*International Journal for Modern Trends in Science and Technology*
*Volume 12, Issue 04*, pages 271-275.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol12issue04.html
DOI: https://doi.org/10.5281/zenodo.19394780

# Advanced Cryptographic Techniques for Secure Data Storage and Erasure

**Guna Gayathri Praseetha K**

*Assistant Professor, Department of Computer Science and Engineering, PBR Visvodaya Institute of Technology and Science, Kavali, India.*

**To Cite this Article**
Guna Gayathri Praseetha K (2026). Advanced Cryptographic Techniques for Secure Data Storage and Erasure. International Journal for Modern Trends in Science and Technology, 12(04), 271-275. https://doi.org/10.5281/zenodo.19394780

**Article Info**
Received: 06 March 2026; Revised: 28 March 2026; Accepted: 01 April 2026.



***KEYWORDS***

*Cloud computing, SSE, TPM, CSS*

**ABSTRACT**

*The delinquent of sheltered records expurgation has been expansively intentional in the preceding with a sarcastic organization of nonfiction vacant. All present software-based elucidations can be potted as after the similar one-bit-return protocol: the obliteration sequencer achieves data destruction and incomes each victory or catastrophe. Conversely, such a one-bit-return etiquette seizures the data erasure system hooked on a black box – the manipulator has to dependence the consequence but cannot straightforwardly authenticate it. This is exclusively challenging when the obliteration database is compressed within a Trusted Platform Module (TPM) and the user has no entree to the code esoteric. In this scheme, we inductee a learning on how to scrub surreptitious data with public verifiability. This is a focus that has not been considered previously, partly since it seems innately intolerable. In this project, we show a clarification is conceivable by relating apposite cryptographic primitives. Based on combining DHIES, Chaum-Pedersen Zero Knowledge Proof and ECDSA, we extant an amended Secure Storage and Erasure (SSE) procedure. The key indication in our clarification is founded on a "trust-but-verify" pattern, which is usually pertinent to many sanctuary glitches but has been fundamentally despicable in the meadow of protected data deletion. Lastly, we extant a material enactment of the SSE scheme to determine its useful feasibility.*

## INTRODUCTION TO CLOUD COMPUTING

Cloud computing is a computing prototype, wherever an enormous tarn of schemes are related in secluded or communal systems, to offer enthusiastically accessible structure for solicitation, facts and organizer storing. With the advent of this expertise, the rate of reckoning, submission presenting, pleased stowing and distribution is bargain ominously. This expertise tolerates for

abundant additional proficient totaling by concentrating data storage, dispensation and bandwidth. An unpretentious sample of cloud computing is Yahoo email, Gmail, or Hotmail etc.

## OBJECTIVE

Although the stowage of business data on distant waiters is not a fresh growth, present enlargement of mist calculating rationalizes a new cautious appearance at its real moments comprising confidentiality and concealment issues. Also, it is habitually deficient to perceive the data venality only when retrieving the data, as it ensures not give manipulators precision pledge for individual's un-accessed statistics and strength be too late to recuperate the statistics forfeiture or impairment. In a word, facilitating unrestricted appraising amenities will performance an essential role for this promising cloud frugality to convert fully recognized somewhere handlers resolve requirement techniques to consider menace and advance belief in the cloud.

## NEED FOR STUDY

There is a tendency for subtle consumer records to be stowed by third parties on the internet. In dispersed locations with delegated servers, such as the cloud many solicitations essential contrivances for multifarious admittance mechanism done converted data. ABE is a new free key created one-to-many encryption that assists entrance switch over scrambled data by contact procedures and attributed elements concomitant with secluded keys and cipher texts the cryptosystem tolerable for decryption when at tiniest k aspects coincided amongst a cipher text and a private key. There are two kinds of ABE schemes: key-policy ABE (KP-ABE) and cipher text-policy ABE (CP-ABE). So we afford the verifiability of the cloud's renovation and providing a scheme to pattern the exactness of the alteration.

## EXISTING SYSTEM

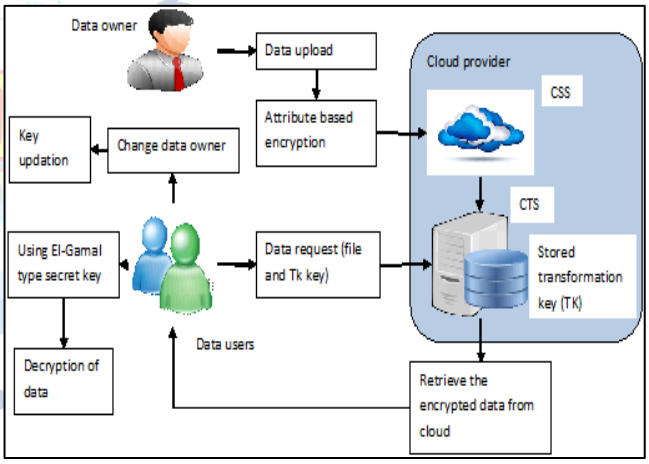
As an allowance of delicate information is collective then clasp on by third-party positions on the net, there'll be an aspiration to cipher indication clench on at these sites. One drawback of converting info is that it will be by assortment mutual merely at a coarse-grained level (i.e., generous alternative revelry your peculiar key). In that, qualities and individual keys are connected to access edifices that accomplish the cipher texts that the user is equipped to modification. It didn't rawhide the set of elements base that the data is decoded.

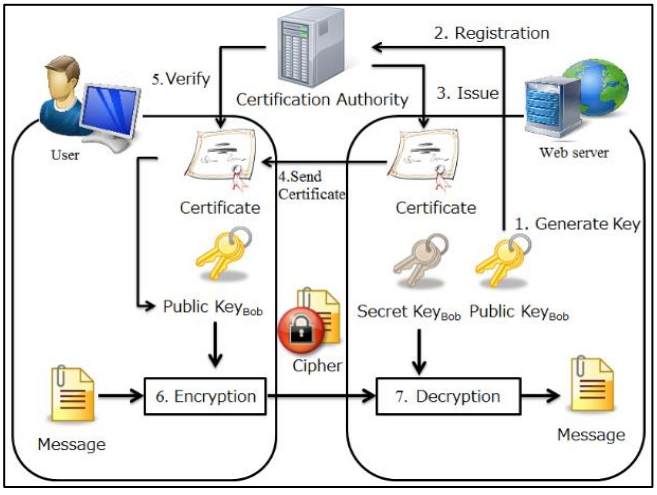
Clandestine inscription is assisted if and individual if the user's trait agreed contents the cipher text entrance configuration. This delivers fine-grained access supervision on united material in numerous utilitarian locales, similarly as sheltered lists and protected multicast. It assistances a modified with well reduced cipher texts and earlier encryption/decryption maneuvers.

**Disadvantages**

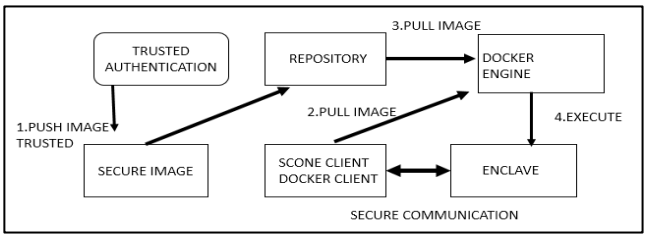
- ABE arrangements are that decryption is luxurious for resource-limited strategies due to combination processes.
- The ABE cloud not safeguards.
- ABE structure with subcontracted decryption abolishes the decryption upstairs.

## SYSTEM ARCHITECTURE



## RESULTS




## MODULES

- Cloud Entities
- TPM
- Cloud Consumer
- SSE Model
- Evaluation criteria

### 1. Cloud Service Provider

Cloud Storage Server (CSS): an entity, which is fared by Cloud Service Provider (CSP), has momentous packing interstellar and reckoning supply to preserve clients' data; the clouds have a large quantity of stowing places and work out possessions, and offer distant data packing facilities to manipulators in a pay-as-you-use manner. When a user needs to subcontract the data, he/she selects a mist, rentals the storing interplanetary and uploads the data to Cloud.

### 2. TPM

The TPM or organizer, who checks cloud data on behalf of the handler and also authenticates the storage correctness of data being subcontracted from the cloud. There are two categories: private auditability and public auditability. To tenancy off the cargo of supervision of records of the data owner, TPM will assessment the data of client. It eradicates the engrossment of the client by examining that whether his data stowed in the haze are undeniably together, which can be vital in attaining thrifts of scale for Cloud Computing.

### 3. Cloud Consumer

The client, who is a separate operator or an association, needs to accumulation and entree their enormous extent of data in the cloud. In this component an operator has to upload their archives in a cloud server, they must chronicle first. Then only they container be competent to upload their file. For that they take to fill their particulars in the recording form. These details are preserved in a database. In this component, the user have to login, they should give their name and password to get validate from the cloud.

### 4. SSE

The TPM connects with the host, subsequent a Secure Storage and Erasure (SSE) etiquette. This decorum is the dominant portion in the all-inclusive organization design. It controls in the same group scenery as ECDSA (or DSA). As a synopsis, the SSE practice requires the resulting API functions:

Key Gen. To brand a random public/private key pair;

Encrypt. To scramble data with a stated public key;

Decrypt. To decrypt data with a specified private key;

Audit. To review if encryption was done appropriately;

Delete. To obliterate a definite cloistered key with a numeral monogram reimbursed as an impervious of obliteration. To demand the above utilities, the user must be authentic first.

ReEncrypt. To decrypt files with an itemized private key will upshot in re-encryption on waitron side

### 5. Performance Evaluation

Through this element, we evidence that SSE completes the chattels of data concealment, data veracity authentication, sheltered data transference and sheltered data destruction. We also exhibit the competence of SSE in expressions of the computational and statement overhead.

## PROPOSED SYSTEM

*SSE Protocol - Deletion by cryptography.*

The foremost impression of this effort monitors the similar enterprise opinion created on "trust-but verify". By rub on cryptographic performances, we permit an end user to confirm the exact enactment of two imperative maneuvers esoteric a TPM: encryption and deletion.

**Advantages**

- This enterprise is immaterially theme to the trap-door attack
- A state-funded rival is able to delivered all scrambled circulation
- Tamper-resistance
- Tamper-resistant hardware with implanted CPU, sheltered reminiscence
- Protected key storage
- Clandestine keys continuously kept privileged locked memory
- Key supervision
- Via a usual of APIs (most difficult part in the design)
- Audit deprived of transferring
- No data seepage or data knowledge

**Hardware Requirements**

- CPU type : Intel Pentium 4
- Clock speed : 3.0 GHz
- Ram size : 512 MB
- Hard disk capacity : 40 GB
- Monitor type : 15 Inch color monitor
- Keyboard type : internet keyboard

**Software Requirements:**

- Operating System : Windows OS
- Language : PHP
- Back End : My SQL
- IDE : Net Beans

## TECHNIQUES USED IN THE PROJECT

## VERIFIABLE OUTSOURCED DECRYPTION

**Setup ()**

The situation procedure receipts as contribution a safekeeping limit $\lambda$ and a minor creation depiction U= {1, 2, 3…, ℓ}. It first tracks G ($\lambda$) to obtain (p, G,$G_T$, e), where G and and $G_T$ are cyclic collections of major instruction . It formerly elects g,u,v,d ∑ G,and $\alpha$,a ∑ $Z_p^*$ evenly at arbitrary, for every one quality i ∑ U,It indicates a accidental value Si ∑ Z* p To finish, it elects a collision-resistant botch task H:G⟶ $Z_p^*$.The free limits PK = (G, $G_T$ ,e,g,u,v,d,$g^a$ , e( g, g)$^\alpha$ ,$T_i = g^{si}$ ∀ i ,H).The main secret key MSK= $\alpha$.

**KeyGen ()**

The key group procedure aimlessly preferences t ∑ Z* p the furtive key $SK_s = (S, K, K_0, K_i)$ is added as

K = $g^\alpha$ $g^{at}$

$K_o$= $g^t$

$K_i$= $T_i^t$ ∀ i∈ s

**Encrypt ()**

The encrypt process practice the open constraints, letter and entree erection. Access erection contains of features and their charting.

$$C = u^{H(M)}v^{H(M)}d$$
$$C_1 = M.e(g.g)^{\alpha s}$$
$$C_1' = g^s$$
$$C_{1,i} = g^{a,A_i,v}T^{-r1,i}\rho(i)$$
$$D_{1,i} = g^{r1,i}\ \forall\ i \in \{1,2,\dots,1\}$$
$$C_2 = M.e(g.g)^{\alpha s}$$
$$C_2' = g^s$$
$$C_{2,i} = g^{a,A_i,v}T^{-r2,i}\rho(i)$$
$$D_{2,i} = g^{r2,i}\ \forall\ i \in \{1,2,\dots,1\}$$

Encrypted data

CT=((A, $\rho$),$\hat{c}$, $C_1, C_1', C_{1,i}, D_{1,i}, C_2, C_2', C_{2,i}, D_{2,i}$)

**Gen T$k_{out}$()**

In supportable subcontracted decryption the user uses Gen T$k_{out}$() system for engendering the renovation key "TKs" and Releasing Key "RKs ".It takes contributions as the Public factors and user's clandestine key "SKs". The operator refer the Alteration vital to the cloud.

SKs = (S, K, $K_0$, $K_1$)

It picks a random value z ∑ Z* p

Conversion key TKs = (S, K′$K_0$′, $K_1$′ )

Salvaging Key RKs = z

$$Transform_{out}()$$

By using the $transformation_{out}$ procedure cloud will create the distorted cipher text. This system takes as effort the communal restrictions PK, cipher text CT, and the change key TKs to engender the converted cipher text CT′. It send the transmuted cipher text to the manipulator.

$$T_1' = [e(c_1', \frac{K'}{[(\prod_{i\in I} (e(C_{1,i}, K_0').e(K'_{\rho(i)}, D_{1,i}))^{\omega i})}]$$

$$= [e(g,g)^{\alpha s/z}e(g,g)^{ats/z}/[\prod_{i\in I} (e(g,g)^{atAi.v\omega i/z}$$

$$= e(g,g)^{\alpha s/z}$$

$$T_2' = [e(c_2', \frac{K'}{[(\prod_{i\in I} (e(C_{2,i}, K_0').e(K'_{\rho(i)}, D_{2,i}))^{\omega i})}]$$

$$= [e(g,g)^{\alpha s'/z}e(g,g)^{ats'/z}/[\prod_{i\in I} (e(g,g)^{atAi.v'\omega i/z}$$

$$= e(g,g)^{\alpha s'/z}$$

Altered cipher text = CT′ =(T=C, $T_1 = C_1, T_1', T_2' = C_2, T_2'$)

$$Decrypt_{out}()$$

Decrypt process customs the communal restrictions, converted cryptogram text and cipher text for authentication. PK = (G,$G_T$ ,e,g,u,v,d,$g^a$ ,e( g, g)$^\alpha$ ,$T_i = g^{si}$ =g ∀ i ,H)

CT = ((A, ϱ),$\hat{c}$, $\hat{c}, C_1, C_1', C_{1,i}, D_{1,i}, C_2, C_2', C_{2,i}, D_{2,i}$,i )

CT′ = (T=C,$T_1 = C_1, T_1', T_2' = C_2, T_2'$) .

RKs = z

## CONCLUSION

This paper suggests an original outline of reaching grained contact ruse for partaking delicate data. Since moderately reliable cloud servers, it maintains that to fully appreciate the perception, patients will have broad controller of their own solitude finished coding their records to let fine-grained entrance. The agenda discourses the unique challenges transported by manifold data owners and users, in that significantly

condense the complication of key super vision while augment the confidentiality securities linked with earlier works. It develops ABE to scramble the mist data, so that employer can consent contact not only by particular users, but also countless operators from public Data proprietor mains with altered expert roles, recommendations and associations. We painstaking a new prerequisite of ABE with farm out decryption: Verifiability. It is castoff to change the unusual perfect of ABE with subcontracted Decryption. This ABE outline with Confirmable farm out decryption and verified that it is sheltered and showable .Our system fixes not trust on haphazard prophecies. A malleable contact mechanism for converted data stockpiled in veil is providing. It excludes Decryption below for users affording to aspects. This Data renovation is surefire to hoard in cloud. This locked trait established cryptographic practice for tough numbers retreat that's being collective in the cloud.

## FUTURE ENHANCEMENT

In forthcoming, we can outspread our grind to contrivance innumerable processes to afford upgraded haven in mist milieus and also scrutinize the several features to encode the data

## Conflict of interest statement

Authors declare that they do not have any conflict of interest.

## REFERENCES


[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 3494, R. Cramer, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Secur., 2006, pp. 89–98.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 321–334.

[4] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 6571, D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, Eds. Berlin, Germany: Springer-Verlag, 2011, pp. 53–70.

[5] Y. Rouselakis and B. Waters, "Practical constructions and new proof methods for large universe attribute-based encryption," in Proc. ACM Conf. Comput. Commun. Secur., 2013, pp. 463–474.

[6] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conf. Comput. Commun. Secur., 2007, pp. 456–465.

[7] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. Ràfols, "Attribute-based encryption schemes with constant-size ciphertexts," Theoretical Comput. Sci., vol. 422, pp. 15–38, Mar. 2012.

[8] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," in Proc. 20th USENIX Secur. Symp., 2011, p. 34.

[9] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343–1354, Aug. 2013.

[10] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 6223, T. Rabin, Ed. Berlin, Germany: Springer-Verlag, 2010, pp. 465–482.

[11] K.-M. Chung, Y. Kalai, and S. Vadhan, "Improved delegation of computation using fully homomorphic encryption," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 6223, T. Rabin, Ed. Berlin, Germany: Springer-Verlag, 2010, pp. 483–501.

[12] B. Chevallier-Mames, J.-S. Coron, N. McCullagh, D. Naccache, and M. Scott, "Secure delegation of elliptic-curve pairing," in Smart Card Research and Advanced Application (Lecture Notes in Computer Science), vol. 6035, D. Gollmann, J.-L. Lanet, and J. Iguchi-Cartigny, Eds. Berlin, Germany: Springer-Verlag, 2010, pp. 24–35.

[13] C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proc. STOC, 2009, pp. 169–178.

[14] C. Gentry and S. Halevi, "Implementing Gentry's fully-homomorphic encryption scheme," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 6632, K. G. Paterson, Ed. Berlin, Germany: Springer-Verlag, 2011, pp. 129–148.

[15] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in Proc. CCS, 1993, pp. 62–73.

[16] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 4, pp. 2201–2210, Aug. 2014. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6642027

[17] A. Beimel, "Secure schemes for secret sharing and key distribution," Ph.D. dissertation, Dept. Comput. Sci., Israel Inst. Technol., Haifa, Israel, 1996.

[18] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," SIAM J. Comput., vol. 38, no. 1, pp. 97–139, 2008.

[19] V. Shoup, "Sequences of games: A tool for taming complexity in security proofs," Dept. Comput. Sci., New York Univ., New York, NY, USA, Tech. Rep. 2004/332, 2004. [Online]. Available: http://eprint.iacr.org/

[20] R. Canetti, H. Krawczyk, and J. B. Nielsen, "Relaxing chosen-ciphertext security," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 2729, D. Boneh, Ed. Berlin, Germany: Springer-Verlag, 2003, pp. 565–582.