International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Cloud Data Security through Post Quantum Cryptography: An Integrated Framework

Mr. Shaik Mohammad Ilias[1*], V. Sathya Durga[2], V. Ceronmani Sharmila[3]

Submitted: 07/02/2024 **Revised**: 14/03/2024 **Accepted**: 20/03/2024

Abstract: Quantum key cryptography is the cryptography that has capability to overcome the threat of quantum computing in future when exploited by adversaries. With quantum computers in the hands of adversaries in future, the existing security schemes might be broken due to massive computing power. As security is not one-time effort, it is a continuous process that needs development of stronger security schemes. Existing PQC schemes focused on either data security or key exchange. Besides, there is need for further improvement towards enhanced PQC primitives. In this paper, we proposed an integrated cloud data security framework with novel schemes towards PQC. For data security with encryption and decryption, we proposed Hybrid Encoding and Data Transformation (HEDT) algorithm. Another key exchange security scheme called Elliptic Curve Super singular Isogeny Diffie–Hellman (ECSIDH) was developed. The key agreement scheme consists of Elliptic-Curve Diffie–Hellman (ECDH) and Super singular Isogeny Diffie–Hellman (SIDH). ECDH combined with SIDH candidate in PQC which enhances the security of the proposed scheme since they strengthen the ECDH with PQC candidate SIDH. The ECSIDH is found more secure than individual key exchange scheme such as SIDH. Security analysis of HEDT revealed that it is more secure than existing algorithms and ECSIDH is more secure PQC candidate.

Keywords: *Post quantum cryptography, security, encryption, decryption, key exchange, ECDH, SIDH*

1. Introduction

With the emergence of quantum computing, the computational power is increased dramatically which may become curse in disguise as adversaries could misuse it to break existing security primitives. Cryptography research to overcome such situations is known as Post Quantum Cryptography. Many researchers identified the need for novel security scheme for data encryption and decryption besides key exchange. As stated by Liu et al. [27], quantum computers will soon come into market. Adversaries might misuse the power of them to break security systems. They emphasized the need for hybrid approaches to improve data security in PQC context. They proposed SIDH model as a key exchange scheme as PQC candidate but suggested to improve it further. Bos and Friedberger [28] investigated on improving SIDH with changes in its arithmetic. From their observations it is found that SIDH needs further improvement to be a strong PQC candidate. Costello et al. [29] investigated on "Elliptic Curve Diffie-Hellman" key exchange and SIDH and found that both are vulnerable to PQC attacks. They suggested to improve it by making a hybrid of both for stronger security. Our contributions in this paper are as follows.

1. We proposed HEDT algorithm with multiple data transformations to be a PQC candidate for data encryption and decryption.
2. For key exchange, we proposed a hybrid security architecture. It is an ECSIDH PQC candidate for key exchange.
3. An integrated security framework is realized with the two schemes proposed and evaluated.

The remainder of the paper is divided into the following sections. In Section 2, the existing situation is comprehensively analyzed literature pertaining to several facets of secure data including key exchange within the framework of Post-Quantum Cryptography (PQC). Section 3 introduces two security techniques that are considered as potential options for post-quantum cryptography (PQC). In Section 4, this paper discusses the findings of the conducted experiments and provides a comprehensive analysis of the security aspects. Section 5 of this study presents the derived results and offers insights into potential avenues for further research.

2. Related Work

This section reviews literature on different security mechanisms pertaining to enhanced data security and key exchange.

2.1 Data Security Schemes

The Advanced Encryption Standard (AES) is a prevalent security protocol that is extensively utilized in practical

[1]*Research Scholar, Department of Computer Science and Engineering, Hindustan Institute of Technology and Science, Chennai, India.*
[2]*Assistant professor, Department of computer science and Engineering, Hindustan institute of technology and science, Chennai, India.*
3 Head of Department, Department of Information Technology, Hindustan Institute of Technology and Science, Chennai, India.
[1] *illusoft54@gmail.com,* [2] *sathyadv@hindustanuniv.ac.in,* [3] *csharmila@hindustanuniv.ac.in*

applications. Et al. [1] investigated data security in cloud measures using HEROKU as the chosen cloud platform. The researchers conducted experiments pertaining to data security, specifically investigating the variables of security latency and security strength. In their study, Yu et al. [2] examined the Scan attack and proposed enhancements to the AES architecture of secured information. In their study, Chinnasamy and Deepalakshmi [3] proposed a hybrid security approach for healthcare applications in the cloud by integrating hashing and cryptographic primitives. Qian and colleagues [4] introduced a novel encryption method that employs the technique of Information Dispersal method (IDA) with many layers, resulting in enhanced security measures. The hierarchical secret sharing strategy developed by Shima and Doi [5] used the Information Dispersal Algorithm (IDA). The purpose of its deployment is to attain information security.

The study conducted by Botacin et al. [6] examined the use of similarity hashing algorithms in practical contexts. The researchers examined the merits and drawbacks of their approach within the framework of identifying malware research. In their study, Marcelín-Jiménez et al. [7] presented a technique aimed at evaluating the intricacy of IDA (Iterative Data Aggregation) and its significance in fault tolerance systems. In their study, Fathurrahmad and Ester [8] investigated the use of the Advanced Encryption Standard (AES) in conjunction with the Rijndael algorithm to enhancean investigation on the use of the Advanced Encryption Standard (AES) in conjunction with the Rijndael algorithm for the purpose of enhancing the security of web data. The researchers discovered that the hybrid model significantly enhances the degree of security. Kumar et al. [9] proposed the importance of AES for the execution on Field devices. Feng et al. [10] introduced hashing, AES, and RSA algorithms to enhance data security. The use of information dispersion theory is prevalent in the field of data security. According to Wijayanto and Harjito [11], it has been suggested that IDA may serve as a secure means of file storage. A approach was presented in order to limit the occurrence of rounding off mistakes in relation to IDA. The research in this area highlights the need of using hybrid techniques to ensure the security of cloud data, while also considering the requirements of post-quantum cryptography (PQC).

2.2 Key Exchange Schemes

This section provides a comprehensive assessment of the existing research on key exchange systems and the contributions made by post-quantum cryptography (PQC). The ECDH system is derived from the Diffie-Hellman exchange of keys technique. The foundation of DH lies in the Discrete logarithmic Problems (DLP) [12]. The Diffie-Hellman (DH) utilizes the multiplicative group of integers, while the Elliptic Curve Diffie-Hellman (ECDH) key exchange protocol favors the additive group of points on an elliptic curve [13]. The security approach described by Moghadam et al. [14] is based on the principles of Elliptic Curve Diffie-Hellman (ECDH) for the purposes of secured exchange of keys and streamlined authentication. The technique for enhancing cybersecurity within wireless sensor networks, known as WSNs, was successfully deployed. The study conducted by Shaikh et al. [15] focused on Elliptic Curve Cryptography (ECC). Additionally, the researchers conducted an analysis of Elliptic Curve Diffie-Hellman (ECDH) protocols. Cai et al. [16] discussed a software_defined networks (SDN). The centralization of security components might potentially facilitate their control.

Swapna and Islam et al. [17] conducted research on the use of Software-Defined Networks (SDNs) in the context of network security. During the course of their investigation, the researchers conducted an analysis of the security measures used in the IEEE 802.21 standard. The researchers conducted an investigation of the security performance of Elliptic Curve Diffie-Hellman (ECDH) for key exchange inside a Software-Defined Networking (SDN) scenario. In their study, Ghribi et al. [18] introduced a novel security mechanism that combines the use of Elliptic Curve Diffie-Hellman (ECDH) with the One Time Pad (OTP) algorithm. The purpose of this hybrid approach is to enhance the security of Unmanned Aerial Vehicle (UAV) networks. The proposed methodology adopts a hybrid strategy for enhancing the security of communications based on blockchain technology.

Li et al. [19] introduced a concept of Securing smart home networks is crucial to protect the privacy and safety of users and their connected devices. Zhang et al. [20] introduced a protocol that utilizes Elliptic Curve Diffie-Hellman (ECDH) is a key exchange protocol used to establish a shared secret key between two parties over an insecure communication channel including edge artificial intelligence (AI). The purpose of this system was to provide identification and exchange of keys that is resistant to leakage. Zhang et al. [21] introduced a Body Area Networks and collected data is often processed in real-time by onboard processors or transmitted to a central server for more in-depth analysis. Machine learning and AI algorithms can be used to extract valuable insights from the data. Santoso and Wun [22] conducted a study on the implementation of security based on Elliptic Curve Diffie-Hellman (ECDH) for the use case of integrating Internet of Things (IoT) in smart homes. Srinivas et al. [23] introduced ECDH technique inside the protocol to create a safe secret key.

The security approach presented by Zhang et al. [24] is based on the use of Elliptic Curve Diffie-Hellman (ECDH)

for networks implemented on technology. In their study, Zhang et al. [25] conducted a comprehensive examination of various security strategies used in applications. The researchers conducted an analysis on the security of several systems, including the Elliptic Curve Diffie-Hellman (ECDH) protocol, which is used for confidential exchange of keys. The Supersingular Isogeny Diffie-Hellman (SIDH) protocol is a prominent key exchange method that has been developed as a post-quantum cryptography (PQC) contender. The study conducted by Koziel et al. [26] examined the topic of Supersingular Isogeny Diffie-Hellman (SIDH), focusing on its technological execution and its resilience against quantum attacks. In addition, they implemented measures to minimize pipeline pauses via the implementation of optimum scheduling techniques. The speed of their implementation surpasses that of software libraries executing affine SIDH algorithms. Alice and Bob can produce temporary public keys within a time frame of 1.655 andthe capability to produce temporary public keys within a time frame of 1.655 as well as 1.490 billion cycles, respectively. When using Vertex-7, the performance is enhanced by a factor of 1.5 compared to the software equivalent with 512-bit SIDH. The empirical investigation conducted by the researchers demonstrated the feasibility of deploying hardware that is both efficient and reconfigurable for isogeny-based methods.

3. Proposed Integrated Security Framework For Post Quantum Crptography

This research presents a novel security architecture called the Integrated Framework for Cloud Data Security (IF-CDS), which is designed to be consistent with Post-Quantum Cryptography (PQC) standards. The framework is presented in Figure 1.

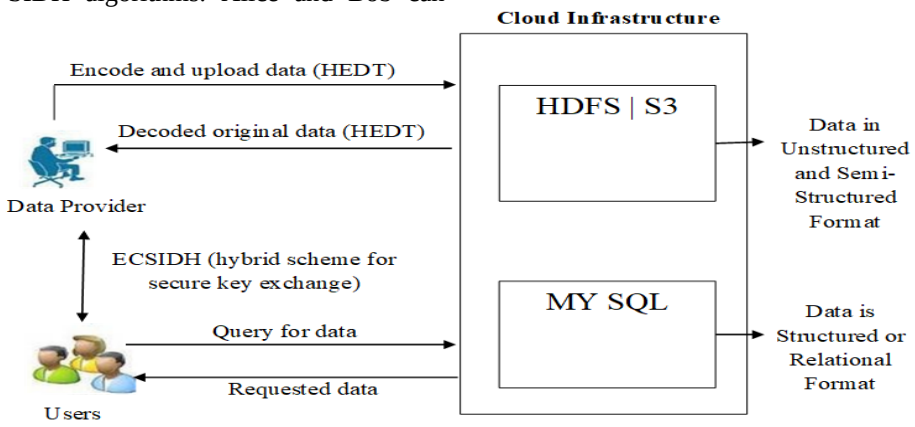

Fig 1: Integrated Framework for Cloud Data Security (IF-CDS)

The integrated framework for cloud data security has provision for secure data outsourcing and secure key exchange in multi-user environment. It is driven by PQC requirements. In the proposal there are two security schemes known as HEDT for secure cloud and ECSIDH combination scheme for secure key exchange in a multi-user distributed settings. The framework presents the data owner and users of data in distributed environment. The data owner and data users can make use of this framework for high level of security.

3.1 The Proposed Algorithm

The proposed HEDT algorithm is presented in this section. The system employs two distinct processes, namely encoding and decoding, to provide robust data transformations that enhance security measures.

Algorithm: *Hybrid Encoding and Data Transformation (HEDT)*

Encoding Procedure

1. *Start*
2. *Data owner inputs a file F*
3. $C \leftarrow ModifedAESEncrypt(F, sk)$
4. $S \leftarrow IDA(C, m, n)$
5. *For each slice s in S*
6. $s \leftarrow NovelHashing(s)$
7. *End For*
8. *Outsource S, hash and id to cloud*
9. *End*

Decoding Procedure

1. *Start*

2. $S \leftarrow GetFromCloud(id)$
3. $Data\ integrity\ verification$
4. $IF\ there\ is\ integrity\ THEN$
5. $C \leftarrow IDAReconstruction(S, m, n)$
6. $F \leftarrow ModifedAESDecrypt(C, sk)$
7. $Return\ F\ to\ data\ owner$
8. $Else$
9. $Recover\ data$
10. $End\ If$
11. End

Algorithm 1: HEDT

As seen in Algorithm 1, there are two methods included. The procedures in consideration are often referred to as the encoding process and the decoding procedure. The first option is designed to facilitate the safe and dependable outsourcing of data, whilst the later option is intended to ensure the secure and trustworthy. The individual or entity that has the data, often referred to as the data owner, submits an information file that is entrusted to an external party or service provider. The file F undergoes modified AES encryption before being subjected to additional methods. The letter F is transformed into ciphertext C. A confidential key, denoted as sk, is used during the encryption procedurethe encryption procedure, a confidential key, denoted as sk, is used. The collected information is then tested using the Incremental Data Aggregation (IDA) processof Incremental Data Aggregation (IDA) in order to produce slices that enhance the dependability, availability, and fault tolerance of the data. The underlying justification for this approach is that a limited number of cross-sectional samples may contribute to the reconstruction of variable C. The slices undergo a revolutionary hashing technique, after which the resulting data and its corresponding hash value aretogether with its corresponding hash value, is sent to a public cloud for storage. The data in question is said to possess the use of hybrid_encoding as well as numerous transformations inside a PQC-driven framework. Decoding, conversely, entails the reversal of the encoding process. The cloud receives data from an external source and through a process of reliability of data verification. The use of hashing enables the possibility of verifying data integrity. Subsequently, the ciphertext C undergoes a process of reconstruction and decryption, restoringthe restoration of the original data F, which is then returned to the rightful data owner. In the absence of data integrity, the process of data recovery is initiated.

3.2 Proposed Model of Hybrid Key Exchange

As previously mentioned within this document, the field of PQC has arisen as a means to counteract the advancements in cryptanalysis achieved via the use of both quantum and conventional computing systems. ECDH and SIDH have been identified as potential candidates for post-quantum cryptography systems. Nevertheless, in order to mitigate the potential risk associated with their individual use, it is imperative to enhance their robustness by amalgamating both strategies. This amalgamation will result in a more formidable solution for PQC in the context of key exchange. In the context of public cloud systems, where a substantial volume of information is preserved, exchanged, and maintained, it is imperative to provide robust security measures for key exchange. In order to achieve this objective, we have put forward an integrated exchange of keys approach that is designed to provide safe key exchange capabilities capable of withstanding PQC challenges. The hybrid key exchange system, referred to as ECSIDH, is a composition of two pre-existing key agreement techniques, namely ECDH and SIDH. The integration of these two methods enhances the security of the proposed system by fortifying the PQC candidate SIDH with the classical primitive elliptic curve Diffie-Hellman. While there exist varying perspectives within the PQC community, there is a strong inclination towards adopting a hybrid approach for the development of a PQC key exchange method. The SIDH and ECDH cryptographic protocols are widely recognized and used for secure key exchange purposes. This study has shown the significance of integrating these two approaches in order to develop a hybrid PQC contender.

The SIDH algorithm is well integrated with the ECDH algorithm, resulting in little additional computational costs. Nevertheless, the simplicity of the hybrid design is a distinguishing feature. The integration of the two techniques may be performed on elliptic curves that adhere to standardization protocols. In order to achieve efficient execution of ECC with enhanced speed, it is essential to include the necessary code that facilitates the implementation of ECC. The hybrid scheme's efficiency is compromised due to the disparate implementations of the two systems. ECDH and SIDH has the potential to enhance the efficacy of the scheme and mitigate issues related to incompatibility.

$Isogenous\ curves\ such\ as\ \ E_a/F_{p^2}:\ y^2 = x^3 + ax^2 + x$ are used in SIDH implementation for p= $2^{372}3^{239} - 1$. $Such\ curves\ do\ have\ \#E_a = 2^i.3^j$, the cryptographic

security of group order reflective elliptic curve cryptography (ECC) over the field E_a/F_(p^2) has been established. When considering a base field, designated as F_p, it is feasible to locate an element $a \in F\_p$ and E_a/F_p and its corresponding $quadratic\ twist$, defined as $〚E'〛\_a/F\_p$, exhibit enhanced cryptographic strength. The twist security of E_a/F_p has been investigated in [5], and it has been determined to be secure.

In this study, we conducted an investigation on the Goldilocks curve in Hamburg, as mentioned in reference [24]. Our findings indicate that this curve aligns with the mathematical expression p=3 mod 4. In addition, our study included an examination of Montgomery's ladder calculation as described in reference [37]. It was determined that the value of (a + 2)/4 remains constant within this context. It is discovered that the values of "a" resulting in the least absolute value are connected with bigger prime numbers, almost four times more than the previous values. The interval (0,p) denotes the absolute value absolute is denoted by the interval (0,p), where p is an integer. The first number, a = 624450, satisfies the given p-value. To distinguish the design of the hybrids method from those of ECDH as well as SIDH, the curves are designated with the following label.

$M\_a/F\_p: y\text{^}2 = x\text{^}3 + ax\text{^}2 + x\ with\ a\ =\ 624450.$

The idea of the Frobenius endomorphism with related trace, designated as t_(M_a), on M_a is also taken into consideration. The value of t_(M_a) may be expressed as follows.

$t\_(M\_a) =$
$0x743FC8888E1D8916BAB6DD6500AD5265DFE2E04882877C$

$26BA8CD28BE24D10D3E729B0BD07BC79699230B6BC69FEAC,$

$It\ leads\ to\ \#M_a\ = p\ +\ 1\ -t_{M_a}$
$= 4\,r_a\ and\ also\ \#M'_a$
$= p\ +\ 1\ +t_{M_a}\ =\ 4\,r'_a$

The two 749-bit prime numbers are represented as ra and r′a. According to the method outlined in reference [5], Fp has a multitude of components, with each element being linked $Ma\ or\ M'a$. The accurate execution of scalar multiplications has been seen in Montgomery's LADDER function. In the present context, it may be said that Ma exhibits resistance against twisting attacks, hence enabling the consideration of all components inside Fp as legitimate public keys. A search is conducted to determine the lowest natural number α for which the bit length of αra is the same as the bit length of (α + 1) ra – 1, with α being equal to 3. The process of parsing secret keys is performed in order to establish a range that includes values more than or equal to 3ra and less than 4ra. The use of LADDER with multidimensional factors has been previously employed. To compute $x([m]P) = LADDER(x(P), m, a)$. The aforementioned calculations are performed for values of m within the range of $(0, ra)\ and\ x(P)$ belonging to the set $P1(Fp)$. Ground fields are of utmost importance in the execution of these calculations. In terms of the development of a hybrid scheme that combines SIDH with ECDH, it has been observed that there are benefits due to the use of SIDH for the necessary computing functions. For example, the SIDH protocol has made modifications to the Montgomery LADDER function, which is used in the process of key creation over the base field E0. The availability of pre-existing routines facilitates the computation of ECDH keys, hence simplifying the procedure. The inclusion of ECDH in the capabilities of SIDH introduces a certain level of additional computational burden, however, this cost may be considered insignificant.

4. Results And Discussion

4.1 Results of HEDH

This section provides an analysis of the performance of HEDT and compares it to other established schemesincluding RSA, AES as well as DES.

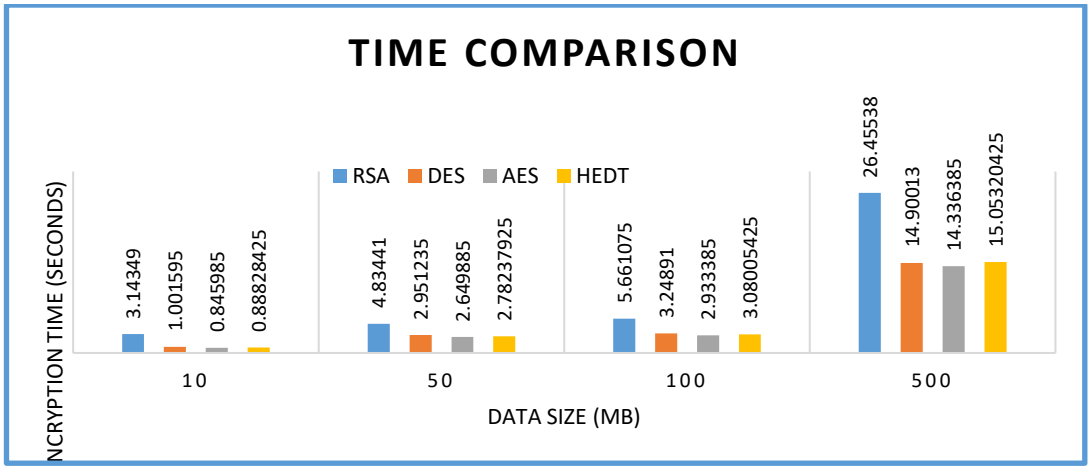

Figure 2: Time required for encryption and encoding of data based on data size

As shown in Figure 2, HEDT performs better in terms of encryption/encoding time than RSA, DES, and AES. Execution time is influenced by workload. The time taken for encryption/encoding is an indication of this. RSA takes more time than any other scheme compared to the results. As compared with AES, HEDT is shown to be a better scheme than others despite taking more time.

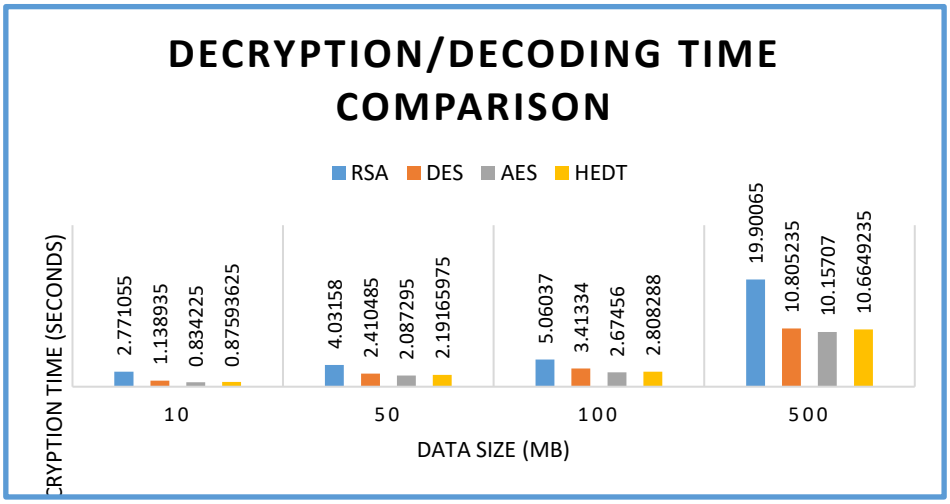

Fig 3: Data size and decryption/decoding time of security schemes

Figure 3 shows HEDT's decryption/decoding performance against other schemes such as RSA, DES, and AES. Execution time is influenced by workload. There is a clear difference in the speed at which the schemes decrypt/decode data. In comparison with all other schemes, RSA took the longest. While HEDT takes more time than AES, it is found to be better than other schemes.

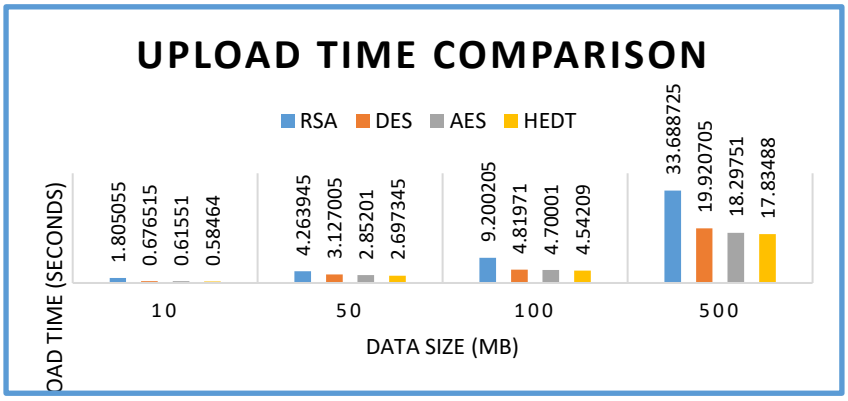

Fig 4: Data size and upload time for security schemes

A comparison of the upload time of HEDT with the upload time of other schemes such as RSA, DES and AES can be found in Figure 4.. In comparison with any other scheme, RSA took the longest. Additionally, PQC-driven security and reliability are provided by the proposed scheme HEDT.

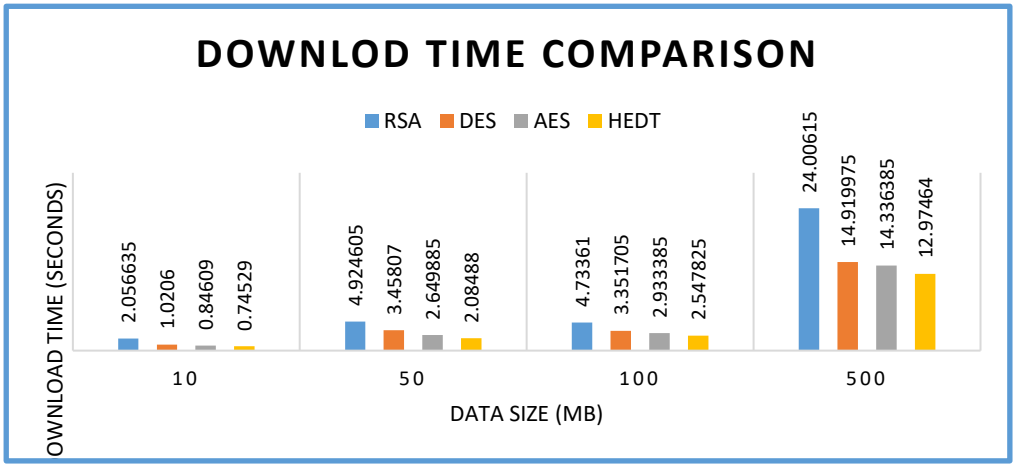

Fig 5: Data size and Download Time Comparison

It is apparent from Figure 5 that HEDT performs well when comparing download times with RSA, DES and AES when compared to those algorithms. Workload has an impact on execution time. HEDT offering PQC driven security and reliability in addition to providing better performance over other schemes.

4.2 Security Analysis of HEDT

In contrast to other methods, the suggested HEDT concept offers several advantages. The degree of security shown by the method is notably high due to the use of PQC approach. The system incorporates encoding and decoding processes that include various data transformations. The approach facilitates data accessibility by ensuring that the information is additionally saved in the cloud, but also includes IDA segments that enable the reconstruction of the original data. Despite the potential loss of data, using slices may facilitate the data recovery processof slices may facilitate the process of data recovery. This characteristic is often referred to as fault tolerance. The implementation of fault tolerance mechanisms may facilitate the process, which facilitate the verification of data integrity. Additionally, the technique facilitates enhanced efficiency in data transfer.

4.3 Results and Security Analysis of ECSIDH

The $hybrid\ PQC$ option, $ECSIDH$, is assessed with regard to of its computational efficiency and security strength. The amount of security provided by the system is assessed using the concept of bit-security, whereas its rate of operation is evaluated in terms of the closest 106 clock cycles, rounded to the next whole number. This study comparesthis study, we compare the hybrid information transfer system ECSIDH with the SIDH scheme. The experimental setup for executing the $SIDH\ and\ hybrid\ scheme$ involves using a computer (PC) equipped with the Windows 11 operating system. The PC is powered by an $Intel(R)\ Core(TM)\ i5-4210U\ CPU$ operating at a frequency of 1.70GHz. The CPU has two cores and supports four logical processors.

The security level of SIDH as well as ECSIDH is quantified in terms of the computational complexity of a challenging task. The assessment is conducted from both a classical viewpoint and a perspective based on the principles of PQC. Both views analyze the amount of security provided by SIDH in comparison to the SSDDH technique. The hybrid technique assesses security by considering the ECDHP from a classical viewpoint and the SSDDH from a PQC.

$\approx$ $bit-security$ ($hard\ problem$)		
$PERSPECTIVE/KEY\ SIZE$	$SIDH$	$ECSIDH$ ($Proposed$)
$Classical$	192	384
PQC	128	128
$Public\ Key\ Size$	564	658

Table 1: Key exchange scheme security analysis

The evaluation of the privacy level associated with SIGH and the proposed ECSIDH is shown in Table 1. The encryption key size for the SIDH protocol is 564 bits, whereas the *public key size* for the ECSIDH protocol is 658 bits. The increase in the overall key's size of ECSIDH is less than 1.17 times. The suggested approach exhibits an enhanced degree of security from a classical standpoint, as seen by a boost in public key size from $192\ bits\ to\ 384\ bits$.

$OPERATION/KEY\ SIZE$	$Speed\ (cc \times 10^6)$	
	$SIDH$	$ECSIDH$ ($Proposed$)
$Key\ Gen\ for\ Alice$	46	52
$Key\ Gen\ for\ Bob$	52	58
$Shared\ Key\ for\ Alice$	44	50
$Shared\ Key\ for\ Bob$	50	57

Table 2: Key exchange scheme cost analysis

The cost evaluation for SIGH versus the proposed ECSIDH is shown in Table 2. The publicly accessible key size for the SIDH scheme is 564 bits, whereas the general key size for the ECSIDH scheme is 658 bits. The total

computation cost of ECSIDH exhibits an average rise of just over 1.13 times when compared to SIDH. The security level of ECSIDH is much greater than that of SIDH, owing to the associated costs involved. The comparative analysis involves evaluating the $public\ key\ size$, degree of security, and operational costs of the proposed system in relation to the SIDH scheme. The increase in the publicly available key's size using ECSIDH is less than 1.17 times. The suggested approach exhibits an enhanced degree of security from a classical standpoint, as seen by a boost in public key size from $192\ bits\ to\ 384\ bits$. The total computation cost of ECSIDH exhibits an approximate rise of $less\ than\ 1.13$ times when compared to SIDH. The security level of ECSIDH is much greater than that of SIDH, owing to the associated incurred expense. In comparison to its predecessor, the ECSIDH demonstrates enhanced security strength as a PQC contender. This improvement is achieved by a modest increase in the size of the public key, which is less than 1.17 times larger, and an overall processing cost that is just 1.13 times more. Assuming that the advantages of enhancing security, such as increased resistance to attacks, are not accompanied by significant increases in the amount of public keys or the total computing cost. Hence, it can be inferred that the ECSIDH scheme presents a more favorable option for PQC in comparison to the SIDH scheme.

5. Conclusion And Future Work

In this paper, we proposed an integrated cloud data security framework with novel schemes towards PQC. For data security with encryption and decryption, we proposed HEDT algorithm. Our proposal for key exchange is called ECSIDH. In addition to ECDH, SIDH is another key agreement scheme. PQC candidate SIDH is strengthened with classical primitive ECDH by combining these two schemes. The ECSIDH is found more secure than individual key exchange scheme such as SIDH. Security analysis of HEDT revealed that it is more secure than existing algorithms and ECSIDH is more secure PQC candidate. The integrated security framework meant for cloud data security and key exchange with PQC candidates needs further evaluation with real time environment. It will be our future endeavour towards improving the integrated security framework.

References

[1] Lee, Bih-Hwang; Dewi, Ervin Kusuma; Wajdi, Muhammad Farid (2018). 2018 27th Wireless and Optical Communication Conference (WOCC) - Data security in cloud computing using AES under HEROKU cloud. , p1–5.DOI:10.1109/WOCC.2018.8372705

[2] Yu, Liting; Zhang, Dongrong; Wu, Liang; Xie, Shuguo; Su, Donglin; Wang, Xiaoxiao (2018). 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) - AES Design Improvements Towards Information Security Considering Scan Attack. , p322–326. DOI: 10.1109/TrustCom/BigDataSE43156.2018

[3] Chinnasamy, P.; Deepalakshmi, P. (2018). 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT) - Design of Secure Storage for Health-care Cloud using Hybrid Cryptography. , p1717–1720.DOI: 10.1109/ICICCT.2018.8473107

[4] Qian, Quan; Yu, Zhi-ting; Zhang, Rui; Hung, Che-Lun (2018). A multi-layer information dispersal based encryption algorithm and its application for access control. Sustainable Computing: Informatics and Systems, p1-12.https://doi.org/10.1016/j.suscom.2018.06.001

[5] Botacin, M., Galhardo Moia, V. H., Ceschin, F., Amaral Henriques, M. A., & Grégio, A. (2021). Understanding uses and misuses of similarity hashing functions for malware detection and family clustering in actual scenarios. Forensic Science International: Digital Investigation, 38, 301220, p1-19.https://doi.org/10.1016/j.fsidi.2021.301220

[6] Marcelin-Jimenez, Ricardo; Ramirez-Ortiz, Jorge Luis; De La Colina, Enrique Rodriguez; Pascoe-Chalke, Michael; Gonzalez-Compean, Jose Luis (2020). On the Complexity and Performance of the Information Dispersal Algorithm. IEEE Access, 8, p159284–159290.DOI: 10.1109/ACCESS.2020.3020501

[7] Fathurrahmad, Ester. (2020). Development And Implementation Of The Rijndael Algorithm And Base-64 Advanced Encryption Standard (AES) For Website Data Security. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH. 9 (11), p6-9.DOI: 10.23919/FRUCT.2019.8711955

[8] Kumar, Keshav; Ramkumar, K.R.; Kaur, Amanpreet (2020). IEEE 2020 8th International Conference on Reliability, Infocom Technologies and Optimization. A Design Implementation and Comparative Analysis of Advanced Encryption Standard (AES) Algorithm on FPGA. , p182–185.DOI: 10.1109/ICRITO48877.2020.9198033

[9] Feng, Ruijue; Wang, Zhidong; Li, Zhifeng; Ma, Haixia; Chen, Ruiyuan; Pu, Zhengbin; Chen, Ziqiu; Zeng, Xianyu (2020). A Hybrid Cryptography Scheme for NILM Data Security. Electronics, 9(7), p1-18.; https://doi.org/10.3390/electronics9071128

[10] Wijayanto, Ardhi; Harjito, Bambang (2019). 2019 International Conference on Computer, Control, Informatics and its Applications (IC3INA) - Reduce

Rounding Off Errors in Information Dispersal Algorithm. , p36–40.

[11] Borges, F., Reis, P. R., & Pereira, D. (2020). A Comparison of Security and its Performance for Key Agreements in Post-Quantum Cryptography. IEEE Access, 8, p142413–142422.DOI: 10.1109/ACCESS.2020.3013250

[12] Moghadam, M. farhadi, Nikooghadam, M., Jabban, M. A. B. A., Alishahi, M., Mortazavi, L., & Mohajerzadeh, A. (2020). An efficient authentication and key agreement scheme based on ECDH for wireless sensor network. IEEE Access, 8, p73182–73192.DOI: 10.1109/ACCESS.2020.2987764

[13] Shaikh, J. R., Nenova, M., Iliev, G., & Valkova-Jarvis, Z. (2017). Analysis of standard elliptic curves for the implementation of elliptic curve cryptography in resource-constrained E-commerce applications. 2017 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS). p1-4.DOI: 10.1109/COMCAS.2017.8244805

[14] Cai, J., Huang, X., Zhang, J., Zhao, J., Lei, Y., Liu, D., & Ma, X. (2018). A Handshake Protocol With Unbalanced Cost for Wireless Updating. IEEE Access, 6, p18570–18581.DOI: 10.1109/ACCESS.2018.2820086

[15] Swapna, A. I., & Islam, N. (2017). Security analysis of IEEE 802.21 standard in software defined wireless networking. 2017 20th International Conference of Computer and Information Technology (ICCIT). p1-5.DOI: 10.1109/ICCITECHN.2017.8281843

[16] Ghribi, E., Khoei, T. T., Gorji, H. T., Ranganathan, P., & Kaabouch, N. (2020). A Secure Blockchain-based Communication Approach for UAV Networks. 2020 IEEE International Conference on Electro Information Technology (EIT). p411-415DOI: 10.1109/EIT48999.2020.9208314

[17] Li, Y., Zhang, Z., Wang, X., Lu, E., Zhang, D., & Zhang, L. (2019). A Secure Sign-On Protocol for Smart Homes over Named Data Networking. IEEE Communications Magazine, 57(7), p62–68.DOI: 10.1109/MCOM.2019.1800789

[18] Zhang, J., Zhang, F., Huang, X., & Liu, X. (2020). Leakage-Resilient Authenticated Key Exchange for Edge Artificial Intelligence. IEEE Transactions on Dependable and Secure Computing, p1–13.DOI: 10.1109/TDSC.2020.2967703

[19] Wang, J., Han, K., Alexandridis, A., Zilic, Z., Pang, Y., & Lin, J. (2018). An ASIC Implementation of Security Scheme for Body Area Networks. 2018 IEEE International Symposium on Circuits and Systems (ISCAS). p1-5.DOI: 10.1109/ISCAS.2018.8351098

[20] Srinivas, J., Mishra, D., Mukhopadhyay, S., & Kumari, S. (2017). Provably secure biometric based authentication and key agreement protocol for wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 9(4), p875–895.DOI: 10.1109/ICCITECHN.2017.8281843

[21] Zhang, Y., Weng, J., Ling, Z., Pearson, B., & Fu, X. (2020). BLESS: A BLE Application Security Scanning Framework. IEEE INFOCOM 2020 - IEEE Conference on Computer Communications. p636-645.DOI: 10.1109/INFOCOM41043.2020.9155473

[22] Zhang, J., Rajendran, S., Sun, Z., Woods, R., & Hanzo, L. (2019). Physical Layer Security for the Internet of Things: Authentication and Key Generation. IEEE Wireless Communications, p1–7.DOI: 10.1109/MWC.2019.1800455

[23] Koziel, B., Azarderakhsh, R., Mozaffari Kermani, M., & Jao, D. (2017). Post-Quantum Cryptography on FPGA Based on Isogenies on Elliptic Curves. IEEE Transactions on Circuits and Systems I: Regular Papers, 64(1), p86–99.DOI: 10.1109/TCSI.2016.2611561

[24] Weiqiang Liu, Jian Ni, Zhe Liu, Chunyang Liu and Maire O'Neill. (2019). Optimized Modular Multiplication for Supersingular Isogeny Diffie-Hellman. *IEEE*, P1-8.DOI: 10.1109/TC.2019.2899847

[25] Joppe W. Bos and Simon J. Friedberger. (2018). Arithmetic Considerations for Isogeny-Based Cryptography. *IEEE*, P1-12.DOI: 10.1109/TC.2018.2851238

[26] Craig Costello, Patrick Longa and Michael Naehrig. (2016). Efficient algorithms for supersingular isogeny Diffie-Hellman, https://doi.org/10.1007/978-3-662-53018-4_21P1-34.