Shahrulniza Musa, Eiad Yafi, Ritu Chauhan	43 - 47
	Id_Paper_30	
9	<b>The Technology Behind Genomic Database</b> Joko Pebrianto Trinugroho, Anzaludin Samsinga Perbangsa, Bens Pardamean	48 - 53
	Id_Paper_32	
10	<b>Web-Based Application For Searching The Event Organizers With Provided Audiences By Using Recommender System Method</b> Budi Yulianto, Rita Layona, Yovita Tunardi	54 - 58
	Id_Paper_38	
11	<b>Generalization Of Public Key Cryptosystem Based On Singular Matrix Using Ring Of Integer Modulo</b> Maxrizal Maxrizal, Baiq Desy Aniska Prayanti, Sujono Sujono	59 - 62
	Id_Paper_44	
12	<b>Air Quality Monitor In Hospital Based On Fog And Cloud Computing</b> Candra Ahmadi, Juan Constantine, Desti Syuhada, Nisya Kintan Qumari	63 - 65
	Id_Paper_46	
13	<b>Elevating Thematic Branding Through Social Media Content: A Visual Concept Of Kayutangan Heritage'S Instagram Feed</b> Ivana Rosaline Tejakusuma, Yudhistya Ayu Kusumawati, Anindya Widita, Faishal Hilmy Maulida, Fransiscus Asisi Agung Dwi Prasetyo Prasetyo	66 - 71
	Id_Paper_52	
14	<b>Automated Essay Scoring Using Machine Learning</b> Jason Sebastian Kusuma, Kevin Halim, Edgard Jonathan Putra Pranoto, Bayu Kanigoro , Edy Irwansyah	72 - 76
	Id_Paper_57	

15	Application Of Design Thinking In The Creation Of Ui/Ux On E-Learning Websites Eko Setyo Purwanto, Elena Bianca Jap, Eugene Salim Wijaya, Ryan Juwanda , Azani Cempaka Sari	77 - 82
16	Id_Paper_58 New Student Prediction Using Algorithm Naive Bayes And Regression Analysis In Potensi Utama University Elsa Aditya, Zakarias Situmorang, B. Herawan Hayadi, Muhammad Zarlis, Wanayumini Wanayumini	83 - 88
17	Id_Paper_62 The Influence Of Consumer Interest On The Use Of Ui And Ux In The E-Commerce Application Abraham Aditya Sudjatmoko, Alfonsius Adrian Susanto, Jeremy Andrew Jayaseputra, Eko Setyo Purwanto, Azani Cempaka Sari	89 - 96
18	Id_Paper_67 Netdet: Concept Of Integrating Basic Computer Network Learning Into Game Mechanics Febrianta Surya Nugraha, Ciske Mulyadi, Lilik Sugiarto, Nurhidayanto Nurhidayanto	97 - 102
19	Id_Paper_68 Design And Development Of Web And Unity3D WebGL Based Immersive Virtual Exhibition Application Sinjiru Setyawan, Cuk Tho	103 - 108
20	Id_Paper_69 Augmented Reality Design Using The Addie Model As An Introduction To Kindergarten Interior Interactive Elements Anneke Anggala, Teresa Teresa, Yovinne Hendro Cipta, Fairuz Iqbal Maulana, Ida Bagus Ananta Wijaya.	109 - 113
21	Id_Paper_70 Fadcovnet: Fast Automatic Detection Covid-19 Based On Inception-Resnet-V2 Model Tinuk Agustin, Siti Rihastuti, Moch. Hari Purwidianoro, Afnan Rosyidi	114 - 122
22	Id_Paper_72 Region Grouping Based On Sales Results Using K-Means Algorithm At Pt Rmk Fathur Muhammad Haekal, Indrajani Sutedja	123 - 128

	Id_Paper_78	
23	Object Detection On Bottles Using The Yolo Algorithm Fathi Sei Pahangai Akbar, Steven Yanuar Prasetyo Ginting, Giovanna Cheryl Wu, Said Achmad, Rhio Sutoyo	129 - 133
	Id_Paper_81	
24	Using Strategy Video Games To Improve Problem Solving And Communication Skills: A Systematic Literature Review Alvin Lie, Anthony Stephen, Louis Ricardo Supit, Said Achmad, Rhio Sutoyo.	134 - 138
	Id_Paper_85	
25	Using Image Upscaling Methods In Digital Platforms To Reduce Internet Usage Willy Lau, Josia Sean Audric Santoso, Ignatius Ronald,Eko Setyo Purwanto, Azani Cempaka Sari	139 - 144
	Id_Paper_88	
26	Factors Influencing The Intention To Use Peduli Lindungi Application Among Indonesians During Covid-19 Ibnu Darmawan, Assed Lussak	145 - 152
	Id_Paper_89	
27	Investigating Cloud-Based Educational Technology Adoption In Advancing Learning Performance Michael Siek, Ivana Wijaya	1543- 160
	Id_Paper_93	
28	Ui/Ux Design Of E-Wallet Appllication Using Design Thinking Approach As'Ad Syafrizal Addany, Nanda Ihsan Pradana, Satria Perdana Putra Prabowo,Ina Sholihah Widiati	161 - 165
	Id_Paper_94	
29	Impact Of Robots, Artificial Intelligence, Service Automation (Raisa) Acceptance, Self-Efficacy, And Relationship Quality On Job Performance Nurul Sukma Lestari, Dendy Rosman, Syafrizal Chan, Lenny Christina Nawangsari, Hana Desy Natalina, Freddy Triono	166 - 171
	Id_Paper_98	
30	Smartphone-Based Virtual Reality Systems (Sbvrs) As A Promotion Tools For Foodservice Industry Dianka Wahyuningtias, Dendy Rosman, Eka Diraksa Putra, Farah Levyta,Ryonaldi Maulana	172 - 175
	Id_Paper_105	
31	Implementation Of Unified Theory Of Acceptance And Use Of Technology (Utaut) Model For Evaluating The Use Of E- Government Sidjp Nine In Indonesia	176 - 180

Levana Dhia Prawati, Martinus Hanung Setyawan, Afriana Lukita Sari, Mahda Karina

- Id\_Paper\_108
- 32 **Modify Linear Congruent Generator Algorithms Using Inverse Elements Of Modulo Multiplication For Randomizing Exams** 181 - 183  
Sujono Sujono, Maxrizal Maxrizal, Syafrul Irawadi, Baiq Desy Aniska Prayanti
- Id\_Paper\_111
- 33 **A Review Of Optical Text Recognition From Distorted Scene Image** 184 - 188  
Oliver Oswin Sumady, Brian Joe Antoni, Randy Nasuta, Nurhasanah Nurhasanah, Edy Irwansyah
- Id\_Paper\_112
- 34 **Smart Lighting System For Children'S Therapy To Prevent Nyctophobia Syndrome At Bedtime** 189 - 193  
Andi Pramono, Badrul Munir, Muchammad Farchan, Satrio Arif Budiman, Baskoro Azis, Wahyu Waskito Putra
- Id\_Paper\_113
- 35 **Students Experience Testing In The Implementation Of The “Gather Town” Meeting Platform As An Alternative Learning Media Other Than Zoom Cloud Meeting Application** 194 - 201  
Eko Setyo Purwanto, Danielson Danielson, Khawen Flawrenxius, Bryan Anderson, Azani Cempaka Sari
- Id\_Paper\_114
- 36 **Smart Trash Cans For Waste Management Using Nodemcu And Ultrasonic Sensor** 202 - 206  
Julian Alifirman Wardana, Andros Clarence Chen, Rahmat Syifana Jaelani, Leonardo Leonardo, Budi Juarto
- Id\_Paper\_123
- 37 **A Blockchain-Based Framework Gamification For Securing Learners Activity In Merdeka Belajar-Kampus Merdeka** 207 - 212  
Henderi Henderi, Muhamad Yusup, Po Abas Sunarya, Ninda Lutfiani, Efa Ayu Nabila
- Id\_Paper\_124
- 38 **Novel Framework To Define Extended & Mixed Reality For Online Learning** 213 - 216  
Bhupesh Rawat, Ankur Singh Bist, Untung Rahardja, Eka Purnama Harahap, Rafly Ananda Dwi Septian
- Id\_Paper\_130
- 39 **Self-Sustain Smart Aquaponic Using Embedded System** 217 - 222  
Jonathan Axel Benaya, Cecilia Valenda, Syahazna Balqis Renzaputri, Stanley Wisely, Mochammad Haldi Widiyanto

	Id_Paper_131	
40	Sentiment Analysis Towards Face-To-Face School Activities During The Covid-19 Pandemic In Indonesia Oei Angela Christabel Gunawan, Denny Alvito Ginting, Rionaldo Alviansa Handoyo, Andrew Willy, Samuel Chandra, Fredy Purnomo, Risma Yulistiani	223 - 229
	Id_Paper_135	
41	Smart Rfid System For Locker Cabinet Security Using Android App Kristianto Wijaya, Jonathan Audris Heriyanto, Davis Inde Satya, Jovianto Godjali, Rissa Rahmania	230 - 237
	Id_Paper_136	
42	Analyzing Ai And The Impact In Video Games Leonardo Jose Gunawan, Brandon Nicolas Marlim, Neil Errando Sutrisno, Risma Yulistiani, Fredy Purnomo	238 - 241
	Id_Paper_145	
43	How Information Technology Literacy Moderated Factors Affecting Quality Of Computer-Based Audit Ang Swat Lin Lindawati, Bambang Leo Handoko	242 - 247
	Id_Paper_153	
44	Sentiment Analysis For Financial News Using Rnn-Lstm Network Kelvin Leonardi Kohsasih, B. Herawan Hayadi, Robet, Carles Juliandy, Octara Pribadi, Andi	248 - 253
	Id_Paper_155	
45	Encrypted Message Hiding On Gif Image Using The Gifshuffle Algorithm Yusfrizal Yusfrizal, Mutiara Sovina, Faisal Amir Harahap, Helmi Kurniawan, Rubianto Rubianto, Frans Ikorasaki	254 - 257
	Id_Paper_159	
46	Factors Influenced User Interest In Payment Transaction Of Shopeepay Digital Wallet Application Bambang Leo Handoko, I Gusti Made Karmawan, Lilis Meliana	258 - 263
	Id_Paper_163	
47	Development Of Papaya Plant Automation Systems With The Internet Of Things Concept Using Fuzzy Logic Ni Luh Gede Pivin Suwirmayanti, Ricky Aurelius Nurtanto Diaz, I Komang Agus Ady Aryanto, Gede Angga Pradipta, Ida Bagus Maha Indra Prasada	264 - 269
	Id_Paper_164	
48	E-Passport Covid-19 Adopting Rfid Implants Based On Microservices Ardian Rianto, Marchel Thimoty Tombeng, I-Shyan Hwang, Andrew Tanny Liem	270 - 274

	Id_Paper_167	
49	Sentiment Identification System For E-Commerce Mobile App Reviews Using Single Layer Neural Network Semmy Wellem Taju, Edson Yahuda Putra, Green Ferry Mandias	275 - 281
	Id_Paper_168	
50	Evaluation Of Elearning Using The Human Organization Technology (Hot) Model Erfan Hasmin, Nurul Aini	282 - 285
	Id_Paper_172	
51	Analysis Of Determination Of Items Ordering Patterns By Using Apriori Method Bob Subhan Riza, Hendra Nusa Putra, Ahmad Zamsuri, Lusiana Efrizoni, Sarjon Defit	285 - 288
	Id_Paper_173	
52	The Development Of A Medical Chatbot Using The Svm Algorithm Ryan Matthew, David Agustriawan, Mario Donald Bani, Muammar Sadrawi, Nanda Rizqia Pradana Ratnasari, Moch Firmansyah, Arli Aditya Parikesit	289 - 294
	Id_Paper_181	
53	Development Of Iot Implementation In Heart Rate And Glucose Monitoring System Gabriel Flavianus, Marcello Octavio Anugrahanto, Dani Suandi, Farrel Nelson Veriano, Daevan Martana, Davy Ronald Hermanus	295 - 300
	Id_Paper_183	
54	Web E-Learning: Automated Essay Assessment Based On Natural Language Processing Using Vector Space Model Syaharullah Disa, Purnamawati Purnamawati, Andi Muhammad Idkhan	301 - 304
	Id_Paper_185	
55	The Impact Of Instagram'S Suggested Algorithm On The Learning Behavior Of The Students Of The Faculty Of Computer Science, Universitas Klabat Reynoldus Andrias Sahulata, Jimmy Moedjahedy, Jody Joseph, Dickson Ryan Jose	305 - 309
	Id_Paper_186	
56	Learning Vector Quantization (Lvq) For Colorectal Cancer Identification Based On Microscopic Network Image Heri Gunawan, Soeheri Soeheri, Deny Adhar, Hardianto, Linda Wahyuni, Charles Bronson Harahap	310 - 314
	Id_Paper_187	

57	Classification Of Papuan Batik Motifs Using Deep Learning And Data Augmentation Suhardi Aras, Arief Setyanto, Rismayani Rismayani	315 - 319
	Id_Paper_188	
58	"A Lone Burglar" Stealth Game Development Using Rapid Application Development Ivan Gananjaya, Jesse Owen Theodore Chandra, Johann Felix Alexander Christanto, Mochammad Haldi Widiyanto, Jesslyn Audrey	320 - 324
	Id_Paper_189	
59	Motion Detection Application To Measure Straight Leg Raise Rom Using Mediapipe Pose Hustinawaty Hustinawaty, Tavipia Rumambi, Matrisnya Hermita	325 - 329
	Id_Paper_195	
60	The Antecedent Of E-Learning Adoption Indriana Indriana, Doni Purnama Alamsyah, Andreas Chang, Ivan Diryana Sudirman	330 - 334
	Id_Paper_197	
61	Development Of Techniques For Speech Emotion Recognition (Ser) In The Context Of Deep Learning Budi Triandi, Herman Mawengkang, Syahril Efendi, Sawaluddin Sawaluddin	335 - 341
	Id_Paper_201	
62	Development Of Internet Of Things-Based Instrument Monitoring Application For Smart Farming Mochammad Haldi Widiyanto, Bryan Ghilchrist, Gerry Giovan, Rachmi Kumala Widyasari, Yovanka Davincy Setiawan	342 - 347
	Id_Paper_202	
63	Empowering The Smart Lighting System In The Office Rooms To Enhance The Worker'S Productivity Salsa Nabillah, Andi Pramono, Delly Minita Asnathasia, Ribka Xantia Kusuma, Yohanes Raynaldi Pereira, Stanley Santoso Sandiawan	348 - 352
	Id_Paper_203	
64	Designing An Optimization Model For Dynamic Facility-Location Problem At Post-Disarter Area Considering Uncertainty Lili Tanti, Syahril Efendi, Maya Silvi Lydia, Herman Mawengkang	353 - 358
	Id_Paper_209	
65	Rice Plants Disease Classification Using Transfer Learning Felix Pherry, Gregorius Gregorius, Jonathan Kristanto, Felix Indra Kurniadi	359 - 362

	Id_Paper_212	
66	Application Of Line Reactors And Harmonic Filters In Electric Power Systems Are Integrated Renewable Energy In Mesh Topology Langlang Gumilar, Arif Nur Afandi, Denis Eka Cahyani, Eli Hendrik Sanjaya, Ahmad Asri Bin Abd Samat	363 - 367
	Id_Paper_215	
67	Human Brain Wave Concentration Pattern Prediction Design Concept Iwan Fitrianto Rahmad, Muhammad Zarlis	368 - 370
	Id_Paper_217	
68	Blockchain Security And Corporate Governance Mochammad Fahlevi, Moeljadi Moeljadi, Siti Aisjah and Atim Djazuli	371 - 375
	Id_Paper_221	
69	Analysis Of Customer Product Interests Using The Market Basket Analysis Model With Hash-Based Algorithm And Association Rules Berlilana, Taqwa Hariguna, Andhika Rafi Hananto	376 - 380
	Id_Paper_222	
70	Prediction Of Students Final Project Values Based On Errors In Scientific Writing Using Data Mining Classification Algorithms Taqwa Hariguna, Taqwa Hariguna, Andhika Rafi Hananto	381 - 386
	Id_Paper_224	
71	Semantic Similarity Of Indonesian Sentences Using Natural Language Processing And Cosine Similarity Reza Fauzan, Muhammad Ikhwanul Atha Labib, Joshua Oktavianus Tarung Johannis, Herlinawati Herlinawati, Syamsudin Noor, Saifullah Saifullah	387 - 390
	Id_Paper_225	
72	He Role Of Gender In Moderating The Effect Of Teachers Empathy, Reputation And System Quality On Student Satisfaction Online Learning Program Mochammad Fahlevi, Lily Leonita and Aries Aries	391 - 394
	Id_Paper_226	
73	E-Messenger In Telecommunication Platform Evi Triandini,Wayan Cahya Ayu Pratami, Agnesia Candra Sulyani, Riza Wulandari, I Gusti Ngurah Satria Wijaya, Sugiarto, I Ketut Putu Suniantara	395 - 400
	Id_Paper_234	
74	Integrating Philanthropy System In Indonesia Using Service-Oriented Architecture	401 - 404



Dewi Khairani, Husni Teja Sukmana, Patriot Muslim, Herlino Nanang, Tabah Rosyadi, Amri Amri

Id\_Paper\_235

- 75 Integrating Ambulance Into Gis In Smart City: Problems And Prospect With P-Median Model 405 - 408

Rafiqa Dewi, Tulus Tulus, Muhammad Zarlis, Erna Budhiarti Nababan

Id\_Paper\_239

- 76 Forest Fire Forecasting Application Implementation Using The Linear Regression Algorithm 409 - 413

Muhammad Khoirul Wiro, Dendi Anggriandi, Sal Sabila Wijayanti, Ariel Yonatan Alin, Maie Istighosah, Kusrini Kusrini

Id\_Paper\_240

- 77 Impact Of Interline Power Flow Control In Wind Power Plant Integrated With Distribution Network 414 - 418

Langlang Gumilar, M. Wahyu Prasetyo, Herpri Melinia

Id\_Paper\_241

- 78 Fire Detection Based On Smoke Image Using Convolutional Neural Network (Cnn) 419 - 423

Jefri Zulkarnain, Mohammad Rezza Pahlevi, Yustikamasy Astica, Widi Pangestuti, Kusrini Kusrini

Id\_Paper\_242

- 79 Development A 3D Catalog Application As A Presentation Means Of Glovic Cafe And Bakery Jember Design By Using Augmented Reality 424 - 429

Althea Adeltrudis Harjo, Lenny Suwondo, Veronica Livianty, Fairuz Iqbal Maulana, Ida Bagus Ananta Wijaya

Id\_Paper\_244

- 80 U-Net Tuning Hyperparameter For Segmentation In Amniotic Fluid Ultrasonography Image 430 - 435

Putu Desiana Wulaning Ayu, Gede Angga Pradipta

Id\_Paper\_247

- 81 Modification Of Attractiveness And Movement Of The Firefly Algorithm For Resolution To Knapsack Problems 436 - 440

David David, Edy Victor Haryanto S, Ronny Ronny, Tri Widayanti

Id\_Paper\_248

82	Media And Information Literacy: Quantitative Exploration Of The Burden Of Information Needs In Librarian Users Irmawan Rahyadi, Dwi Ramadhona, Masyhur Duncik, Rara Sativa, Matthew Austin Naibaho	441 - 445
	Id_Paper_249	
83	Classification Of Indonesian Music Genres Using The Support Vector Machine Method Yuni Yuniar, Doni Purnama Alamsyah, Asti Herliana	446 - 451
	Id_Paper_250	
84	Design Of Collaborative Cloud Classroom (Cccr) For Ethno-Flipped Classroom Teaching Model Rahmi Ramadhani, Edi Syahputra, Elmanani Simamora, Abdul Meizar.	452 - 456
	Id_Paper_251	
85	3D Low Poly Asset Creation Based On Balinese Local Wisdom Concept Putu Devi Novayanti, Padma Nyoman Crisnapati, Ricky Aurelius Nurtanto Diaz	457 - 461
	Id_Paper_252	
86	A New Approach Feature Selection For Intrusion Detection System Using Correlation Analysis Dandy Pramana Hostiadi, Yohanes Priyo Atmojo, Roy Rudolf Huizen, I Made Dharma Susila, Gede Angga Pradipta, I Made Liandana	462 - 467
	Id_Paper_253	
87	Optimization Of Student Database Confidentiality Using Elgamal Algorithm And Fermat Method Rubianto Rubianto, Roslina Roslina, Rika Rosnelly	468 - 473
	Id_Paper_254	
88	Applying Minimum Message Length To The Clustering Of Mutual Funds Yudi Agusta	474 - 479
	Id_Paper_255	
89	Vr Real Run: An Immersive Oculus Quest 2-Based Virtual Reality Exergaming Joe Yuan Mambu, Rismayani Rismayani, Jay Idoan Sihotang, Vivi Peggy Rantung	480 - 485
	Id_Paper_259	
90	Ear Feature Extraction Methods – A Review Lilis Yuningsih, Gede Angga Pradipta, Putu Desiana Wulaning Ayu, Roy Rudolf Huizen, Dandy Pramana Hostiadi	486 - 490
	Id_Paper_260	

91	Adaptive Neuro-Fuzzy Inference System For Medical Image Classification – A Review Lilis Yuningsih, Roy Rudolf Huizen, Gede Angga Pradipta, Putu Desiana Wulaning Ayu, Dandy Pramana Hostiadi	491 - 499
	Id_Paper_261	
92	Classification Of Rice Leaf Diseases Based On Texture And Leaf Colour Evi Dewi Sri Mulyani, Hendri Julian Pramana, Lina Listiani, N. Nelis Febriani Sm, Restu Adi Wiyono, Firah Putri Pratiwi	500 - 505
	Id_Paper_262	
93	Internet Of Things System For Freshwater Fish Aquarium Monitoring And Automation Using Iterative Waterfall Theodorus Ezra Suherman, Mochammad Haldi Widiyanto, Zefany Athalia	506 - 511
	Id_Paper_263	
94	It Governance: Performance Assessment Of Maturity Levels Of Rural Banking Industry Sandy Kosasi, Untung Rahardja, I Dewa Ayu Eka Yuliani, Robertus Laipaka, Budi Susilo, Herlina Kikin	512 - 517
	Id_Paper_264	
95	The Business Prospect In Metaverse And Nft Era (User, Accountant, And Gaming Community Perspectives) Kenny Thenjono, Felix Ratana, Setiani Putri Hendratno	518 - 523
	Id_Paper_265	
96	Investigating The Role Of It-Based Operational Improvement And It-Based Service Innovation To Achieve Business Survival Assed Lussak, Ibnu Darmawan	524 - 527
	Id_Paper_267	
97	An Analysis Air Traffic Prediction During A Pandemic Darmeli Nasution, Herman Mawengkang, Fahmi Fahmi, Muhammad Zarlis	528 - 533
	Id_Paper_269	
98	Examining The Impact Of It Experience, Training, Self-Efficacy And Anxiety On Remote Work Quality In Indonesia Assed Lussak, Ibnu Darmawan	534 - 537
	Id_Paper_270	
99	Vehicle Routing Problem In Electric Fleet Sundari Retno Andani, Muhammad Zarlis, Herman Mawengkang, Sutarman Sutarman	538 - 540

	Id_Paper_272	
100	Geofencing Application For Parents Tracking Children Using Push Notification In Universitas Klabat Based On Mobile Stenly Ibrahim Adam, Oktoverano Hendrik Lengkong, Stenly Richard Pungus, Suvin Raj Kollabathula	541 - 546
	Id_Paper_273	
101	Mobile-Based Road Infrastructure Damage Reporting Service Application Stenly Ibrahim Adam, Reymon Rotikan, Prince Siachin Pasombaran, Gabriel Janes Posumah	547 - 553
	Id_Paper_274	
102	Online Handwritten Recognition For Alphabet Writing Practice Ni Putu Linda Santiari, I Gede Surya Rahayuda	554 - 559
	Id_Paper_278	
103	Communication Signal Network Optimization Model Based On The Concept Of Ubiquitous Clouds Sumarlin Sumarlin, Muhammad Zarlis, Suherman, Syahril Efendi	560 - 562
	Id_Paper_280	
104	Ridge Polynomial Neural Network For Brain Cancer Based On Android Riah Ukur Ginting, Poltak Sihombing, Syahril Efendi, Amila, Burhanuddin Damanik	563 - 567
	Id_Paper_281	
105	Text-Based Emotion Detection Using Cnn-Bilstm Denis Eka Cahyani, Aji Prasetya Wibawa, Didik Dwi Prasetya, Langlang Gumilar, Fadhilah Akhbar, Egi Rehani Triyulinar	568 - 572
	Id_Paper_286	
106	Footstep Detection For Indoor Positioning Using Accelerometer And Magnetometer Sensor On Smartphone Made Liandana, Bagus Made Sabda Nirmala, Gede Angga Pradipta, Dandy Pramana Hostiadi	573 - 579
	Id_Paper_287	
107	Development Of A Chatbot For The Online Application Telegram Chat With An Approach To Classification Of Emotions On Text Using The Indobert-Lite Method Khodijah Hulliyah, Faishal Rayyan, Normi Sham Awang Abu Bakar	580 - 583
	Id_Paper_288	
108	Dogs Feed Smart System With Food Scales Indicator Iot Based Robby Kurniawan Harahap, Eri Prasetyo Wibowo, Dyah Nur'Ainingsih, Andrian Kharisma Wijaya, Widyastuti Widyastuti, R. A. Sekar Ciptaning Anindya	584 - 590

	Id_Paper_289	
109	Classify Malaria Dataset Human Blood Images Using Convolutional Neural Networks Purnawarman Musa, Eri Prasetyo Wibowo, Matrisnya Hermita, Raihan Firas Muzhaffar	591 - 598
	Id_Paper_292	
110	Prediction Of Feed Quantity Using Multiple Linear Regression Algorithm For Clarias Farming Esmi Nur Fitri, Sri Winarno, Farrikh Al Zami, Affandy Affandy, M. Hafidz Ariansyah	599 - 602
	Id_Paper_293	
111	Clarias Size Clustering To Determine Market Segmentation Using K-Means Algorithm M. Hafidz Ariansyah, Sri Winarno, Farrikh Al Zami, Affandy Affandy, Esmi Nur Fitri	603 - 607
	Id_Paper_294	
112	Prototype Nft/Dft Hydroponic Data Collection Using Iot System IGKG Puritan Wijaya ADH, I Nyoman Rudy Hendrawan, I Made Bhaskara Gautama, I Made Arya Budhi, I Gusti Ngurah Wikranta Arsa	608 - 613
	Id_Paper_295	
113	Microrna And Gene Relationship Between Ethnicity And Cancer Stage As Potential Biomarker And Treatment For Lung Adenocarcinoma Nadya Natasya, David Agustriawan	614 - 620
	Id_Paper_296	
114	Amplitude And Frequency Based Evaluations For Algorithm Development Of Premature Ventricular Contraction Detection System Joshua Sun, Mario Donald Bani, Moch Firmansyah, David Agustriawan, Muammar Sadrawi	621 - 624
	Id_Paper_298	
115	Sentiment Analysis Of Government Policy Regarding Ppkm On Twitter Using Lstm Green Arther Sandag, Eben Haezar Ekoputra Soegiarto, Lidya Laoh, Andre Gunawan, Debby Sondakh	625 - 630
	Id_Paper_299	
116	Modifying The Revised Niosh Lifting Equation Using Anthropometric Variables To Calculate Horizontal And Vertical Multipliers Moehamad Adi Rochmat, Sarifuddin Madenda, Tri Handhika, Ernastuti Ernastuti	631 - 638

# Optimization of Student Database Confidentiality Using Elgamal Algorithm and Fermat Method

Rubianto  
Faculty of Engineering and Computer  
Science  
Universitas Potensi Utama  
Medan, Indonesia  
rubiantoditpi@gmail.com

Roslina  
Faculty of Engineering and Computer  
Science  
Universitas Potensi Utama  
Medan, Indonesia  
roslinanich@gmail.com

Rika Rosnelly  
Faculty of Engineering and Computer  
Science  
Universitas Potensi Utama  
Medan, Indonesia  
rikarosnelly@gmail.com

**Abstract**— Every Islamic boarding school institution must have many databases, one of which is the student database. Securing the student database is needed to protect student data and information from database theft. To create an optimal system in securing the student database with the aim of avoiding accessing and processing data and information by unauthorized persons, the student database processed in this study used the ElGamal algorithm and the Fermat method with key formation using prime numbers and solving the problem requires discrete logarithm calculations. The keys used by this algorithm are the public key and the private key. The result of testing this method is that the student database is encrypted. The algorithm used to generate these prime numbers is to use Fermat. The ElGamal algorithm is very helpful in securing the student database at the Darul Hikmah Islamic Boarding School TPI Medan. In testing the encryption of the student database file with the file name "santri.mdf" it was successfully converted into a file with the new name "santri\_mdf.encrypt", and in the decryption process it could return to plaintext with the name "santri.mdf".

**Keywords**— student database, Elgamal algorithm, Fermat method

## I. INTRODUCTION

Computer system security is becoming increasingly important along with the development of computerized business processes. A computerized business process is a business process that most of its activities use computer technology and make computers as a storage medium for important data so that it can be said that computer media is an important factor in running business processes. Computer system security that is in the spotlight is not only the computer equipment, but also the security for the network, software or application programs and also database security [1].

Data processing is a routine thing in educational institutions, especially in Darul Hikmah Islamic Boarding School TPI Medan. For example, in teaching activities and evaluating the report of student learning outcomes at the end of each semester. This evaluation will be vulnerable if the work process carried out is still using the old system. The system still uses a simple method, namely handwriting and data processing using a computer system that relies on Microsoft Excel.

The security and confidentiality of the data stored in the database is one of the important aspects of an information system, as the data is safe from information leakage. Security of computer networks connected to databases no longer guarantees data security because data leaks can be caused by insiders or parties directly related to databases such as database administrators [2].

Database security can be done in various ways, starting from limiting user access rights to the database itself, using field names that are only understood by administrators so that not all employees who are given permission to access the database understand the existing database flows to avoid data theft, data destruction and so on [3]. So on, to the implementation of cryptographic algorithms by administrators on records in the database with the aim of making stored records more secret and difficult to read by other parties.

One mechanism to improve the security of data in the database is to use encryption technology. The data stored in the database is modified in such a way that it is not easy to read. So encryption is a process that is carried out to secure data (called plaintext) into hidden data (called cipher text). Cipher text is data that can no longer be read easily [4].

Elgamal's security is based on discrete logarithm problems to encrypt and decrypt messages separately. An intruder trying to decrypt a disconnected message can try to recover the private key [6]. For this purpose logarithms need to be calculated. There is no actual method for this, given that certain needs in the initial group are met.

Generating prime numbers is an essential problem in computer science and number theory, especially in the field of cryptography. This is because public key encryption protocols are based on the use of large prime numbers. While the security of public key cryptography systems is often based on the difficulty of getting the prime factors of a very large prime number. Although the algorithm to determine the primacy of a number that has been found is still relatively slow for the current problem, a probabilistic algorithm can be formed using the Fermat method [7].

Prime numbers are widely used by the field of cryptography. Even so, there is no exact algorithm that can determine the primacy of a number efficiently. By using Fermat's Theorem, an alternative can be done, namely creating a probabilistic algorithm to determine the prime value of a number [7].

Due to this probabilistic nature, the result of this algorithm is not exact but is probabilistic. However, the possibility of this algorithm producing errors can be minimized by using some calculations. In the computer world, several ways have been found to find these prime numbers, one of which is by using the Fermat method to find these prime numbers.

## II. RELATED WORK

In a study conducted by Haval I. Hussein & Wafaa M. Abdullallah proposed to overcome the existing weaknesses. Modifications are made to reduce the size of the cipher text

and speed up execution time. This is done by using additional operations instead of looping in the encryption process. Based on the experimental results, the proposed scheme reduces the expansion rate by 89%. As well as speed up execution time which makes the proposed scheme performs better. So, the goal of increasing the efficiency of the ElGamal Cryptosystem is significantly increased. The security of the proposed scheme is not affected in the same way as the existing security is based on the difficulty of solving discrete logarithm problems [8].

Another research conducted by Demba Sow & Mamadou Ghouraisiou Camara resulted in a new variant of ElGamal signature scheme called "General ElGamal signature scheme" proposed in 2011. The General ElGamal signature scheme is a modified ElGamal signature scheme. In this study, a proof of security of the Generalized ElGamal signature scheme is proposed in a random oracle model. Some security signature scheme ideas and demonstrate the security of modified ElGamal Signature scheme. We have succeeded in proving the existential exogism of the Generalized ElGamal signature scheme, adaptively to selected message attacks, in a random oracle model [9].

Research conducted by Djebaili Karima & Melkemi Lamine proposed a secure version of the Elgamal public key cryptosystem, and proved that it is semantically secure assuming what we call the two-dimensional Diffie-Hellman decision problem (2DDDH), this cryptosystem is distinguished by the speed of the encryption process and decryption and by its resistance to active enemies [10]. Since the 2DDDH problem is more difficult than the decisional Diffie-Hellman (DDH) problem (as will be seen), we can conclude that the model strengthens the security of the exchange compared to existing cryptosystems in the same context, also we discuss the difficulty of the problem that ensures its security. In this study, a new computational problem called the Diffie-Hellman (2DDDH) two-dimensional decision problem [11]. This extension can be used in many cryptographic constructs based on DL problems. In addition, the 2DDDH problem is more difficult than the regular DDH problem that some logarithmic problem-based schemas rely on. Our new paradigm has many applications. As one such application, we present a new variant of ElGamal encryption with very simple proof of security [11].

Research conducted by Gupta et al presents a cryptosystem derived from the quantum version of diffie-hellman as described previously, but it may be seen as an improvement because the Elgamal Cryptosystem can be used to sign messages or encryption in one direction without direct interaction between the parties. The protocol for exchanging qubit sequence pairs between two parties via a quantum channel and using a computational base as a parameter for the commutative quantum rotation transformation to decrypt the message. Quantum postal cryptography is the latest field of research to emerge after the introduction of the Short algorithm. Classic cryptosystems like RSA, Diffie-Hellman and ElGamal will be completely obsolete with quantum computers [12].

Research also conducted by E. Jincharadze explained that cryptography is the science or study of secret writing techniques, especially code and cipher systems, methods, and the like. Cryptography must ensure a high level of security in transferring and storing data. There are two types of

cryptographic algorithms such as symmetric key cryptography and asymmetric key cryptography [13]. Currently there are various types of cryptographic algorithms that provide high information security, but they also have some drawbacks. To improve the weakness of this algorithm, in this paper we propose a new hybrid cryptographic algorithm model. This algorithm is designed using a combination of two cryptographic algorithms AES and Elgamal. An analysis and comparison of the performance of the proposed algorithm has been carried out by following the parameters of encryption time, decryption time and system requirements [14]. For this cryptographic algorithm, a program is made in Java in the NetBeans IDE. Implementation and analysis of the performance of the proposed model is carried out by Java. The final result shows that the hybrid model has better performance than the AES and Elgamal systems [15].

Another research conducted by Yuling Luo, et al resulted in research on security issues regarding key management and distribution for symmetric image encryption schemes, a new asymmetric image encryption method is proposed in this paper, which is based on ElGamal elliptic curve (EC-ElGamal) cryptography and chaotic theory. In particular, the SHA-512 hash was first adopted to generate the initial values of the chaotic system, and the cross permutations in terms of the order of the chaotic indexes were used to randomize the ordinary images [16]. Furthermore, the generated random image is embedded into an elliptic curve to be encrypted by EC-ElGamal which can not only improve security but can also help solve key management problems. Finally, a game of diffusion-combined chaos with DNA sequences is played to get the cipher image. Experimental analysis and performance comparison show that the proposed method has high security, good efficiency, and strong resistance to selected plain text attacks which makes it have potential applications for secure image communication [17].

Other research on Elgamal encryption was also carried out by Motilal Singh Khoirom, et al. Encrypting using Elgamal public key encryption in a limited field requires the insertion of messages represented by integers. This integer must be implanted to a coordinate location that satisfies the equation of the elliptic curve using the Koblitz embedding technique [18]. Thus, data expansion occurs because every integer must be represented as a coordinate. The recommended elliptic curve has a large modulo prime, so for any small integer representation of a message, the expansion in the cipher text is very large. The above factors hinder the use of the ElGamal method for encryption of large data sizes. In the ameliorated version, any coordinate in the elliptic curve equation can be used to perform encryption operations [19]. The typical Koblitz embedding technique to certain coordinates that satisfy the elliptic curve equation can be avoided. Data expansion issues are addressed by using basic conversion operations with some audio data. The simulation results and performance comparison with other public key cryptosystems indicate that the proposed method is suitable for audio encryption operations [20].

### III. RESEARCH METHODOLOGY

The research methodology will greatly assist the author in the problem solving work process. This research has several stages in carrying out the activities contained in the sequence of research activities, namely identifying problems, analyzing problems, determining goals, studying literature,

collecting data, designing systems, implementing the Elgamal algorithm and the Fermat method on database security, testing and drawing conclusions.

The following will describe the methodology and sequence of research activities used in the completion of this research. The sequence of these activities is the stages that will be carried out in order to solve the problems that will be discussed. The sequence of activities from this research can be seen in Figure 1.

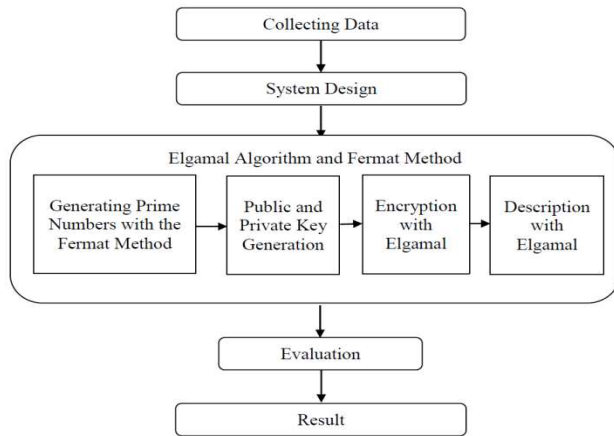


Fig. 1. Research Methodology

Based on Figure 1, the following is a description of the following sequences of research activities:

1. Collecting data, done by requesting data from the student admin about the student database at the TPI Medan Islamic Boarding School, taking data from books and journals about database security. This data will be used as a reference in making the student database security application.
2. Designing the system, at this stage the data collected is then designed into a system that will be processed and implemented with predetermined methods. The design of the system is to change the raw data that has been obtained into data that is ready to be processed so that it is expected that the results of the processing can be as expected.
3. Implementing the Elgamal and Fermat Algorithms, the data obtained are then analyzed and implemented to produce useful information. At this stage, data processing is carried out to secure the student database at the TPI Medan Islamic Boarding School. In accordance with data processing, at the implementation stage, testing of the application of the Elgamal algorithm is carried out to secure the database of the designed application.
4. Evaluation, at this stage, the results of data analysis that have been processed previously will be tested using the specified application. Testing the Elgamal Algorithm can be done by trying the encryption and decryption process of the student database at the TPI Medan Islamic Boarding School. At the system testing stage, two methods are used, namely functionality testing and validity testing. The functionality test is carried out by black box testing while the validity test is carried out by testing the similarity of the calculation results of the program code and manual calculations. The approach taken by writing in testing the system made is Black Box

Testing where this test aims to show the software functions on how to operate, whether the encryption and decryption processes are running correctly and the application can be used by users.

5. Results, after being tested, at this stage the database security cryptography application passes the testing stage and the results are ready to be used by Windows users. It is possible that this system will experience changes when it is used by users. Changes can occur due to errors that appear and are not detected during testing. The support or maintenance phase can repeat the development process starting from specification analysis for changes to existing information systems, but not to create new information systems.

#### IV. ANALYSIS AND RESULT

The steps in the general stage of analysis will be almost the same as those in the steps that will be taken in defining the system plan. In the analysis phase, the scope of the task is more detailed. In this system analysis, the research that will be carried out by systems analysis is a detailed study, while in system planning it is only a preliminary study.

The first step is to do a system analysis. System analysis aims to gain knowledge related to the confidentiality of the SQL Server database using the Elgamal algorithm and the Fermat method. This application is used to convert the original text contained in the SQL Server database into secret text so that it cannot be read by the authorities.

The problem of database security and confidentiality is one of the important aspects of an information system. Information is only intended for certain parties, it is related to how the information cannot be accessed by unauthorized people. File security in the database can be done by using several asymmetric algorithms that can lock database files, including the Elgamal algorithm and the Fermat method.

In this case, there are still many people who do not understand how to access or secure database files so that the data contained in them cannot be seen by others. This is due to the difficulty of computer security procedures when using the facilities provided by each operating system. For that, we need an application that can easily and quickly lock and secure the user's computer by using the password entered into it.

Therefore we need a database security system that aims to improve data security, protect data or messages from being read by unauthorized parties, and prevent unauthorized parties from inserting, deleting, or changing data.

The problem-solving stage is carried out starting from the process of analyzing, designing, evaluating and improving the system according to needs, so that the system that is being made can be used optimally. This study uses the Elgamal algorithm and the Fermat method for cryptographic techniques as a way to secure the student database at the Darul Hikmah Islamic Boarding School TPI Medan.

This research resulted in an Elgamal encryption and decryption application program which was built using visual basic. The resulting application is used to encrypt the database files. The results of the research carried out are changing the original database file into an encrypted database file where the contents of the database file cannot be read, returning the unreadable database file to the original



database file with the Elgamal method without destroying and changing the contents of the database file, and changing the file. The original database as the plaintext change into cipher text, which will be unreadable codes.

The following is the application of the Elgamal algorithm and examples of manual calculations on securing student data at the Darul Hikmah Islamic Boarding School TPI Medan:

#### 1. Encryption Process

Suppose A generates a key pair by choosing a random prime number as the key used is  $p = 97$ ,  $g = 7$  and  $x = 2$ .

Then  $p$ ,  $g$ ,  $x$  are used to calculate  $y$ .

So,  $y = gx \bmod p = 72 \bmod 97 = 49$ .

So A's public key is:  $y = 49$ ,  $g = 7$ ,  $p = 97$  and A's private key is:  $x = 2$ ,  $p = 97$ . Convert characters into ASCII numbers denoted by  $m$ . Determine the value of  $k$ , in this case  $k = 2$ .

Suppose B wants to send plaintext "ABDUL MEIZAR" to A, then each character of the plaintext is converted into ASCII form denoted by  $m$ , resulting in the following:

**$m = \text{ABDUL MEIZAR}$**

ASCII plaintext

**A = 65**

**B = 66**

**D = 68**

**U = 85**

**L = 76**

**space = 32**

**M = 77**

**E = 69**

**I = 73**

**Z = 90**

**A = 65**

**R = 82**

Then the ASCII values are entered into blocks of  $m$  values sequentially.

For the plaintext block ( $m_1$ ), namely the character "A", change the character "A" to an ASCII value of 65. Then do the encryption process, in this process the values  $a$  and  $b$  will be obtained as cipher text obtained by the formula:  $a = g^k \bmod p$  and  $b = y^k m \bmod p$ . For more details see the following calculations.

**Character A = 65 as the value of  $m_1$ .**

Then, we get the cipher text ( $a$ ,  $b$ ):

$a = g^k \bmod p = 72 \bmod 97 = 49$

$b = y^k m \bmod p = (492 \times 65) \bmod 97 = 89$

From the above calculation results obtained cipher text of the letter A is block C1 = (49,89).

**Character B = 66 as the value of  $m_2$ .**

Then, we get the cipher text ( $a$ ,  $b$ ):

$a = g^k \bmod p = 72 \bmod 97 = 49$

$b = y^k m \bmod p = (492 \times 66) \bmod 97 = 65$

From the above calculation results obtained cipher text of the letter B is block C2 = (49,65).

**Character D = 68 as the value of  $m_3$ .**

Then, we get the cipher text ( $a$ ,  $b$ ):

$a = g^k \bmod p = 72 \bmod 97 = 49$

$b = y^k m \bmod p = (492 \times 68) \bmod 97 = 17$

From the results of the above calculation, it is obtained that the cipher text of the letter D is block C3 = (49,17).

**Character U = 85 as the value of  $m_4$ .**

Then, we get the cipher text ( $a$ ,  $b$ ):

$a = g^k \bmod p = 72 \bmod 97 = 49$

$b = y^k m \bmod p = (492 \times 85) \bmod 97 = 94$

From the results of the above calculation, it is obtained that the cipher text of the letter U is block C4 = (49,94).

**Character L = 76 as the value of  $m_5$ .**

Then, we get the cipher text ( $a$ ,  $b$ ):

$a = g^k \bmod p = 72 \bmod 97 = 49$

$b = y^k m \bmod p = (492 \times 76) \bmod 97 = 19$

From the results of the above calculation, it is obtained that the cipher text of the letter L is block C5 = (49,19).

**Space character = 32 as the value of  $m_6$ .**

Then, we get the cipher text ( $a$ ,  $b$ ):

$a = g^k \bmod p = 72 \bmod 97 = 49$

$b = y^k m \bmod p = (492 \times 32) \bmod 97 = 8$

From the calculation results above, the cipher text of spaced letters is block C6 = (49,8).

**The character M = 77 as the value of  $m_7$ .**

Then, we get the cipher text ( $a$ ,  $b$ ):

$a = g^k \bmod p = 72 \bmod 97 = 49$

$b = y^k m \bmod p = (492 \times 77) \bmod 97 = 92$

From the above calculation results, the cipher text of the letter M is block C7 = (49,92).

**Character E = 69 as the value of  $m_8$ .**

Then, we get the cipher text ( $a$ ,  $b$ ):

$a = g^k \bmod p = 72 \bmod 97 = 49$

$b = y^k m \bmod p = (492 \times 69) \bmod 97 = 92$

From the above calculation results obtained cipher text of the letter E is block C8 = (49,90).

**Character I = 73 as the value of  $m_9$ .**

Then, we get the cipher text ( $a$ ,  $b$ ):

$a = g^k \bmod p = 72 \bmod 97 = 49$

$b = y^k m \bmod p = (492 \times 73) \bmod 97 = 91$

From the above calculation results, the cipher text of the letter E is block C9 = (49,91).

#### Character Z = 90 as the value of m10.

Then, we get the cipher text (a, b):

$$a = g^k \bmod p = 72 \bmod 97 = 49$$

$$b = y^k m \bmod p = (492 \times 90) \bmod 97 = 92$$

From the results of the above calculation, it is obtained that the cipher text of the letter E is block C10 = (49,71).

#### Character A = 65 as the value of m11.

Then, we get the cipher text (a, b):

$$a = g^k \bmod p = 72 \bmod 97 = 49$$

$$b = y^k m \bmod p = (492 \times 65) \bmod 97 = 89$$

From the results of the above calculation, it is obtained that the cipher text of the letter E is block C11 = (49,89).

#### The character R = 82 as the value of m12.

Then, we get the cipher text (a, b):

$$a = g^k \bmod p = 72 \bmod 97 = 49$$

$$b = y^k m \bmod p = (492 \times 82) \bmod 97 = 69$$

From the results of the above calculation, it is obtained that the cipher text of the letter E is block C12 = (49,69).

After getting the values of a and b, the calculation results are arranged in the following pattern: a1, b1, a2, b2, a3, b3, a4, b4, a5, b5, a6, b6, a7, b7, a8, b8, ...a12, b12 . Then obtained:

**Plaintext = ABDUL MEIZAR**

**Ciphertext=49,89,49,65,49,17,49,94,49,19,49,8,49,92,49,90,49,91,49,71,49,89,49,69.**

## 2. Decryption Process

A decrypts the cipher text of B by doing calculations with the keys used are  $p = 97$ ,  $g = 7$  and  $x = 2$ . So,  $y = gx \bmod p = 72 \bmod 97 = 49$ . Determine the value of k, in this case  $k = 2$ .

**Cipher text=**

**49,89,49,65,49,17,49,94,49,19,49,8,49,92,49,90,49,91,49,71,49,89,49,69.**

For the cipher text block  $(C^{-1}) = a, b$  with values  $a = 49$  and  $b = 89$ , the decryption process to produce plaintext is carried out by calculation using the formula  $a^{(p-1-x)} \bmod p$ , then proceed with the calculation with the formula  $b * (a^{(p-1-x)} \bmod p) \bmod p$ . Then the ASCII value will be obtained, change this value into the form of character values to get plaintext. For more details, see the following calculation.

**Ciphertext1(a,b) = (49,89)**

$$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$$

$$b * (a^{(p-1-x)} \bmod p) \bmod p = (89 \times 4) \bmod 97 = 65.$$

Convert the ASCII number 65 to the character i.e. m1 = "A".

**C2(a,b) = (49,65)**

$$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$$

$$b * (a^{(p-1-x)} \bmod p) \bmod p = (65 \times 4) \bmod 97 = 66.$$

Change the ASCII number 66 to the character i.e. m2 = "B".

**C3(a,b) = (49,17)**

$$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$$

$$b * (a^{(p-1-x)} \bmod p) \bmod p = (17 \times 4) \bmod 97 = 68.$$

Convert the ASCII 68 number to the character i.e. m3 = "D".

**C4(a,b) = (49,94)**

$$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$$

$$b * (a^{(p-1-x)} \bmod p) \bmod p = (94 \times 4) \bmod 97 = 85.$$

Convert the ASCII 85 number to the character i.e. m4 = "U".

**C5(a,b) = (49,19)**

$$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$$

$$b * (a^{(p-1-x)} \bmod p) \bmod p = (19 \times 4) \bmod 97 = 76.$$

Convert the ASCII number 76 to the character i.e. m5 = "L".

**C6(a,b) = (49,8)**

$$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$$

$$b * (a^{(p-1-x)} \bmod p) \bmod p = (8 \times 4) \bmod 97 = 32.$$

Convert the ASCII 32 number to the character i.e. m6 = "SPACE".

**C7(a,b) = (49,92)**

$$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$$

$$b * (a^{(p-1-x)} \bmod p) \bmod p = (92 \times 4) \bmod 77 = 76.$$

Change the ASCII number 77 to the character i.e. m7 = "M".

**C8(a,b) = (49,90)**

$$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$$

$$b * (a^{(p-1-x)} \bmod p) \bmod p = (90 \times 4) \bmod 77 = 69.$$

Change the ASCII number 69 to the character i.e. m8 = "E".

**C9(a,b) = (49,91)**

$$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$$

$$b * (a^{(p-1-x)} \bmod p) \bmod p = (91 \times 4) \bmod 77 = 73.$$

Change the ASCII number 73 to the character i.e. m9 = "I".

**C10(a,b) = (49,71)**

$$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$$

$$b * (a^{(p-1-x)} \bmod p) \bmod p = (71 \times 4) \bmod 77 = 90.$$

Convert the ASCII number 90 to the character i.e. m10 = "Z".

**C12(a,b) = (49,89)**

$$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$$

$$b * (a^{(p-1-x)} \bmod p) \bmod p = (89 \times 4) \bmod 77 = 65.$$

Convert the ASCII number 65 to the character i.e. m11 = "A".

**C13(a,b) = (49,69)**

$$a^{(p-1-x)} \bmod p = 49^{(97-1-2)} \bmod 97 = 4$$

$$b * (a^{(p-1-x)} \bmod p) \bmod p = (69 \times 4) \bmod 77 = 82.$$

Change the ASCII number 82 to the character i.e. m12 = "R".

After getting the value of the results of the decryption process, the calculations are arranged in a pattern: m1, m2, m3, m4, m5, m6, m7, m8, m9, m10, m11, m12.

Then obtained:

**Cipher text=**

**9,89,49,65,49,17,49,94,49,19,49,8,49,92,49,90,49,91,49,71,49,89,49,69.**

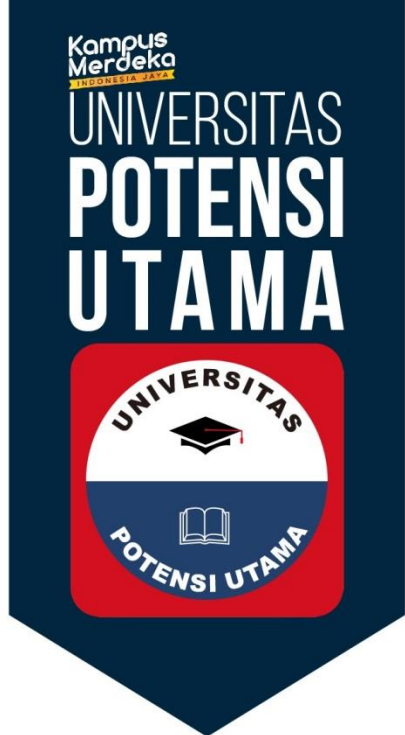
**plaintext = ABDUL MEIZAR**

## V. CONCLUSIONS

Based on the research and discussion conducted, the author can make the following conclusions that the stages of the research process regarding securing student databases at the Darul Hikmah Islamic Boarding School TPI Medan with an application designed using the Elgamal algorithm, it can be concluded that the Elgamal algorithm can be used to encrypt the contents and database files (cipher text) so that they cannot be read by data thieves, and can only be decrypted into the contents and the original database file (plaintext) if the password is entered correctly.

## REFERENCES

- [1]. V. Subbarao, K. Srinivas, and R. S. Pavithr, "A survey on internet of things based smart, digital green and intelligent campus," in *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 2019, pp. 1–6.
- [2]. A. Al-Harrasi, A. K. Shaikh, and A. Al-Badi, "Towards protecting organisations' data by preventing data theft by malicious insiders," *Int. J. Organ. Anal.*, 2021.
- [3]. R. O. Obe and L. S. Hsu, *PostgreSQL: up and running: a practical guide to the advanced open source database*. "O'Reilly Media, Inc.," 2017.
- [4]. E. S. I. Harba, "Secure data encryption through a combination of AES, RSA and HMAC," *Eng. Technol. Appl. Sci. Res.*, vol. 7, no. 4, pp. 1781–1785, 2017.
- [5]. V. Edy, "Optimizing the Confidentiality of Lecturer Database using Elgamal Algorithm," 2020.
- [6]. M. Al-Zubi and A. A. Abu-Shareha, "Efficient signcryption scheme based on El-Gamal and Schnorr," *Multimed. Tools Appl.*, vol. 78, no. 9, pp. 11091–11104, 2019.
- [7]. M. Kasianchuk, I. Yakymenko, S. Ivasiev, R. Shevchuk, and L. Tymoshenko, "The method of factorizing multi-digit numbers based on the operation of adding odd numbers," 2018.
- [8]. H. I. Hussein and W. M. Abdullallah, "An efficient ElGamal cryptosystem scheme," *Int. J. Comput. Appl.*, vol. 43, no. 10, pp. 1088–1094, 2021.
- [9]. D. Sow and M. G. Camara, "Provable security of the generalized elgamal signature scheme," *J. Math. Res.*, vol. 11, no. 6, pp. 1–77, 2019.
- [10]. A. Ali *et al.*, "Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography," *Sensors*, vol. 22, no. 2, p. 528, 2022.
- [11]. D. Karima and M. Lamine, "Two dimensional ElGamal public key cryptosystem," *Inf. Secur. J. A Glob. Perspect.*, vol. 28, no. 4–5, pp. 120–126, 2019.
- [12]. D. S. Gupta and G. P. Biswas, "Design of lattice-based ElGamal encryption and signature schemes using SIS problem," *Trans. Emerg. Telecommun. Technol.*, vol. 29, no. 6, p. e3255, 2018.
- [13]. P. Chinnnasamy, S. Padmavathi, R. Swathy, and S. Rakesh, "Efficient data security using hybrid cryptography on cloud computing," in *Inventive Communication and Computational Technologies*, Springer, 2021, pp. 537–547.
- [14]. S. Rani and H. Kaur, "Implementation and comparison of hybrid encryption model for secure network using AES and Elgamal," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 3, 2017.
- [15]. E. Jincharadze, "Hybrid Encryption Model of Symmetric and Asymmetric Cryptography with AES and Elgamal Encryption Algorithms," *Sci. Pract. cyber Secur. J.*, pp. 2587–4667, 2018.
- [16]. A. Sahasrabuddhe and D. S. Laiphrakpam, "Multiple images encryption based on 3D scrambling and hyper-chaotic system," *Inf. Sci. (Ny)*, vol. 550, pp. 252–267, 2021.
- [17]. Y. Luo, X. Ouyang, J. Liu, and L. Cao, "An image encryption method based on elliptic curve elgamal encryption and chaotic systems," *IEEE Access*, vol. 7, pp. 38507–38522, 2019.
- [18]. A. Abdaoui, A. Erbad, A. K. Al-Ali, A. Mohamed, and M. Guizani, "Fuzzy Elliptic Curve Cryptography for Authentication in Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9987–9998, 2021.
- [19]. A. Banik, Z. Shamsi, and D. S. Laiphrakpam, "An encryption scheme for securing multiple medical images," *J. Inf. Secur. Appl.*, vol. 49, p. 102398, 2019.
- [20]. M. S. Khoirom, D. S. Laiphrakpam, and T. Tuithung, "Audio encryption using ameliorated ElGamal public key encryption over finite field," *Wirel. Pers. Commun.*, vol. 117, no. 2, pp. 809–823, 2021.
- [21]. L. Tanti, Safrizal, M. A. E. Nasution, R. Puspasari, B. S. Riza, and J. Indriani, "Modeling of Decision Support System as an Assistant Tool in Selecting Health Equipment Suppliers with TOPSIS Method," 2021, doi: 10.1109/CITSM52892.2021.9588818.



# CERTIFICATE

Of Appreciation

**Proudly Presented To**

Rubianto, Roslina, Rika Rosnelly



As an Author with The Title:

Optimization of Student Database Confidentiality Using  
Elgamal Algorithm and Fermat Method

The 4<sup>th</sup> International Conference on Cybernetics  
and Intelligent System (ICORIS)

**ICORIS**  
**INTERNATIONAL  
CONFERENCE**

8<sup>th</sup> & 9<sup>th</sup> 2022, Hotel Khas Parapat - North Sumatera  
UNIVERSITAS POTENSI UTAMA - MEDAN - INDONESIA

**HOST**



**CO-HOST**



**SUPPORTED BY**



**Dr. Rika Rosnelly, S.Kom., M. Kom**  
Rector of Universitas Potensi Utama

**Dr. Ir. Djoko Soetarno, DEA**  
CORIS Advisor



**Heimi Kurniawan, M. Kom.**  
ICORIS Chairman