



ORIGINAL

Secure and Privacy Preserving Predictive Framework for Iot Based Health Cloud System Using Cryptographic Modfels

Marco predictivo seguro y que preserva la privacidad para un sistema de nube de salud basado en IoT que utiliza modfels criptográficos

Salim Davlatov¹ , Navruzbek Qurbonov² , Aziza Yunusova³ , Nodira Tursunova⁴ , Ra'no Narbekova⁵ , Akhmadjon Abdumaruf⁶ , Nadira Mirametova⁷ 

¹Bukhara State Medical Institute named after Abu Ali ibn Sino. Bukhara, Uzbekistan.

²Samarkand State Medical University, Uzbekistan.

³Samarkand State Medical University, Samarkand, Uzbekistan.

⁴Tashkent Medical Academy, Uzbekistan.

⁵Jizzakh state pedagogical university, Uzbekistan.

⁶Fergana Medical Institute of Public Health.

⁷Ajiniyaz Nukus State Pedagogical Institute.


Cite as: Davlatov S, Qurbonov N, Yunusova A, Tursunova N, Narbekova R, Abdumaruf A, et al. secure and privacy preserving predictive framework for iot based health cloud system using cryptographic modfels. Health Leadership and Quality of Life. 2024; 3:177. <https://doi.org/10.56294/hl2024.177>

Submitted: 25-02-2024

Revised: 18-06-2024

Accepted: 19-11-2024

Published: 20-11-2024

Editor: PhD. Prof. Neela Satheesh 

Corresponding author: Salim Davlatov 

ABSTRACT

People have been impacted by COVID-19 not just physically but also psychologically, and the epidemic has had a significant societal impact, particularly in underdeveloped nations. During such perplexing circumstances, there is undoubtedly a significant increase in psychosocial discomfort. On the other hand, more people are now seeking mental health assistance. The researcher identified a tool to help promote mental wellness and bring about a behavioural change in people's minds using the broaden and build theory of psychological wellness (Fredrickson 1998), with the goal of promoting positivity and mental well-being. This was done by utilising design research methodology and human centred design principles. Through the use of human-centered design, the study illustrated how issues can be found, verified, and their impact mitigated through the use of an intervention. In order to delve deeply into the problems that emerged during the COVID19 pandemic and ultimately lessen the psychological effects of a pandemic, the research will help the public in times of hardship and policy makers. By offering suitable, sympathetic insights and solutions in relation to human-centered design, and particularly in terms of design for the healthcare and wellness space, the study results also demonstrate further steps towards developing advanced design research during a psychosocial distress situation on people's mental wellness.

Keywords: COVID Pandemic; AI Intelligent; Chatbot; Deep Learning.

RESUMEN

La COVID-19 ha afectado a las personas no solo a nivel físico sino también psicológico, y la epidemia ha tenido un impacto social significativo, en particular en las naciones subdesarrolladas. En circunstancias tan desconcertantes, sin duda se produce un aumento significativo del malestar psicosocial. Por otro lado, ahora más personas buscan asistencia en materia de salud mental. El investigador identificó una herramienta para ayudar a promover el bienestar mental y generar un cambio de comportamiento en la mente de las personas utilizando la teoría de ampliar y construir el bienestar psicológico (Fredrickson 1998), con el objetivo de

promover la positividad y el bienestar mental. Esto se hizo utilizando la metodología de investigación de diseño y los principios de diseño centrado en el ser humano. Mediante el uso del diseño centrado en el ser servicios en la nube, incluidas bases de datos, aplicaciones y almacenamiento, a través de una red. El Internet de las cosas (IoT) ofrece una amplia gama de aplicaciones de campo para la monitorización continua en muchas industrias, incluida la atención médica. Se realizan numerosos estudios para garantizar la privacidad de los datos de los pacientes. Otro componente desafiante de los sistemas de salud es el uso de datos de pacientes de dispositivos IoT para predecir enfermedades. Proteger la información confidencial del acceso no autorizado es necesario para aumentar su seguridad. Para mejorar la privacidad de los datos en la nube, se han aplicado muchos algoritmos criptográficos clásicos. Sin embargo, persisten algunos problemas con la privacidad de los datos debido a su seguridad inadecuada. Como resultado, este artículo propone un método innovador para proteger la privacidad de los datos en la nube. El sistema de cifrado EGEC sugerido puede ser utilizado por los usuarios que poseen los datos para descifrar datos como, por ejemplo, operaciones de suma y multiplicación.

Palabras clave: Cifrado; Descifrado; Diabetes; Aprendizaje Automático.

INTRODUCTION

IoT gives businesspeople the tools to improve their business processes and challenges them to reevaluate how their companies are conducting business. IoT is widely used in manufacturing, transportation, and utility associations, allowing for the use of sensors and other IoT devices.⁽¹⁾ Nonetheless, it has furthermore added to electronic change for particular affiliations by settling utilise cases for partnerships in the agriculture, infrastructure, and home atomisation sectors. IoT in agricultural can benefit ranchers by streamlining their tasks.⁽²⁾ IoT can also be used in a number of other agricultural domains, including insect monitoring, irrigation, soil humidity monitoring, and water quality monitoring. Internet of Things (IoT) tools utilised in the agro sector include PIR sensors, ultrasonic range devices, and web cameras.⁽³⁾ Using IoT in agricultural has several major benefits, including cost effectiveness, optimising water use, and producing high-quality crops. Connectivity limitations, the difficulty of developing an IoT product, security concerns, and time and resource constraints are some of the challenges associated with IoT in agribusiness.⁽⁴⁾ The Internet of Things is being used in agriculture for a variety of purposes, including soil quality detection, weather monitoring, and crop monitoring.⁽⁵⁾ IoT technology aid in reducing waste and raising productivity for formers. From anywhere at any time, the formers can keep an eye on the field conditions.⁽⁶⁾ Every industry is impacted by the Internet of Things, including retail, finance, and medical services. An effective means of safeguarding interconnected IoT networks and devices is through IoT security.⁽⁷⁾ The primary obstacles to IoT security include financial and functional limitations, insufficient security knowledge, rapid implementation, and newly established markets.⁽⁸⁾ IoT network security, authentication, IoT encryption, and IoT API security are some of the emerging technologies that are employed to address the security issues in IoT. The most widely used IoT security technologies are Flutter, Eclipse IoT Project, and Node RED. unsecured web interfaces, inadequate authentication, unsecured mobile interfaces, insecure software, and inadequate physical security are the main IoT security problems with IoT devices.⁽⁸⁾ Numerous vulnerabilities exist in IoT, including poor authentication, unpatched vulnerabilities, and vulnerable APIs.⁽¹⁰⁾ DDoS attacks, botnet attacks, and malware-based attacks are a few significant IoT security threats. Wearable technology carries a significant risk in that it occasionally gathers a lot of personal data from users.⁽¹¹⁾ Unauthorised individuals can quickly learn the secret information. The typical IoT security vulnerabilities are guessable passwords, lack of network access security, insufficient privacy protection, and lack of device management.⁽¹²⁾ The primary hazard in IoT is hacking. For IoT users, privacy is still a big concern. Companies that produce and ship Internet of Things (IoT) gadgets to customers, for instance, occasionally utilise those devices to obtain and resell personal data. In addition to disclosing private information about specific individuals, IoT poses a threat to the foundation, which includes transportation, energy, and financial services.⁽¹³⁾ For this market to succeed, linked IoT devices must have end-to-end security. In order for all parties to be able to rely on a safe and reliable market, businesses must be in charge of integrating security from the beginning and at every point of the IoT value chain. The variety of the IoT industry necessitates a flexible security architecture and light-touch regulations that ensure market security while encouraging growth and successful IoT development. The mobile sector is best suited to create and execute a sufficient security framework that satisfies these needs because it has vast experience offering safe, dependable solutions.⁽¹⁴⁾

Research Objectives

Information may now be processed and saved by devices all around the world to be accessed at a later time thanks to the Internet of Things. To comprehend this potential possibility, though, is hindered greatly by the vast distance that exists between data collecting and processing/analysis capabilities.⁽¹⁵⁾ The newest innovation,

cloud computing linked with IoT, combines multiple internet-connected technologies to deliver applications in real-time across multiple environments and places. The health sector has profited greatly from the introduction of IoT, which is used for everything from treating chronic diseases to preventing various health disorders.⁽¹⁶⁾ The advent of cloud computing combined with IoT to the healthcare industry offers a number of advantages, such as high performance, virtualisation, scalability, and reliability.⁽¹⁷⁾ Healthcare resource sharing will be improved by the development and use of public clouds. It saves a tonne of running costs while building a very effective patient observation and control system. IoT also guarantees convenience for other healthcare tasks, such as patient tracking and monitoring.⁽¹⁸⁾ IoT devices gather healthcare data through remote access mechanisms that provide certain security and privacy problems. The sensor gathers data, which is then sent via the internet to cloud storage.⁽¹⁹⁾ Since the data is secured in one place, it creates security risks and allows for breaches and assaults. The introduction of IoT, key aspects, its framework, security needs for IoT, how to protect IoT devices, and various security threats on IoT have all been covered.⁽²⁰⁾ Connectivity, sensing, heterogeneity, and a dynamic environment are the key components of the Internet of Things. Some methods for safeguarding IoT devices were proposed in this study article, including hardware tamper resistance, failover design, device identity spoofing, and strong authentication. According to,⁽²¹⁾ IoT devices should meet certain basic security standards. The small size of multiple linked devices and limited processing power may cause problems for encryption and other strict security measures. Because of their size and the methods used to provide protection, people need to consider the disadvantages of devices.⁽²²⁾ The difficulties in implementing end-to-end security and embedded system protection are the findings of this study. The numerous surveys and technical evaluations on the subject of IoT applications in health cloud systems, cloud data privacy, and diabetes and heart disease prediction.⁽²³⁾ The proposal aims to use ElGamal elliptic curve homomorphic encryption to address privacy concerns with cloud data. In Internet of Things (IoT) based health cloud systems, the HERDE MSNB approach is also utilised to guarantee security and disease prediction.

The organization of the remaining sections is as follows: section 2 provides an informative survey on related works pertaining to the role of IoT in the health care system, in Section 3 provides the implementation of a privacy-preserving IoT based health cloud system. Section 4 presents the findings and discussion of the proposed model, and Section 5 concludes the work.

Proposed system

Disease overview

Diabetes condition poses major health hazards since it prevents different areas of the body from obtaining energy from meals. Diabetes is a condition when the blood's amount of insulin rises. For diabetic people, a threshold value of 126 milligrammes per decilitre (mg/dL) is deemed dangerous. It is a natural occurrence for food particles consumed by humans to be transformed into glucose and combined with blood. When food is broken down by the human digestive system, the blood glucose level rises. The body's cells will use the sugar combined with blood to provide energy for the human body. The pancreas produces insulin, which is used in the aforementioned process.⁽²⁴⁾ India is referred to as the global hub for diabetes, with data showing that 50 billion people worldwide suffer from the disease. India is therefore having difficulty overcoming the situation. Nevertheless, the medical analysts suggested that diabetic people can overcome their condition and enjoy normal lives if they make the correct early forecast and decision. India is the nation with the greatest number of diabetic patients, and we also have a serious health problem there. According to the World Health Organisation (WHO), excessive blood sugar caused 3,5 million deaths in India.

Proposed Framework

The cloud is currently the IT industry's fastest-emerging technology. The cloud allows us to store and retrieve data. Data security and privacy preservation are the most common issues in the cloud. Protecting confidential information from unauthorised access is necessary to increase its security. To improve privacy while protecting cloud data, a variety of conventional cryptographic techniques have been applied. However, because of its lower security, there are still certain issues with privacy protection.⁽²⁵⁾ Therefore, this chapter proposes an ElGamal Elliptic Curve (EGEC) homomorphic encryption strategy to protect cloud-stored data secrecy. The ElGamal Elliptic Curve (EGEC), a novel and effective technique, is presented in this study to protect the privacy. Examine the multi-cloud model depicted in figure 1 in this context. It combines the capabilities of public and private clouds. User data is encrypted and kept in a private cloud using the EGEC technique. Data saved in a public cloud is shared via cloud storage and is accessible with restricted access through the use of an access policy. The homomorphic scheme is actually an algorithm for symmetric cryptography. However, the suggested method implements the homomorphic scheme as an imbalanced cryptography computation since EGEC is modified in accordance with the homomorphic scheme's capabilities and makes use of a 512-digit key size. This approach takes advantage of a multi-cloud environment to securely store and retrieve data while addressing a number of security issues, such as data integrity and management accessibility. The client

requests access to information held in distributed storage by sending a solicitation. In order to restrict access to cloud data, the cloud server verifies the specifics of the entry plan. After access is restricted, keys are generated. Using a technique known as message encoding, messages are addressed as Elliptic bend focusses in this study. ElGamal Elliptic Bend (EGEC) Homomorphic Encryption is used to jumble these focusses. Thus, the disorganised concentrations undergo a fully homomorphic process before being dispatched to the designated customer.^(26,27) Finally, the homomorphic systems and ElGamal Elliptic Bend (EGEC) decoding technique are used to produce a unique point. The final stage in communicating the Elliptic bend focusses into a message is message interpretation. The suggested approach takes advantage of a multi-cloud environment to ensure the security of cloud information. Consider a clinic for medical purposes. The information owner is the medical clinic overseer, who can manage the entire security system, assign tasks to clients, and maintain each client's unique secret phrase. The cloud service provider (CSP) acts as a go-between for the data user and the hospital administration. Among the people who use data in a hospital context are doctors, nurses, patients, and receptionists. The cloud server checks the request's access policy each time a user submits a request to access data stored in the cloud before allowing the user access authorisation to obtain the needed data from the cloud.

Significant age inside A calculation is utilized in cryptography to create keys. Produced keys are generally utilized for information encryption and decoding. The most common way of changing over a message into elliptic bend focusses is known as message encoding. Plans using the ElGamal Elliptic Bend (EGEC) can encode and decode explicit focusses on the elliptic bend – not text information that is placed. Consider an information instant message to be encoded in the recommended manner. The info message is separated into fixed-size blocks, with one person making up each block. Then, an ASCII esteem is doled out to each person in a text, and these qualities are then straightforwardly planned to the focusses on an elliptic bend. The most common way of transforming figure text into plain text is called unscrambling. The recommended work includes the extraction of the code point from the scrambled point by homomorphic calculation, like expansion or augmentation activities.^(28,29)

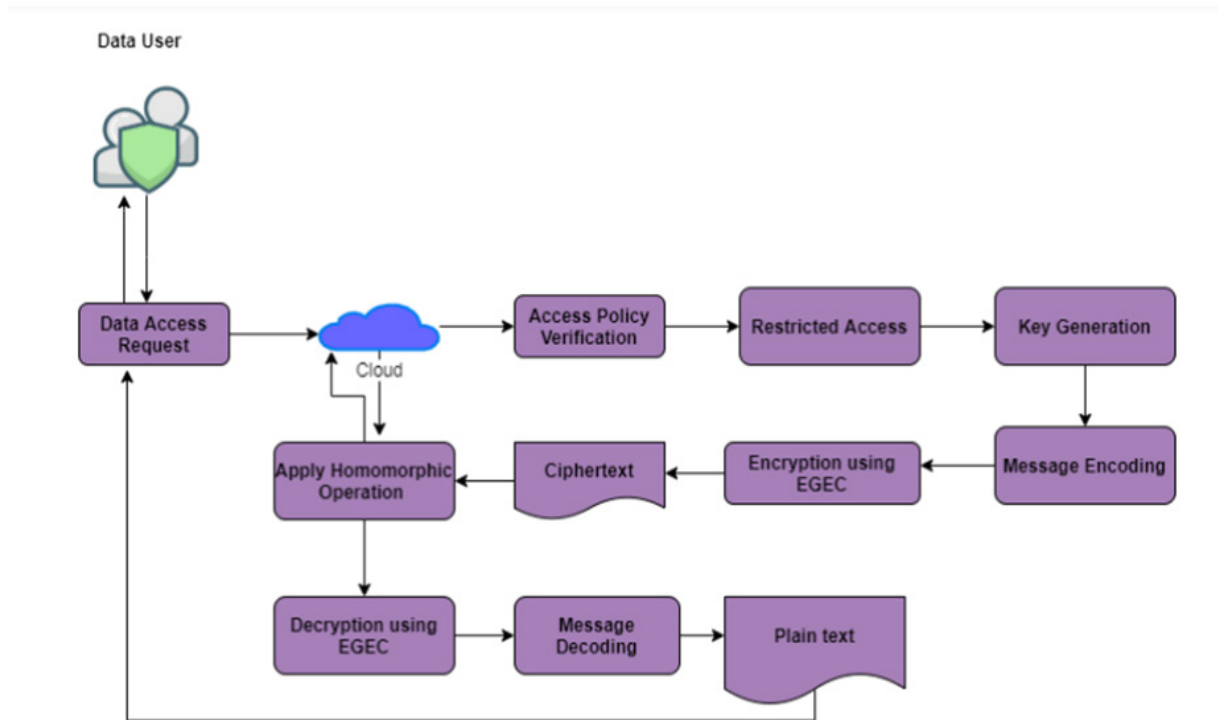


Figure 1. Proposed Framework

RESULTS AND DISCUSSION

One well-known open-source cloud operating system that supports many cloud settings is called OpenStack. The host computer must have at least two gigabytes of RAM, twenty gigabytes of disc space, Internet access, and a processor with hardware virtualisation extensions. The Java programming language has been used to implement the suggested EGEC scheme.

An extensive variety of execution boundaries, including execution time, encryption and decoding time, memory use, and encryption and unscrambling throughput, are utilized to assess the trial results for both existing and new frameworks. Framework activity for randomisation and encryption (MORE) and polynomial activity for randomisation and encryption (PORE) are the ebb and flow approaches used in this exploration attempt.

How much time expected by the technique to change over plain text into figure text as well as the other way around in distributed storage is known as execution time. Figure 2 thinks about the execution seasons of the proposed EGEC conspire and the flow frameworks in light of various key sizes.

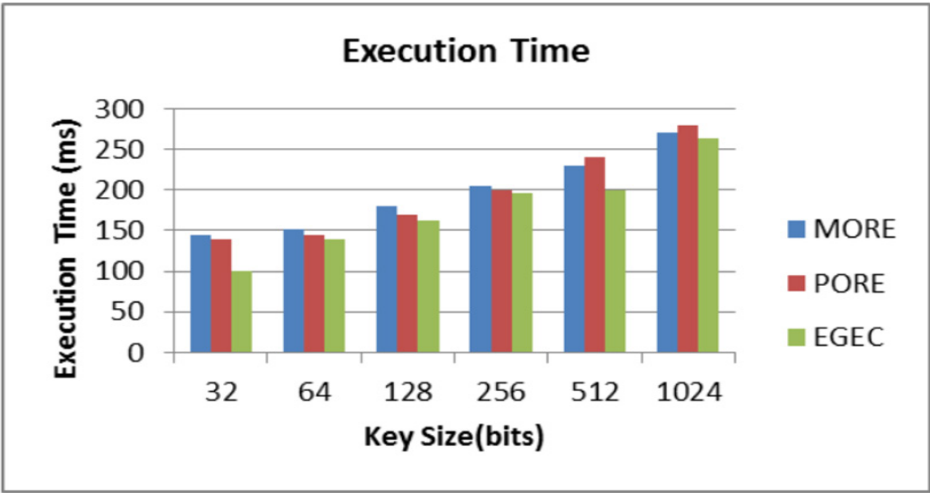


Figure 2. Comparison of Execution Time

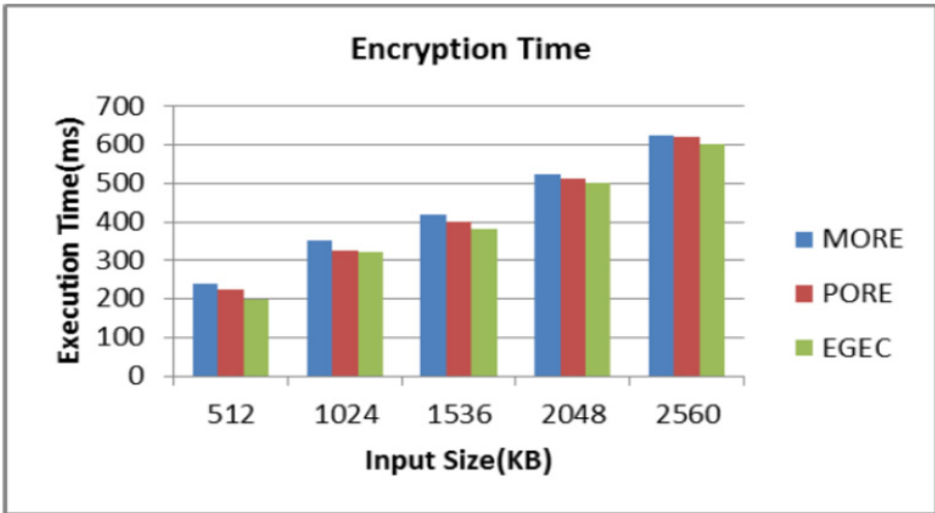


Figure 3. Comparison of Encryption Time

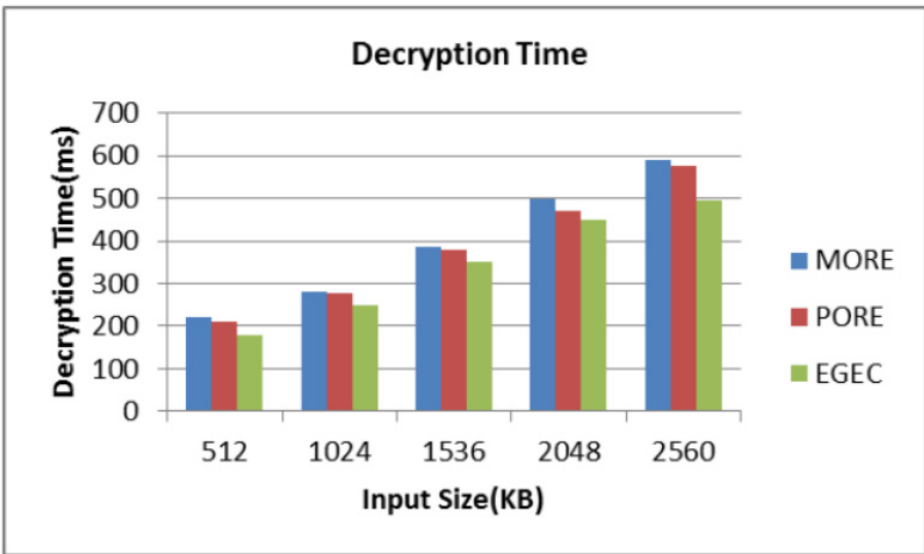


Figure 4. Comparison of Decryption time

The time it takes the calculation to interpret the encoded content once more into plain text is known as the unscrambling time. One more method for communicating the unscrambling time is in milliseconds. Figure 4 looks at the decoding seasons of the proposed EGEC conspire with the current methods.

The timeframe the calculation takes to change the information text into figure text is known as the encryption time. Milliseconds can be utilized to communicate the encryption time. Figure 3 analyzes the encryption seasons of the recommended EGEC plot with the momentum plans.

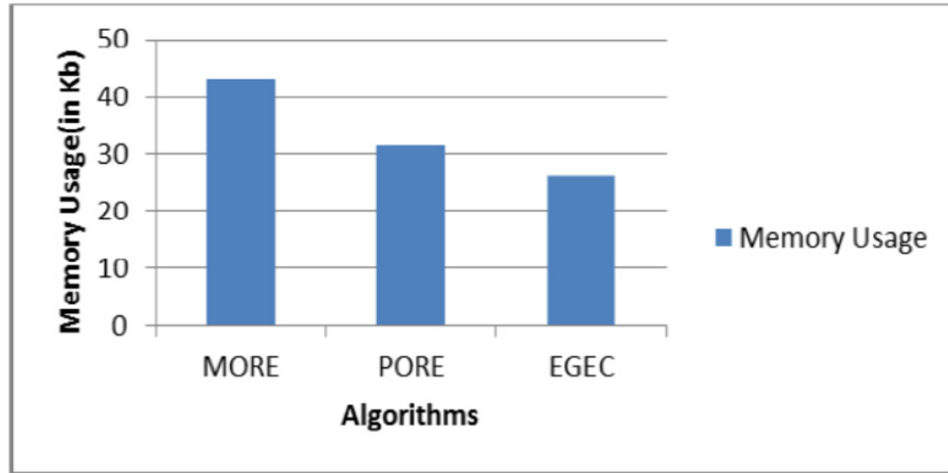


Figure 5. Comparison of Memory Usage

The amount of memory expected to execute the encryption and decoding calculations is known as memory usage. The ongoing methodology involves 43,2 KB of Smash for MORE and 32,8 KB for PORE. In 26,2 KB of memory, the recommended EGEC homomorphic framework was executed. The memory use of the MORE, PORE, and proposed EGEC homomorphic procedures is portrayed in Figure 5. As per the memory utilization investigation, the EGEC Homomorphic technique, which we introduced, requires less memory.

CONCLUSIONS

Secure cloud information is guaranteed by the proposed ElGamal Elliptic bend homomorphic encryption. Six unmistakable cycles make up the proposed EGEC homomorphic encryption: key age, message encoding, EGEC encryption, EGEC unscrambling, and message deciphering. At the point when a client demands admittance to information put away in the cloud, the CSP checks their consent of access. EGEC homomorphic encryption is utilized by the information proprietor to encode the information. On scrambled information, the homomorphic activity is done. The first message is acquired by applying the EGEC unscrambling procedure. The ElGamal Elliptic bend homomorphic encryption framework that has been proposed is analyzed as far as execution time, encryption time, unscrambling time, memory utilization, and throughput for both encryption and decoding. Examinations are made between the proposed EGEC homomorphic encryption plan and current plans like MORE and PORE.

REFERENCES

1. Kumar, P. Praveen, T. Ananth Kumar, R. Rajmohan, and M. Pavithra. "AI-based robotics in E-healthcare applications." In *Intelligent Interactive Multimedia Systems for E-Healthcare Applications*, pp. 249-269. Apple Academic Press, 2022.
2. Janani, S., R. Dilip, Suryansh Bhaskar Talukdar, Veera Bhaskar Talukdar, Krishna Nand Mishra, and Dharmesh Dhabliya. "IoT and Machine Learning in Smart City Healthcare Systems." In *Handbook of Research on Data-Driven Mathematical Modeling in Smart Cities*, pp. 262-279. IGI Global, 2023.
3. Sinha, Ambarish Kumar, and Gaurav Kumar. "Artificial Intelligence in Healthcare and Its Application in Brain Stroke Diagnosis." In *Bioinformatics Tools and Big Data Analytics for Patient Care*, pp. 91-104. Chapman and Hall/CRC, 2022.
4. Pattnayak, Parthasarathi, Sanghamitra Patnaik, Arpeeta Mohanty, and Tulip Das. "Application of E-Healthcare Based on Machine Learning in an Internet of Things Ecosystem." In *2023 3rd International Conference on Innovative Sustainable Computational Technologies (CISCT)*, pp. 1-5. IEEE, 2023.

5. Chaturvedi, Shivi. "Clinical prediction on ML based internet of things for E-health care system." *International Journal of Data Informatics and Intelligent Computing* 2, no. 3 (2023): 29-37.
6. Tenepalli, Deepika, and Navamani TM. "A systematic review on IoT and machine learning algorithms in e-healthcare." *International Journal of Computing and Digital Systems* 16, no. 1 (2024): 279-294.
7. Kumar, Shailesh, Rohini Srivastava, Shashwat Pathak, and Basant Kumar. "Cloud-based computer-assisted diagnostic solutions for e-health." In *Intelligent Data Security Solutions for e-Health Applications*, pp. 219-235. Academic Press, 2020.
8. Das, Sima, Jaya Das, Subrata Modak, and Kaushik Mazumdar. "Internet of things with machine learning-based smart cardiovascular disease classifier for healthcare in secure platform." In *Internet of Things and Data Mining for Modern Engineering and Healthcare Applications*, pp. 45-64. Chapman and Hall/CRC, 2022.
9. Adewole, Kayode S., Abimbola G. Akintola, Rasheed Gbenga Jimoh, Modinat A. Mabayoje, Muhammed K. Jimoh, Fatima E. Usman-Hamza, Abdullateef O. Balogun, Arun Kumar Sangaiah, and Ahmed O. Ameen. "Cloud-based IoMT framework for cardiovascular disease prediction and diagnosis in personalized E-health care." In *Intelligent IoT systems in personalized health care*, pp. 105-145. Academic Press, 2021.
10. Sworna, Nabila Sabrin, AKM Muzahidul Islam, Swakkhar Shatabda, and Salekul Islam. "Towards development of IoT-ML driven healthcare systems: A survey." *Journal of Network and Computer Applications* 196 (2021): 103244.
11. Khatun, Mirza Akhi, Sanobar Farheen Memon, Ciarán Eising, and Lubna Luxmi Dhirani. "Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation." *IEEE Access* (2023).
12. Santhosh, V., and E. Pandiyan. "Heart Disease Identification Method Using Machine Learning Classification in E Healthcare."
13. Sharma, Yojana, Shashwati Ray, and Om Prakash Yadav. "Applications of Machine Learning Algorithms in Fetal ECG Enhancement for E-Healthcare." In *Intelligent Interactive Multimedia Systems for e-Healthcare Applications*, pp. 199-222. Apple Academic Press, 2022.
14. Jayachitra, S., A. Prasanth, S. Hariprasath, R. Benazir Begam, and M. Madijagan. "AI enabled internet of medical things in smart healthcare." In *AI models for blockchain-based intelligent networks in IoT systems: Concepts, methodologies, tools, and applications*, pp. 141-161. Cham: Springer International Publishing, 2023.
15. Karthikeyan, B., K. Nithya, Ahmed Alkhayyat, and Yousif Kerrar Yousif. "Artificial Intelligence Enabled Decision Support System on E-Healthcare Environment." *Intelligent Automation & Soft Computing* 36, no. 2 (2023).
16. Khalikova, R., Jumaeva, F., Nazarov, A., Akmalova, M., Umarova, F., Botirov, E., Khaydarova, L., & Abduraimova, M. (2024). Integrating environmental conservation and sustainability into coal mining education. *Archives for Technical Sciences*, 2(31), 259-268. <https://doi.org/10.70102/afts.2024.1631.259>
17. Sushma, S., Mani, R., Perumalraja, R., Vasanthan, R., & Mohamed, A. (2024). Accounting Information Systems for Strategic Management: The Role of Intellectual Capital in Mediating the Relationship between Customer, Company, and Performance. *Indian Journal of Information Sources and Services*, 14(2), 160-166. <https://doi.org/10.51983/ijiss-2024.14.2.23>
18. Teshabaeva, D., Umarova, M., Babadjanova, N., Pulatova, M., Pardaev, A., Khidirov, O., Kamolova, S., & Turabayeva, Z. (2024). Architectural innovations of the medieval era through structural and material advancements. *Archives for Technical Sciences*, 2(31), 340-350. <https://doi.org/10.70102/afts.2024.1631.340>
19. Raj, D. S., & Dharmaraj, A. (2024). Rural Women's Saving and Investment Habits: A Study with Special Reference to Kuttampuzha Area, Ernakulam District. *Indian Journal of Information Sources and Services*, 14(3), 39-44. <https://doi.org/10.51983/ijiss-2024.14.3.06>
20. Almudhafar, R. Z., Almudhafar, S. M., & Almayahi, B. A. (2024). Environmental characteristics in Al-

manathira district and its spatial relationship in the distribution of livestock. Archives for Technical Sciences, 2(31), 359-367. <https://doi.org/10.70102/afts.2024.1631.359>

21. Gonzales, A. V. D., López, R. J. C., Neyra-Panta, M. J., Calderón, E. A. B., Rojas, C. Q. H., & Vela, J. R. (2024). Neuromarketing Applied in Organizations: A Scientific Production Study. Indian Journal of Information Sources and Services, 14(4), 35-41. <https://doi.org/10.51983/ijiss-2024.14.4.06>

22. Khakimov, O., Ortiqov, O., Ramazanov, N., Okbutaev, B., Mukhammadieva, O., Abdinazarov, U., Khamidov, A., & Khudoymurodova, K. (2024). Unveiling geological history through stratigraphy and mineralogy. Archives for Technical Sciences, 2(31), 305-310. <https://doi.org/10.70102/afts.2024.1631.305>

23. Sakib Biswas, M. (2023). Pleasure Reading and the Role of Libraries: A Review of the Literature. Indian Journal of Information Sources and Services, 13(1), 32-38. <https://doi.org/10.51983/ijiss-2023.13.1.3537>

24. Bošković, I., Đukić, D., Mašković, P., Mandić, L., Perović, S., Govedarica Lučić, A., & Malešević, Z. (2018). Mineral Composition of Plant Extracts from the Family Boraginaceae. Archives for Technical Sciences, 2(19), 85-90.

25. Imam, A., & Ilori, M. E. (2022). Challenges of Reprographic Information Resources within the Library and Some Selected Private Business Centers in Three Universities in Ogun State, Nigeria. Indian Journal of Information Sources and Services, 12(2), 10-15. <https://doi.org/10.51983/ijiss-2022.12.2.3236>

26. Saidova, K., & et al. (2024). Developing framework for role of mobile app in promoting aquatic education and conservation awareness among general people. International Journal of Research and Environmental Studies. 4. 58-63. <https://doi.org/10.70102/IJARES/V4S1/10>.

27. Saidova, K., & et al. (2024). Assessing the Economic Benefits of Climate Change Mitigation and Adoption Strategies for Aquatic Ecosystem. International Journal of Research and Environmental Studies. 4. 20-26. <https://doi.org/10.70102/IJARES/V4S1/4>.

28. Saidova, K., & et al. (2024). Assessing the impact of invasive species on native aquatic ecosystems and developing management strategies. International Journal of Research and Environmental Studies. 4. 45-51. <https://doi.org/10.70102/IJARES/V4S1/8>.

29. Ebenezar, U. S., Vennila, G., Balakrishnan, T. S., & Krishnan, P. (2024, June). Optimizing Healthcare Delivery through CloudBased Clinical Decision Support Systems. In 2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0 (pp. 1-6). IEEE. <https://doi.org/10.1109/OTCON60325.2024.10687659>

30. Mitra, A., Ammu, V., Chowdhury, R., Kumar, P., & Glory, E. (2024, August). An Adaptive Cloud and Internet of Things-Based Disease Detection Approach for Secure Healthcare system. In 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-7). IEEE. <https://doi.org/10.1109/IACIS61494.2024.10721944>

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Salim Davlatov, Navruzбек Qurbonov, Aziza Yunusova, Nodira Tursunova, Ra'no Narbekova, Akhmadjon Abdumaruf, Nadira Mirametova.

Data curation: Salim Davlatov, Navruzбек Qurbonov, Aziza Yunusova, Nodira Tursunova, Ra'no Narbekova, Akhmadjon Abdumaruf, Nadira Mirametova.

Formal analysis: Salim Davlatov, Navruzбек Qurbonov, Aziza Yunusova, Nodira Tursunova, Ra'no Narbekova, Akhmadjon Abdumaruf, Nadira Mirametova.

Research: Salim Davlatov, Navruzбек Qurbonov, Aziza Yunusova, Nodira Tursunova, Ra'no Narbekova, Akhmadjon Abdumaruf, Nadira Mirametova.

Methodology: Salim Davlatov, Navruzбек Qurbonov, Aziza Yunusova, Nodira Tursunova, Ra'no Narbekova, Akhmadjon Abdumaruf, Nadira Mirametova.

Project management: Salim Davlatov, Navruzбек Qurbonov, Aziza Yunusova, Nodira Tursunova, Ra'no Narbekova, Akhmadjon Abdumaruf, Nadira Mirametova.

Resources: Salim Davlatov, Navruzбек Qurbonov, Aziza Yunusova, Nodira Tursunova, Ra'no Narbekova, Akhmadjon Abdumaruf, Nadira Mirametova.

Software: Salim Davlatov, Navruzбек Qurbonov, Aziza Yunusova, Nodira Tursunova, Ra'no Narbekova, Akhmadjon Abdumaruf, Nadira Mirametova.

Supervision: Salim Davlatov, Navruzбек Qurbonov, Aziza Yunusova, Nodira Tursunova, Ra'no Narbekova, Akhmadjon Abdumaruf, Nadira Mirametova.

Validation: Salim Davlatov, Navruzбек Qurbonov, Aziza Yunusova, Nodira Tursunova, Ra'no Narbekova, Akhmadjon Abdumaruf, Nadira Mirametova.

Display: Salim Davlatov, Navruzбек Qurbonov, Aziza Yunusova, Nodira Tursunova, Ra'no Narbekova, Akhmadjon Abdumaruf, Nadira Mirametova.

Drafting - original draft: Salim Davlatov, Navruzбек Qurbonov, Aziza Yunusova, Nodira Tursunova, Ra'no Narbekova, Akhmadjon Abdumaruf, Nadira Mirametova.