Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.028548
Article

Tech Science Press

Data Mining with Privacy Protection Using Precise Elliptical Curve Cryptography

B. Murugeshwari[1,*], D. Selvaraj[2], K. Sudharson[3] and S. Radhika[4]

[1]Department of Computer Science and Engineering, Velammal Engineering College, Chennai, 600066, India
[2]Department of Electronics and Communication Engineering, Panimalar Engineering College, Chennai, 600123, India
[3]Department of Information Technology, Velammal Insitutue of Technology, Chennai, 601204, India
[4]Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, 600124, India
*Corresponding Author: B. Murugeshwari. Email: murugeshwariniyansree@gmail.com
Received: 12 February 2022; Accepted: 18 March 2022

Abstract: Protecting the privacy of data in the multi-cloud is a crucial task. Data mining is a technique that protects the privacy of individual data while mining those data. The most significant task entails obtaining data from numerous remote databases. Mining algorithms can obtain sensitive information once the data is in the data warehouse. Many traditional algorithms/techniques promise to provide safe data transfer, storing, and retrieving over the cloud platform. These strategies are primarily concerned with protecting the privacy of user data. This study aims to present data mining with privacy protection (DMPP) using precise elliptic curve cryptography (PECC), which builds upon that algebraic elliptic curve in finite fields. This approach enables safe data exchange by utilizing a reliable data consolidation approach entirely reliant on rewritable data concealing techniques. Also, it outperforms data mining in terms of solid privacy procedures while maintaining the quality of the data. Average approximation error, computational cost, anonymizing time, and data loss are considered performance measures. The suggested approach is practical and applicable in real-world situations according to the experimental findings.

Keywords: Data mining; cryptography; privacy preserving; elliptic curve; information security

1 Introduction

Data extraction or mining is a technique for extracting knowledge from existing databases. Those datasets are currently spreading around the globe. Because dispersed data must be obtained from many places and stored in the central repository, secure communication and secrecy are required. The transferred dataset includes personal or business secrets that must be protected. Data mining technology includes tools for instantly and effectively transforming massive amounts of data into wisdom appropriate to user's needs. Unfortunately, using data mining skills to obtain sensitive personal data jeopardizes their privacy rights.

Furthermore, data mining tools might provide crucial details about company activities. As a result, there is a strong demand to avoid the exposure of personal private details and the transmission of essential data in a particular environment. The focus of a current study project is on data mining privacy. As a result, the academic community has created a novel class of data extraction methodologies called privacy-preserving data mining (PPDM). These strategies aim to obtain information from a central repository while maintaining secrecy. As described in [1], several PPDM strategies have evolved over the centuries; however, there is no uniformity in these strategies. Data mining that preserves privacy often uses various approaches to alter the actual data or information created (measured, extracted) by data mining technologies. Five characteristics or dimensions must consider getting optimal outcomes while preserving the confidentiality of personal information. These aspects include (1) simple data dispersion, (2) how general information altering, (3) which extraction technique utilizing, (4) if basic information or principles conceal, and (5) whether different privacy protection mechanisms are employed. This review demonstrates how various approaches and strategies employs in the framework of PPDM from a technological standpoint.

Cloud technology has resulted in a significant shift in asset use by treating resources as a service that a cloud consumer may acquire out of any location at any time [2]. End usage of cloud technology takes advantage of the latest cloud services without recognizing their specific location, allowing for better data processing and storing [3–5]. This cloud infrastructure also opens up the possibility of establishing and maintaining cloud resources without spending extra funds, emphasizing the need for high-capacity network access [6–8]. The cloud technology also requires exchanging that information regularly, regardless of where it is kept in the multi-cloud architecture [9]. The bulk of the published idea in the research for assuring security has shown that anonymity is an excellent strategy for maintaining security and eliminating the significant burden in cloud data distribution [10–12]. In contrast, they found the cost of identity production and confirmation to be higher during the integrity assurance anonymous procedure implementation.

Nowadays, most businesses have various data feeds spread across various places that must examine to produce intriguing patterns and regularities. Instead of sending information to be extracted, that is probable to be quite large, mining the frequent patterns at various sources and forwarding the standards to a central authority. It is appropriate to combat various databases (where information is just to be extracted and dispersed between many relations on the different database management systems). Text mining claims to uncover previously undisclosed information. If the data is personalized or business, it can divulge information that others consider confidential. In the current scenario, Devise k-anonymity categorization, grouping, and association rules to ensure PPDM. Privacy issues are growing as text mining becomes more widespread in today's world. Companies gain personal data for their purposes. It may be necessary for various divisions inside an institution to transmit messages. Each company should not breach personal liberty and divulge confidential business data.

We offer a cryptographic technique for ensuring the privacy of private information in this work. We employed PECC based on elliptic curves. At an acceptable computational and communication cost, our technique ensures security and privacy at a given degree against parties concerned and the attacker. The remaining article layout is as follows: Chapter 2 covers some background information. Then, chapter 3 describes several essential principles utilized in our suggested strategy, while chapter 4 provides a complete discussion of the suggested framework. Next, we discuss the analysis of the suggested method in Section 5. Finally, in last chapter 6, we conclude and set a few goals for the future.

2 Related Works

The author of [13] uses Elliptical Curve Cryptography (ECC) to provide layered security controls for a Defense messaging service. The system uses intrinsic qualities of Elliptic encryption. The system built is safe, multi-site, and enables worldwide communication. It also shows that ECC has a higher level of

security while using fewer bits and is faster than other techniques. By analyzing the energy usage of ECC processors on Field Programmable Gate Arrays (FPGA), the researcher in [14] conducted tests on side-channel threats and ECC systems that employ bitwise techniques. A side-channel threat uses to estimate the private key for encrypting and decrypting by observing physical variations in device adverse effects. The side-channel exploitation test in this paper was 100 percent effective in obtaining the key by measuring the power requirements of the ECC processing unit. According to the ever-increasing need for gadget compression and task scheduling for situations in ECC with storage, throughput, and computing constraints, the researcher in [15], has identified a massive opportunity for future study.

The Ciphertext Policy-Based Encryption (CPBE) approach [16] used a dependable reputation supervisor to control the credentials and their qualities, assuring the device's potential security. This CPBE system also included considerable authority to make revoking and encrypting more efficient. The ciphertext policy's intricacy shows to be outstanding in assuring proper privacy protection in file storage clouds. Then, a privacy protection strategy related to information quality and security affords for using the intrinsic properties of congestion mending and high availability. Syam Kumar et al. [17] suggested an effective and convenient privacy-preserving solution for cloud services in multi-cloud technology. In the cloud, the probabilistic cryptosystem approach can retrieve the documents, encrypt data, and prioritize text search on that encrypted data. This strategy's primary goal is to encrypt information in the cloud while maintaining data confidentiality effectively. Unfortunately, this method fails to provide effective and robust data processing and prioritizes text search over encrypted information.

Aldeen et al. [18] introduced a new anonymizing approach for periodic and dispersed information on cloud technology to achieve greater confidentiality with enormous data usefulness. It discovered that high-value information on cloud technology provided more excellent privacy protection. They use the gradual anonymizing approach to strengthen the safety of cloud storage. The anonymized information was merged into the cloud systems using the privacy protection metric and other metrics such as storage and computational. Huang et al. [19] presented a safe and confidential digital management method to make content trade and distribution easier. This approach used homomorphic and enabled content providers to send encrypted files to a centralized content server. It also lets the user acquire material using the license server's licenses.

Furthermore, a safe contents key exchange strategy develops using proxy re-encryption and homomorphic encryption probability encryption keys. This system also ensured privacy by keeping people secret about the service supplier and critical servers. However, the method's main downside is its high level of intricacy. In [20] suggested a technique for privacy-preserving spectrum calculation in a two-party fully decentralized manner dependent on an elliptic curve analog of EIGamal cryptography. They conducted various experiments to investigate the novel solution's efficiency. Their approach has lower computational costs than the previous protocol. The findings of the experiments reveal that their approach is practical.

Furthermore, their suggested technique created PPDM solutions that were both private and efficient while maintaining excellent accuracy. In [21], there is a trade-off among these two aspects, with one sacrificing usefulness favoring another. As a result, data unloaded or accessible over cloud applications must preserve both usefulness and confidentiality. They created a utility privacy paradigm that used Deep Adaptive Clustering (DAC) to create utility and the Elliptic Curve Digital Signature Algorithm (ECDSA) to accomplish privacy. The application works by grouping the input information with DAC and keeping the data private with ECDSA. The model performs on introducing precise to assess the model's effectiveness, and the findings show increased clustering accuracy and effective confidentiality metrics compared to previous approaches.

The records evaluate to gather techniques to create the transitioning datasets in [22] this proposed strategy. These records collect information to select response data for encrypting and decrypting. The

input value determines the response data chosen technique. The data growth includes arriving at the threshold limit for the cumulative sustaining discharge. Data are sensitive to an ECC system that encrypts the data for isolation. For securing cloud data, Data encryption storage technology regulations they use. Encoding all transitory data sets is neither efficient nor capable. According to the testing results, the isolation defense cost of transitioning datasets may be significantly compressed by our approach over available ones when the complete datasets are encoded. In light of this, this research [23] developed a practical privacy-preserving data gathering approach with high availability in the smart grid. The suggested approach is lightweight, symmetrical homomorphic encryption and elliptic cryptography. The suggested approach can still receive information even if certain smart meters are damaged. Furthermore, the suggested data aggregation approach has been proven secure, and it meets all security standards. Finally, the suggested scheme's performance assessment demonstrates its minimal computing expense and transmission delay compared to other relevant systems [24–27].

3 Proposed Work

3.1 Design Goals

The PECC privacy-preserving should fulfill the minimum security and privacy issues in an unprotected transmission medium among collaborating sites:

1) No network must be capable of learning something about other encompassing channels;
2) Opponents should never be capable of affecting the security and privacy of the communicating entities or even the worldwide mining outcome by tracking the line of communication among engaging channels, and
3) It must have low computing power and cost.
4) To protect individual private details, it must have precise information with minimum noise.

3.2 System Model

Fig. 1 depicts the innovative structure. This integrated architecture slices into three parts. Before data send to the Central Repository, the initial process involves identifying precise data providers and encrypting them with PECC. The next step is to decryption sent from multiple data sources to transform. The process of transforming data into acceptable content for Central Repository is conversion. It also entails data cleansing and consolidation. Then, the processed data putting into the next stage. The last stage is the DMPP technique [28], which employs data warping to safeguard the confidentiality of personal data.

3.3 Data Preparation (Phase I)

Before the privacy protection, there are processes to preparing the data. Data Preparation is ready directly after receiving the data from the various data source in this situation. Data cleaning or any consolidation of information conducted during the early operations. For example, we have data with dependent dimensions in one property, and we need to transform them into three characteristics while removing the asterisks. *Data Preparation* is a notion used before implementing any iterative approach and is only used once during the operation [29–31].

Above Fig. 2 depicts accuracy and precision about data, must categorize data from various sources before moving on to the cloud storage. Precision refers to how fast, measurable values about one another and how many decimal digits are present in the entire measuring. Precise is crucial. The accuracy of a test value refers to how near it is to the genuine value. Precision is essential, but it is even better when precise and accurate observations. Once we obtain the precise data set from phase 1 after cleaning and consolidation, we move on to the phase 2, the PECC phase.

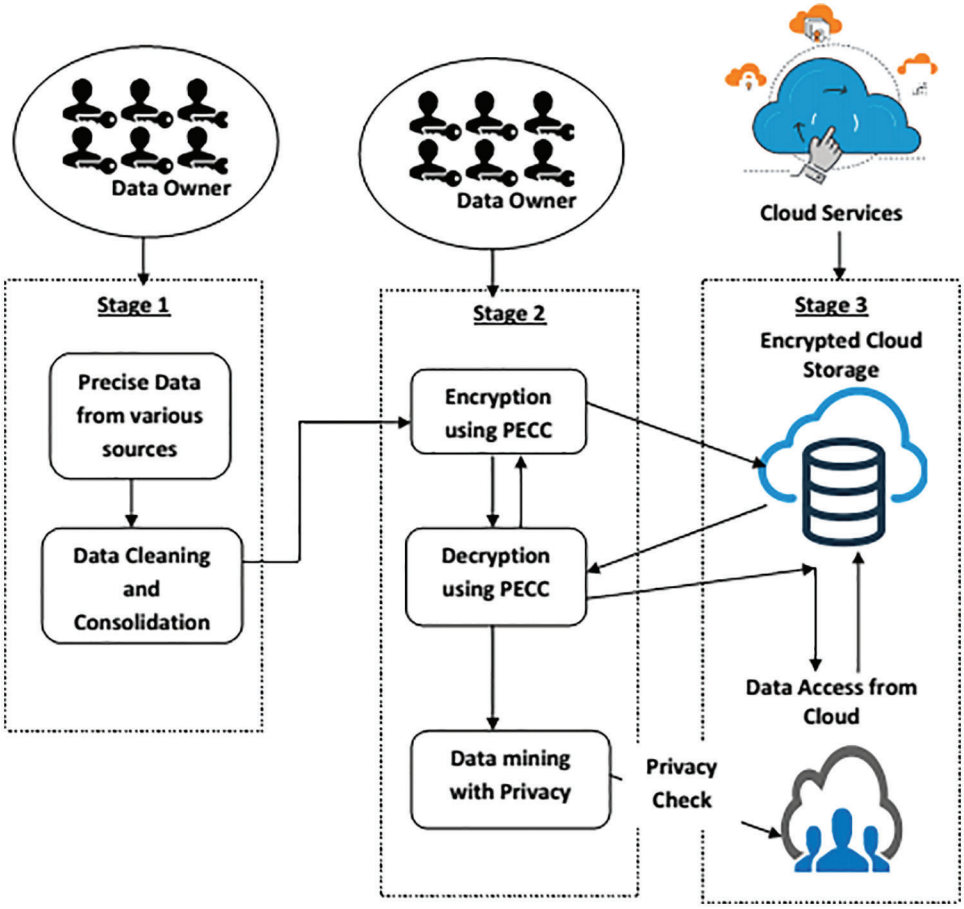

Figure 1: Framework embedding data mining with privacy protection using PECC architecture

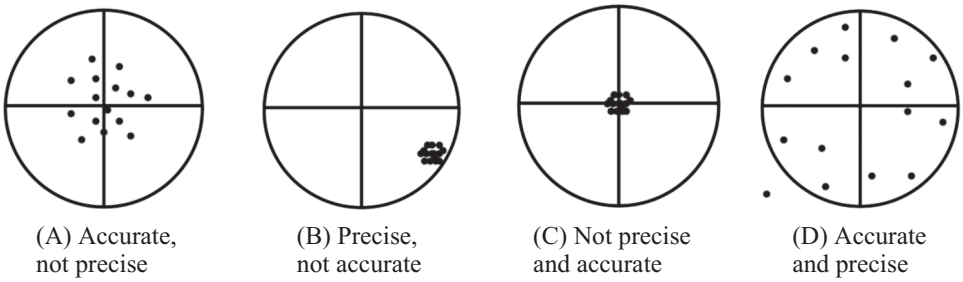

Figure 2: Data categorization

3.4 PECC (Phase II)

PECC suggests reducing the number of bits required for cipher-text creation while simultaneously lowering the computational burden. In addition, PECC is a public key cryptographic algorithm that is efficient and secure. Using PECC, this research aims to keep data secure while retaining privacy.

A precise elliptic curve (PEC) has the following expression:

$$C : y^2 + e(x)y = m(x) \tag{1}$$

$$e, m \in F[x], de(m) = 2g + 1, de(e) \leq c, m \text{ is single} - \text{variable} \tag{2}$$

$$\text{where collection } c = (de(m) - 1)/2. \tag{3}$$

On PEC, the edges need not constitute a collection. Instead, the Jacobian version of V across a field F, a finite algebraic expression, is used to establish a collective rule.

PEC over Finite Field Fp is defined as:

$$C : y^2 + e(x)y = m(x)(\text{mod}p), e, m \in F[x], de(m) = 2c + 1, de(e) \leq c, m \text{ is single} - \text{variable}, \tag{4}$$

$$\text{where collection}(c) = (de(m) - 1)/2 \tag{5}$$

The Discrete Logarithm Problem is the foundation for the PECC, which is defined as follows: "Assume Fn is a fixed field with size n. Calculate mZ such that in the Jacobian, d2 = md1 taken two prime factors, d1 and d2." P_1 and P_2 are precise data sources spread globally. A three-level structure can be like to wide angles. The sources of data and Online Transaction Processing (OLTP) locates on the lower standard. The design of the database system is at the intermediate tier. The DMPP framework is at a superior stage. The benefit of this technique is that every tier is separate from the others in the implementation stage. PECC is often used to move data from various sources to the databases for the first time. The database systems entries are encoded as m and delivered as an x-y point Pm in the first stage of this approach. Transmitter Sr1 and Sr2 are supposed to have sent the databases P_1 and P_2. Dt_1, who manages the database system, is the recipient. The associated phenomena will use by both Sr_1 or Sr_2. P_M will be encoded and then decoded as a cipher [32]. We cannot just encrypt the information as a point's u or v coordinate since not all position coordinates are in Ep (x, y). Like a key exchange, an encoding system needs a point G and an elliptic groups Ep(x, y) as inputs. Sr_1 or Sr_2 produces a public key and picks a private key Pr_K.

3.5 Public as well as Private Key Generation

Feed: PEC Pc, (p-prime, d-divisor)

Outcome: Public Key- Pc_A and Secure Private Key- Pr_K.

$Pr_K \in R$ Z [In N, pick a prime factor (Pr_K) randomly].

Pc_A [Pr_K] d [Using the Mumford representation to depict the Pc_A, it has the format (x(a), x(b))].

return Pc_A and Pr_K.

3.5.1 Encrypting Algorithm

The text "M" express as a succession of dots (x(a),x(b)). eM stands for cipher-text. Sr follows these procedures to encode and send out a message to Dt:

1. $q \in R$ N (In Z, pick a positive prime factor q at randomly).
2. Q [q]d (d - divisor & Q format is (x(a),x(b))).
3. Pr_K [q]Pc_B (Pc_B:(x(a),x(b)) is receiver's(Dt's)public key)
4. return Pc_A and Pr_K.
5. $C_M\{$ Q, $P_M + Pr_K$ $\}$ (The encrypted message to be transmitted is CM:(x(a),x(b))).

3.5.2 Decrypting Algorithm

To obtain the encoded message's initial condition "Q" and multiplies it with its Private Key (Pr_K), then deducts the output from the secondary Position to decode the encrypted C_M.

1. $E_M + kPc_B - Pr_K(Q) = E$
2. $= E_M + kPc_B - k(Pr_K\ d_i)$
3. $= E_M + kPc_B - Pr_K(kd_i)$
4. $= E_M + kPc_B - kP_B$
5. $= E_M$

"Sr" has added kPc_B to the packet E_M to conceal it. Though Pc_B is a public key, no one can eliminate the disguise kPc_B since only "Sr" knows the value of k. To delete a message, an intruder must calculate k out from provided d_i and $[k]d_i$, i.e., Q, which is problematic. It is worth noting that Sr utilizes Pc_B, Dt's public key. Therefore, Dt multiplies the first position in the combination by Dt's private key and deducts the output from the second part to decrypt the ciphertext:

$$P_M + xPc_B - n_B(xGr) = P_M + x(n_BGr) - nB(xGr) = P_M \quad (6)$$

Sr has added xPc_B to the text P_M to conceal it. Because only Sr recognizes the value of x, no one can eliminate the disguise xPc_B, even if Pc_B is a public key. Nevertheless, Sr contains a "hint," which is sufficient to eliminate the disguise if the secret key n_B is known. To retrieve the information, an intruder had to calculate x from Gr and xGr, which is problematic. Similarly, Sr will safely send P_1's information base to Dt.

3.6 Storing and Accessing Data (Phase III)

3.6.1 Authenticity of Clients

Step 1: Clients enroll with the data center by giving the required information. The Internet address of the system in which the client/user registration is one of the required data.

Step 2: For enrolled customers, the distributed storage center offers a unique id as well as a set of credentials, either public or private, for PECC cryptography.

This id is treated separately for both users and clients. It saves the information in a secure database. Whenever the client/user logs in with his legitimate identity the next time, the distributed storage center examines the registry to see whether the customer has previously enrolled. Beyond approval, the user nodes permit to access the distributed storage center's functions.

3.6.2 Encryption/Decryption of Data

Throughout this operation, information encodes and decodes were conducted on the customer side to avoid identity leaking with key. In addition, it preserves system resources, allowing computational resources [33,34] to use more efficiently. The preceding are some of the steps:

Step 1: Before saving information in the data station, the authorized customer encodes the information using the data agency's public key utilizing elliptic curve encryption.

Step 2: When a receiving device requires data, the data is encoded and decoded using a secret key issued by the datacentre to the customer. Customers might use the information.

4 Performance Analysis

In this part, we use the Framework to evaluate the results of our approach and the original standards in the Java platform environment [35]. It is worth noting that in our approach, all public key activities specify on the 25519 secure curvatures. The present protocol employs 256-bit secret keys and 3072-bit cryptographic

keys with the same degree of security as the 25519 curvatures. Furthermore, our tests demonstrate that the Intel Core i3 CPU has 2.60 GHz and 6 GB of RAM.

4.1 Computational Cost

In Tab. 1, the prevalence of PECC, ECC, and Triple DES algorithms is examined in this study using units ranging from 100 to 10,000. In contrast to ECC and Triple DES, the PECC method gives a greater ceiling in the implementation and validation phases. The PECC method's run duration spans from 0.0525s to 0.547s. PECC method has a cheap computing cost due to the short time required for formation and validation. The estimated cost of PECC, when analyzed with a truthfulness measurement of 0.4, is found to be 40 percent and 45 percent higher than when analyzed with an authenticity parameter of 0.4. Furthermore, the estimation cost of PECC when analyzed with a truthfulness parameter of 0.4 is 28 percent and 32 percent higher than when evaluated with an authenticity parameter of 0.4. Fig. 3 depicts the simulation results.

Table 1: Computational cost

Packet size (MB)	Computational cost (ms)		
	PECC	ECC	Triple DES
100	0.38	0.45	0.63
200	0.45	0.6	0.72
300	1.25	1.48	1.75
400	1.38	1.59	1.83
500	2.12	2.51	2.73
600	2.34	2.75	3.05
700	3.51	3.67	4.03
800	3.72	3.86	4.52
900	4.32	4.57	5.3
1000	4.51	4.72	5.5

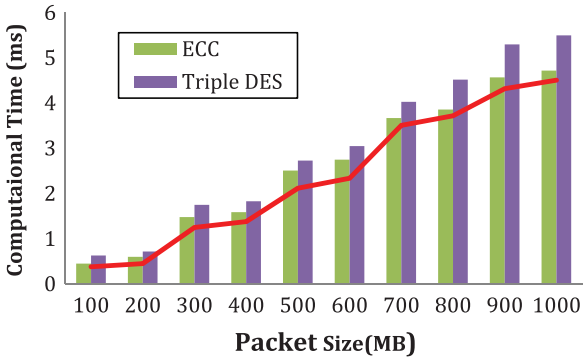

Figure 3: Computational cost

4.2 Average Approximation Error

The relative error measurements determined the likelihood of error during the entire procedure. The simulations carry files ranging from 128 MB to 1 GB. The findings show that the suggested PECC strategy has meager error rates than conventional methods. Tab. 2 presents the findings, whereas Fig. 4 depicts the simulation results.

Table 2: Average approximation error

Packet size (MB)	Avg approximation error (mb/sec)		
	Triple DES	ECC	PECC
128	0.0017	0.0052	0.0004
256	0.0052	0.0149	0.00069
512	0.0105	0.0195	0.00121
1024	0.0213	0.0357	0.00139

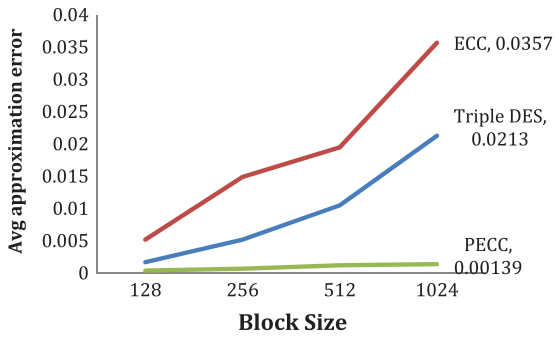

Figure 4: Average approximation error

4.3 Time Consumption

This measure calculates the total time required to generate the keys, encryption, and decode keys. The computations perform on files ranging from 128 MB to 1 GB. The analysis shows that, in comparison to conventional approaches, the suggested PECC technique takes much less time. Tab. 3 presents the findings, whereas Fig. 5 depicts the simulation results.

Table 3: Time consumption

Packet size (MB)	Time consumption (sec)		
	Triple DES	ECC	PECC
128	16.79	11.52	5.987
256	37.92	22.83	14.515
512	62.78	43.24	32.933
1024	131.75	73.86	57.986

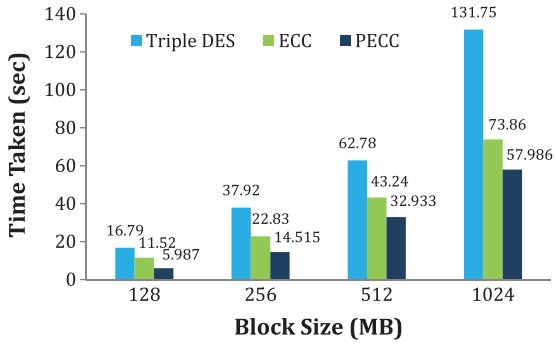

Figure 5: Time consumption

4.4 Anonymizing Time

The computations carrying for files range from 128 MB to 1 GB; Anonymizing time is a statistic that measures how long it takes to anonymize data. The findings demonstrated that the new PECC approach takes less time to anonymize when compared to previous approaches. Tab. 4 summarizes the findings, whereas Fig. 6 depicts the simulation model.

Table 4: Anonymizing time

Packet size (MB)	Anonymizing time (sec)		
	Triple DES	ECC	PECC
128	109.75	57.69	47.51
256	200.45	85.98	68.72
512	499.01	112.21	79.83
1024	891.85	137.43	90.12

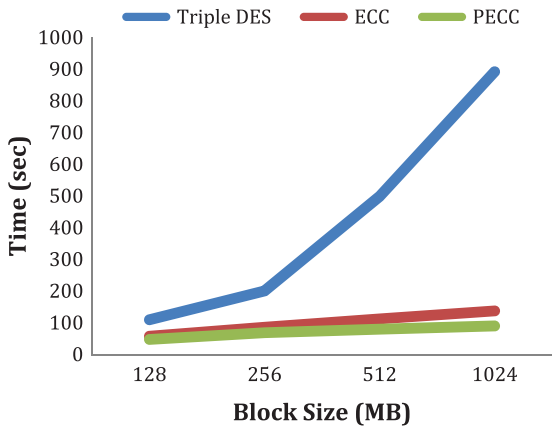

Figure 6: Anonymizing time

4.5 Data/Information Loss

The volumes of data lost and the delay incurred during the cryptographic procedure [36,37] refer to data loss—the computations carrying files ranging from 128 MB to 1 GB. The findings show that the suggested

PECC technique causes less risk of data loss when compared to previous approaches. Tab. 5 presents the findings, whereas Fig. 7 depicts the simulations.

Table 5: Information loss

Packet size (MB)	Information loss (KB)		
	Triple DES	ECC	PECC
128	735.57	212.78	95.17
256	1098.32	297.45	193.328
512	2104.06	455.76	372.07
1024	3900.49	899.91	640.98

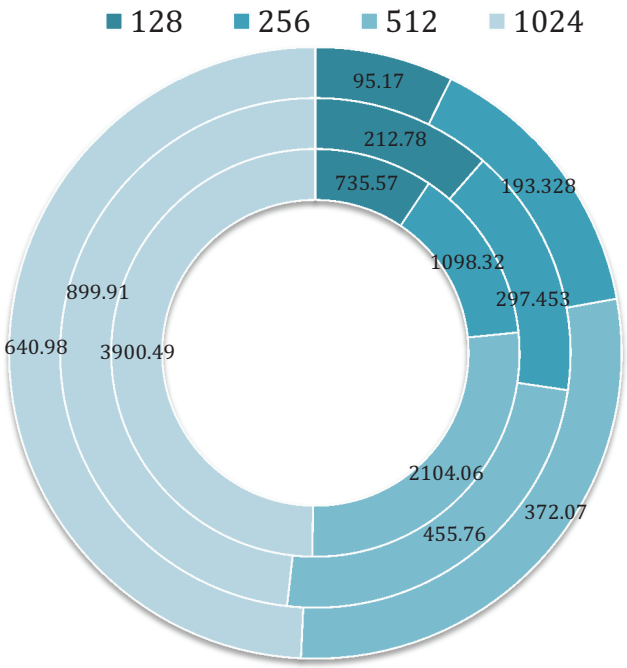

Figure 7: Data/Information loss

5 Conclusion and Future Scope

The work aims to offer a multi cloud-based privacy-preserving technique based on PECC. The PECC's goal is to minimize computation time while simultaneously reducing mistake incidence and privacy breaches. PECC operates faster than the previous research methods due to its flexible character. Furthermore, precise keys in data protection in PECC could lower overhead in data exchange and guarantee dependable data protection through concealed data approach readily accessible to users. PECC's empirical analysis demonstrates that it outperforms existing approaches safeguarding privacy during split and grouped processing. We can apply PECC for online messaging, secure transmission, pseudo-random generation, and other operations. PECC successfully implements message encryption, cryptographic certificates, and authentication. Also, we have an idea to research advanced ways by

adding quantum techniques into our algorithm in the future. We plan to use the quantum technique, the key sharing mechanism.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Y. Sarhan and S. Carr, "A highly-secure self-protection data scheme in clouds using active data bundles and agent-based secure multi-party computation," in *2017 IEEE 4th Int. Conf. on Cyber Security and Cloud Computing (CSCloud)*, New York, NY, USA, pp. 228–236, 2017.

[2] A. Balu and K. Kuppusamy, "An expressive and provably secure ciphertext-policy attribute-based encryption," *Information Sciences*, vol. 276, no. 2, pp. 354–362, 2014.

[3] X. Zhu, Q. Liu and G. Wang, "A novel verifiable and dynamic fuzzy keyword search scheme over encrypted data in cloud computing," in *2016 IEEE Trustcom/BigDataSE/ISPA*, Tianjin, China, pp. 845–851, 2016.

[4] X. Pei, Y. Wang, W. Yao, J. Lin and R. Peng, "Security enhanced attribute based signcryption for private data sharing in cloud," *IEEE Trustcom/BigDataSE/ISPA*, vol. 2, no. 1, pp. 45–58, 2016.

[5] S. Wang, K. Liang, J. K. Liu, J. Chen, J. Yu *et al.,* "Attribute-based data sharing scheme revisited in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1661–1673, 2016.

[6] S. Sundari and M. Ananthi, "Secure multi-party computation in differential private data with data integrity protection," in *Int. Conf. on Computing and Communications Technologies (ICCCT)*, Chennai, India, pp. 67–79, 2015.

[7] K. Yang, X. Jia, K. Ren, B. Zhang and R. Xie, "DAC-MACS: Effective data access control for multiauthority cloud storage systems," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1790–1801, 2013.

[8] A. Wainakh, T. Grube, J. Daubert and M. Muhlhauser, "Efficient privacy-preserving recommendations based on social graphs," in *13th ACM Conf. on Recommender Systems (RecSys '19). Association for Computing Machinery*, New York, NY, USA, pp. 78–86, 2019.

[9] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 7, pp. 1735–1744, 2014.

[10] J. Hong, K. Xue and W. Li, "DACMACS: Effective data access control for multiauthority cloud storage systems/ security analysis of attribute revocation in multiauthority data access control for cloud storage systems," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1315–1317, 2015.

[11] P. Srilakshmi, "Data access control with revocable multiauthority cloud storage," *International Journal of Engineering and Computer Science*, vol. 2, no. 1, pp. 67–78, 2017.

[12] M. B. Krishna and M. S. Krishna, "Hierarchical attribute based revocable data access control for multi authority cloud storage," *IOSR Journal of Computer Engineering*, vol. 19, no. 04, pp. 91–97, 2017.

[13] H. C. Chen and P. P. Lee, "Enabling data integrity protection in regenerating-coding-based cloud storage: Theory and implementation," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 407–416, 2014.

[14] J. N. Begum, K. Kumar and V. Sumathy, "Multilevel access control in defense messaging system using Elliptic curve cryptography," in *2010 Second Int. Conf. on Computing, Communication and Networking Technologies*, Karur, India, pp. 1–9, 2010.

[15] S. A. Kadir, A. Sasongko and M. Zulkifli, "Simple power analysis attack against elliptic curve cryptography processor on FPGA implementation," in *2011 Int. Conf. on Electrical Engineering and Informatics*, Bandung, Indonesia, pp. 1–4, 2011.

[16] R. K. Pateriya and S. Vasudevan, "Elliptic curve cryptography in constrained environments: A review," in *2011 Int. Conf. on Communication Systems and Network Technologies*, Katra, India, pp. 120–124, 2011.

[17] P. Syam Kumar, R. Subramanian and B. Rajkumar, "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing," *Journal of Network and Computer Applications*, vol. 64, no. C, pp. 12–22, 2016.

[18] Y. A. A. S. Aldeen, M. Salleh and Y. Aljeroudi, "An innovative privacy preserving technique for incremental datasets on cloud computing," *Journal of Biomedical Informatics*, vol. 62, no. C, pp. 107–116, 2016.

[19] Q. huang, Z. feng, Y. Yang, F. Jing-yi and X. niu, "Secure and privacy-preserving DRM scheme using homomorphic encryption in cloud computing," *The Journal of China Universities of Posts and Telecommunications*, vol. 20, no. 6, pp. 88–95, 2013.

[20] T. Van Vu, T. D. Luong and V. Q. Hoang, "An elliptic curve-based protocol for privacy preserving frequency computation in 2-part fully distributed setting," in *2020 12th Int. Conf. on Knowledge and Systems Engineering*, Can Tho, Vietnam, pp. 91–96, 2020.

[21] N. Yuvaraj, K. Praghash and T. Karthikeyan, "Data privacy preservation and trade-off balance between privacy and utility using deep adaptive clustering and elliptic curve digital signature algorithm," *Wireless Personal Communications*, 2021.

[22] J. Sasidevi, R. Sugumar and P. Shanmuga Priya, "Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud," *International Journal of Business Intelligence and Data Mining*, vol. 15, no. 3, pp. 273–287, 2019.

[23] Y. Li, Y. Zhao and P. Yang, "Efficient privacy-preserving data aggregation scheme with fault tolerance in smart grid," *Security and Communication Networks*, vol. 2022, pp. 1–18, 2022.

[24] N. Partheeban, K. Sudharson and P. J. Sathish Kumar, "SPEC- serial property based encryption for cloud," *International Journal of Pharmacy & Technology*, vol. 8, no. 4, pp. 23702–23710, 2016.

[25] K. Sudharson, A. Mudassar Ali and N. Partheeban, "NUITECH – natural user interface technique formulating computer hardware," *International Journal of Pharmacy & Technology*, vol. 8, no. 4, pp. 23598–23606, 2016.

[26] J. Aruna Jasmine, V. Nisha Jenipher, J. S. Richard Jimreeves, K. Ravindran and D. Dhinakaran, "A traceability set up using digitalization of data and accessibility," in *2020 3rd Int. Conf. on Intelligent Sustainable Systems (ICISS)*, Thoothukudi, India, pp. 907–910, 2020.

[27] D. Dhinakaran and P. M. Joe Prathap, "Ensuring privacy of data and mined results of data possessor in collaborative ARM," in *Pervasive Computing and Social Networking Lecture Notes in Networks and Systems*. Vol. 317. Singapore: Springer, 2022.

[28] D. Yang, B. Qu and P. Cudre-Mauroux, "Privacy-preserving social media data publishing for personalized ranking-based recommendation," *IEEE Transactions on Knowledge and Data Engineering*, vol. 31, no. 3, pp. 507–520, 2019.

[29] S. Arun and K. Sudharson, "DEFECT: Discover and eradicate fool around node in emergency network using combinatorial techniques," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–12, 2020.

[30] C. Ma, B. Wang, K. Jooste, Z. Zhang and Y. Ping, "Practical privacy-preserving frequent itemset mining on supermarket transactions," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1992–2002, 2020.

[31] S. K. Thakur, B. Bhagat and S. Bhattacharjee, "Privacy-preserving outsourced mining of d-eclat association rules on vertically partitioned databases," in *2018 Fourth Int. Conf. on Computing Communication Control and Automation (ICCUBEA)*, Pune, India, pp. 1–5, 2018.

[32] K. Agrawal and V. Tewari, "Analysis of privacy preserving mechanisms for outsourced data mining," in *2017 Int. Conf. on Recent Innovations in Signal processing and Embedded Systems (RISE)*, Bhopal, India, pp. 572–576, 2017.

[33] K. Sudharson and V. Parthipan, "A survey on ATTACK–anti terrorism technique for adhoc using clustering and knowledge extraction," in *Advances in Computer Science and Information Technology. Computer Science and Engineering. CCSIT 2012. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Vol. 85. Berlin, Heidelberg: Springer, pp. 508–514, 2012.

[34] S. Qiu, B. Wang, M. Li, J. Liu and Y. Shi, "Toward practical privacy preserving frequent itemset mining on encrypted cloud data," *IEEE Transaction on Cloud Computing*, vol. 8, no. 1, pp. 312–323, 2020.

[35] V. Baby and N. Subhash Chandra, "Privacy preserving association rule mining based on homomorphic computations," *International Journal of Information Privacy, Security and Integrity*, vol. 3, no. 4, pp. 268–283, 2018.

[36] X. R. Zhang, W. F. Zhang, W. Sun, X. M. Sun and S. K. Jha, "A robust 3-D medical watermarking based on wavelet transform for data protection," *Computer Systems Science & Engineering*, vol. 41, no. 3, pp. 1043–1056, 2022.

[37] X. R. Zhang, X. Sun, X. M. Sun, W. Sun and S. K. Jha, "Robust reversible audio watermarking scheme for telemedicine and privacy protection," *Computers, Materials & Continua*, vol. 71, no. 2, pp. 3035–3050, 2022.