Indonesian Journal of Electrical Engineering and Computer Science
Vol. 12, No. 3, December 2018, pp. 1143~1150
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v12.i3.pp1143-1150

Secure and Efficient Bi-Directional Proxy Re-Encyrption Technique

Chadrakala[1], S. C. Lingareddy[2]
[1]Department of CSE, VTU, Bangalore, India
[2]Department of CSE, ACE, Bangalore, India

Article Info

Article history:

Received Jan 3, 2018
Revised Apr 23, 2018
Accepted Aug 21, 2018

Keywords:

Cryptography
Data sharing
Proxy Re-encryption
Security

ABSTRACT

The low cost availability of smart devices and broadband connection has led to rapid growth of communication over Internet. As of today the internet based communication service is widely used in various application services such as in E-Mail transaction of sensitive data (medical data), online money transaction etc. all these services requires a strong security. There has been continuous ongoing research by various cryptanalyst to enhance security of cryptography especially in semi-untrusted server. However, performance, computation time and ease of use play a significant role in using the algorithm for implementation. Proxy re-encryption plays a significant role in protecting data that are stored in semi-untrusted server. Many existing Proxy re-encryption technique induces high computation overhead due to adoption of public key cryptography such RSA (Rivet Shamir Adleman), ECC (Elliptical Curve Cryptography) etc. and it suffer from quantum attack. To address this lattice based cryptography is adopted by various approaches which is based on Learning With Error which shows resilience against quantum attacks such Chosen Cipher data attack and Chosen Plain Text attack. The drawback with existing lattice cryptography based approach is that they are unidirectional and adopts bilinear pairing which compromise security and induces high computation cost. To address this work present a Bidirectional Proxy Re-encryption scheme by adopting lattice based cryptography technique. Experiment is conducted for computation overhead by varying key and data size which attained significant performance improvement over existing Proxy Re-encryption scheme.

Corresponding Author:

Chadrakala,
Department of CSE,
VTU, Bangalore, India.
Email: chadrakala.pi@gmail.com

1. INTRODUCTION

The wide availability low cost broadband/internet service has led to the growth of financial and business across various industries/organization. The growth of internet has led the organization to deliver customer services online such as social networking, online transaction, and customer service and so on. Internet has been integral part of every user as of today. Despite these benefit it still faces several issues and challenges such as integrity, confidentiality and privacy of data which is not trustable. To address this, cryptography mechanism has been adopted. Encryption and decryption is the integral part of cryptography mechanism. In Encryption the message are encoded by sender by applying some transformation technique and in decryption the message are decoded by receiver. The cryptographic technique has been adopted in various domains such as cloud, social networking, Email service etc. when developing cryptography mechanism generating unbreakable cipher data is an art not technology. With the availability of high

computing device and cloud technologies have led to development of strong cryptography mechanism which is the need of the hour.

Let consider a scenario that a person is on vacation and he is not able to access internet/mail. You would want the server to forward your encoded mail data to the receiver B who can decrypt the cipher data using his private key. A simple way is to store the private key in mail server. In that case when user receive the mail the server decode it using private key that is stored in server and re-encrypt message using B's public key. Yet, such method is not desired solution, particularly for untrusted service provider [1-3], since the provider can obtain both your private key and actual data.

Proxy Re-Encryption [4] is an efficient strategy that assures sender secure storage and sharing of data/message on public storage environment and solves key management problems [4-5]. Proxy Re-Encryption has been adopted by application domain ranging from encrypted email forwarding [6], vehicular ad hoc networks (VANETs) [7-8] digital right management (DRM) [9-10], distributed computing [11-12], to group key management [13]. In Proxy Re-Encryption scheme a sender encode it file using public key and then store the cipher data on the semi-trusted server. When receiver request for data, the sender send the proxy key or re-encryption key associated with the intended receiver to the server as proxy. Then the receiver receives the re-encrypted cipher text then finally the receiver decrypt the cipher text with his private key to retrieve original data. The Proxy Re-Encryption technique generally assures security (1) that the proxy cannot re-encrypt the cipher data in a useful form before receiving the encryption key, and (2) that neither the receiver nor the server/proxy can obtain meaningful information of re-encrypted data.

The Proxy Re-Encryption is of two forms unidirectional and bi-directional. If re-encryption key $a^{k_{1,2}}$ inevitably permits the proxy to transform cipher data under a^{k_1} into cipher data under a^{k_2} then it is called as unidirectional. If re-encryption key $a^{k_{1,2}}$ inevitably permits the proxy to transform cipher data under a^{k_1} into cipher data under a^{k_2} and vice versa, then it is called as bidirectional. Any unidirectional scheme can be transformed into bidirectional but converse should hold. In [1], [3] presented a bilinear pairing unidirectional Proxy Re-Encryption to protect against CPA (Chosen Plaintext Attack). However it lacks security to protect attack against CCA (Chosen Cipher data Attack). To address this [14] presented CCA-secure bidirectional Proxy Re-Encryption technique. To address RCCA (Repayable Attack Chosen-Cipher data) security [15] presented a unidirectional Proxy Re-Encryption technique. Both these technique adopt bilinear pairing which requires high computation cost for modular exponentiation in finite fields [16] which adopts public key based cryptography mechanism.

To address this lattice based cryptography mechanism is adopted by various approaches. To resist the quantum attack, [17] presented the first lattice based Proxy Re-Encryption mechanism that realizes non-interactivity and collusion resilience. Further they presented, the security proof of their methodology is given in the selective model under the Learning with Error [18] assumption. As in [18-19] the Learning with Error assumption analytically has strong connection to lattice hardness assumptions, which are assumed safe in various factors. Though, there are passible "attacks" on Learning with Error, as in [20-22]. Therefore when designing a Learning with Error we need consider real world environment threat as in [20] among them Search-Learning with Error is most effective attack. In [23] presented unidirectional and multiple usage Proxy Re-Encryption technique by adopting multi-linear map [24] considering strong multi-linear groups and address the issues of [14] in designing Proxy Re-Encryption unidirectional and multihop.

This work presents a Bidirectional Proxy Re-encryption scheme by adopting lattice based cryptography technique which is multihop (it supports multiple re-encryptions). The paper organization is as follows: In section two the proposed Bidirectional Proxy Re-encryption scheme is presented. Section three the experimental result are discussed. The last section paper is concluded with future work.

2. LITERATURE SURVEY

To improve the security and computation complexity in implementing cryptography mechanism various methodologies have been proposed in recent times among them proxy Re-encryption is the most sorted out mechanism which are surveyed below.

In [25] presented a Proxy Re-Encryption which adopts state of art public key cryptography. Their model depends on the validity of public key to verify certificate. Before encrypting a message sender has to verify its certificate [26]. In order to address the overhead caused for verification of certificate in public key cryptography Identity based Proxy Re-Encryption [27] is presented, which incorporates identity for encryption [28]. The model in [29] proved random hash model in random oracle is secure and [28] in standard model.

In [27] proved a case of stronger security in standard model for chosen-cipher data attack. These model supports only coarse-grained data sharing i.e. user sends the key to proxy server, all cipher data can be re-encrypted and then the intended user can access these data, else the cipher data are not accessible by any

user and cipher data cannot be re-encrypted. To address this in [30] presented conditional based Proxy Re-Encryption which achieved fine grained access mechanism which is considered to be safe against chosen-cipher attack.

In [30] they combined the both conditional and identity based Proxy Re-Encryption and in [31] they combined both conditional based Proxy Re-Encryption and broadcast encryption and they achieve fine-grained access and assure security against chosen cipher data attack and chosen plain message attack and they support one to many user data sharing.

In [25] presented a Proxy Re-Encryption methodology to support anonymous data sharing. In [32] they extended this and presented a bi-directional Re-Encryption which support multihop (multiple re-encryptions) among two users. These scheme support security against attack chosen cipher attack in standard and random oracle model, similarly in contrast in [33] presented multihop unidirectional Proxy Re-Encryption technique. The issue with these techniques is that they used public based cryptography such as RSA, Diffe Hellman etc. which induce high key computation overhead and are prone to quantum attack [17]. To address this [17] presented a lattice based Proxy Re-Encryption cryptography technique which is collusion resilient collusion resilience and non-interactivity. Further they provided security under Learning With Error case.

In [34] presented a lattice based Proxy Re-Encryption technique, namely Key-private Proxy Re-Encryption. Here they identified the computation overhead due to bilinear pairing, adoption of group based public key cryptography and Learning With Error correctness. They also identified when pairing is considered they will never guarantee long term safety especially against quantum attacks. The Learning With Error is a hardness problem and involves long-term security issues, they showed that the existing Learning With Error is prone to real world attack [22]. To address all these here they presented Key-private Proxy Re-Encryption, which does not leak any information of both sender and receiver and provides additional confidentiality due to Pseudo-arbitrary proxy key generation. Their model is chosen plaintext attack secure in standard model and chosen cipher data Attack secures in random oracle model. They approach is multihop and unidirectional and provided security with standard Learning With Error. The drawback with this strategy is that the proxy Re-Encryption involves high computation due to inverse transformation of proxy keys and they are unidirectional. To address this work propose a Proxy Re-Encryption technique which is multihop and bi-directional which is presented in next section below.

3. PROPOSED MODEL

This work present Bidirectional Proxy Re-encryption scheme by adopting lattice based cryptographic technique and architecture of Proxy Re-encryption is shown in Figure 1.

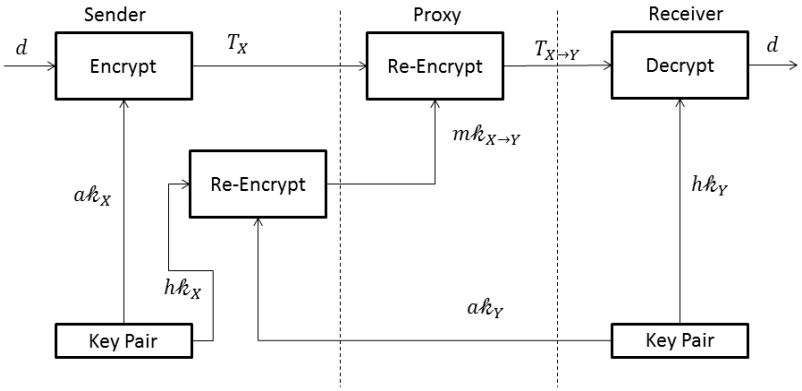

Figure 1. Architecture of Proxy Re-Encryption

Let the Alice be person X and bob be person Y. The proposed Bidirectional Proxy Re-encryption scheme consists of following entities.

GenerateKey( ): A pair of public and master key $(a\hbar_X, m\hbar_X)$ is the outcome of generate key function strategies for person X. If it randomly selects a polynomial pairs of $(h_X, n_X) \in F_Q^2$, with fixed coefficient equivalent to $0, -1$ and the h_X has to be congruent to 1 mod a. The public key consist of $a\hbar_X$that polynomial $t_X = a \cdot n_X . \frac{1}{h_X} \% b$ were the private key $h\hbar_X$is the polynomial h_x.

RegenerateKey($m\hbar_X, m\hbar_Y$): The input for re-encryption strategy is master key $m\hbar_X = h_x$ and $m\hbar_Y = h_Y$. The re-encryption key is computed among person X and Y as $p\hbar_{X\to Y} = m\hbar_X \cdot m\frac{1}{h_Y} = h_X \cdot \frac{1}{h_Y}$. The proxy key is computed where neither proxy nor X, Y can obtain information about master key is as follows, Let X choose an arbitrary $p \in {}^{F_Q}/_b$ and transmit p to proxy and $p \cdot h_X \% b$ to Y. Similarly Y transmits $p \cdot h_X \cdot \frac{1}{h_Y} \% b$ to the proxy and then computation is done by proxy as $ph_{X\to Y} = h_X \cdot \frac{1}{h_Y} \% b$.

Encrypt$(a\hbar_X, D)$: On a given public key $a\hbar_X$ and data $D \in {}^{F_Q}/_b$ as input, the encrypt function produces a ciphertext $T_X = l_X m + D$ as and produces a trivial arbitrary polynomial $m \in {}^{F_Q}/_b$ as output.

ReEncrypt$(p\hbar_{X\to Y}, T_X)$: On a given ciphertext T_X and re-encryption key $p\hbar_{X\to Y}$ as input. The ReEncrypt function generates ciphertext $T_Y = T_Y \cdot p\hbar_{X\to Y} + aw$ and generates arbitrary polynomial $w \in {}^{F_Q}/_b$ as output.

Decrypt$(m\hbar_X, T_X)$: On a given ciphertext T_X and master key $m\hbar_X = h_x$ as input. The Decrypt function process $\mathbb{T}_X = (T_x \cdot h_x) \% b$ and produces the actual data $D = (\mathbb{T}_X \% a)$as output.

The Re-Encrypted cipher data form are represented as follows:

$$\begin{aligned} T_X &= (T_x \cdot p\hbar_{X\to Y} + aw) \\ &= \left(an_X {}^{1}/_{h_X} m + D\right).h_X {}^{1}/_{h_Y} + aw \\ &= an_X {}^{1}/_{h_Y} m + aw + h_X {}^{1}/_{h_Y} D \end{aligned} \quad (1)$$

When the re-encrypted cipher data is decrypted, the receiver multiplies the cipher data with its master key h_X is as follows:

$$\begin{aligned} T_Y \cdot T_X &= \left(an_X {}^{1}/_{h_Y} + aw + h_X {}^{1}/_{h_Y} D\right).h_B \\ &= an_X m + awh_Y + h_X D \end{aligned} \quad (2)$$

The additional term is get ridden by obtaining mod a and to obtain $H_X = 1 \% a$ we required master key polynomial h_X, therefore $(T_Y \cdot h_Y) \% a = (an_X m + awh_Y + h_X D) \% a = D$, which is the actual data.

To prevent the simple cipher data only attack from the receiver we include the term w in the process of re-encryption. Let consider that the cipher data form as $T_Y = T_x \cdot p\hbar_{X\to Y} = T_x \cdot h_X {}^{1}/_{h_Y}$ i.e. without arbitrary w. Then the receiver could compute the master key of the sender based on criteria that $T_Y \cdot h_Y = T_X \cdot h_X$ is true, since $T_Y = T_X \cdot p\hbar_{X\to Y}$. Now let consider that T_X is invertible mod b, the malicious/intruder can compute the master key by evaluating $h_X = {}^{1}/_{T_X} \cdot T_Y \cdot h_Y$. Our models support multiple re-encryptions and it is bidirectional i.e. $p\hbar_{X\to Y} = h_X {}^{1}/_{h_Y}$, the proxy can compute $p\hbar_{Y\to X} = {}^{1}/_{(p\hbar_{X\to Y})} = h_X {}^{1}/_{h_Y}$. This shows how the re-encryption keys are computed$\left(p\hbar_{X\to Y} = m\hbar_X . {}^{1}/_{m\hbar_Y}\right)$, for bidirectional methodology.

The proposed Bidirectional Proxy Re-encryption scheme is evaluated and compared with existing Proxy Re-encryption scheme in terms of computation overhead for varied key and data size which is shown in below section.

4. EXPERIMENTAL RESULT AND ANALYSIS

We The experiment is conducted on windows 2007 enterprises operating system, I-5 3.2 Ghz quad core processor, CUDA NVIDIA 2GB dedicated graphic card, 8 GB Ram. The Proposed and Existing algorithm [34] is implemented by using java cryptography libraries in eclipse Neon IDE (version 4.6). Simulation is conducted by varying key size and keeping the file size constant (1024 bytes) and the computation time are noted for Encryption, Re-encryption, Decryption and Total computation time (ms). The total computation is composed of the entire process including time taken to generate key.

In Figure 2 the key sizes are varied and simulation is conducted for both proposed and existing method. The performance improvement of proposed model for encryption when key size is (256-1536) is 16.67%, for (256-4094) is 13.05% and for (320-4094) is 14.53% over Existing model. An average improvement of 14.75% is achieved by Proposed Model over Existing Model interm of computation time for encryption.

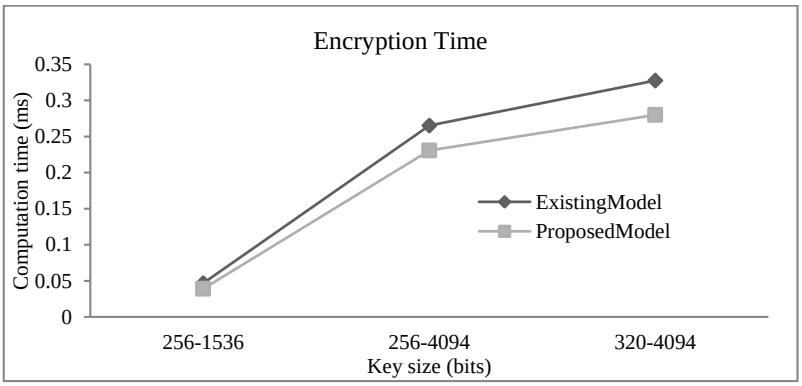

Figure 2. Computation time for Encryption for varied key size

In Figure 3 the key sizes are varied and simulation is conducted for both proposed and existing method. The performance improvement of proposed model for re-encryption when key size is (256-1536) is 94.32%, for (256-4094) is 95.78% and for (320-4094) is 95.47% over Existing model. An average improvement of 94.001% is achieved by Proposed Model over Existing Model interm of computation time for re-encryption.

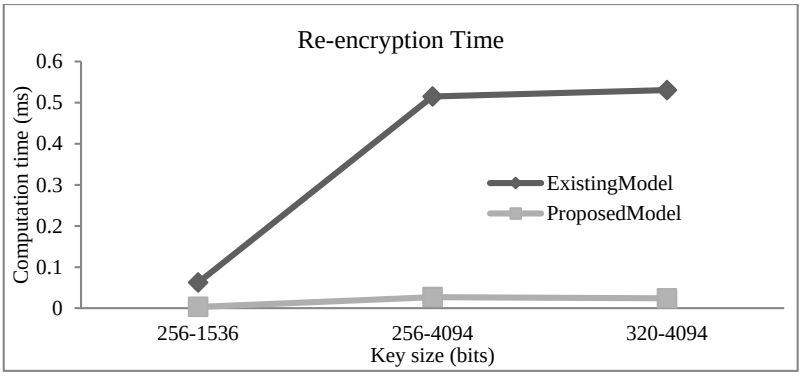

Figure 3. Computation time for Re-encryption for varied key size

In Figure 4 the key sizes are varied and simulation is conducted for both proposed and existing method. The performance improvement of proposed model for decryption when key size is (256-1536) is 18.97%, for (256-4094) is 21.26% and for (320-4094) is 20.64% over Existing model. An average improvement of 20.208% is achieved by Proposed Model over Existing Model interm of computation time for decryption.

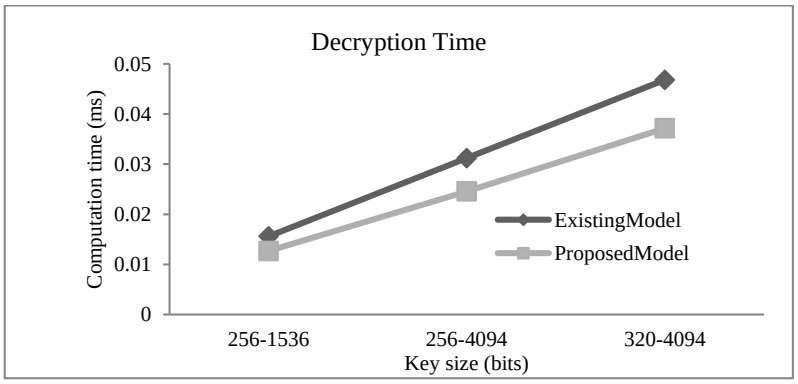

Figure 4. Computation time for Decryption for varied key size

In Figure 5 the key sizes are varied and simulation is conducted for both proposed and existing method. The performance improvement of proposed model for key generation when key size is (256-1536) is 23.08%, for (256-4094) is 25.12% and for (320-4094) is 24.43% over Existing model. An average improvement of 24.21% is achieved by Proposed Model over Existing Model interm of computation time for key generation.

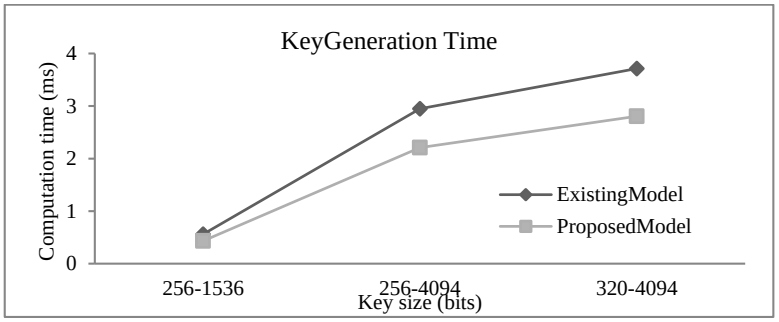

Figure 5. Computation time for Key Generation for varied key size

In Figure 6 the key sizes are varied and simulation is conducted for both proposed and existing method. The performance improvement of proposed model for Proxy key generation when key size is (256-1536) is 33.33%, for (256-4094) is 35.17% and for (320-4094) is 36.25% over existing model. An average improvement of 34.92% is achieved by Proposed Model over Existing Model interm of computation time for Proxy key regeneration.

In Figure 7 the key sizes are varied and simulation is conducted for both proposed and existing method. The performance improvement of proposed model when key size is (256-1536) is 43.33%, for (256-4094) is 47.02% and for (320-4094) is 51.03% over Existing model. An average improvement of 52.82% is achieved by Proposed Model over Existing Model interm of total computation time.

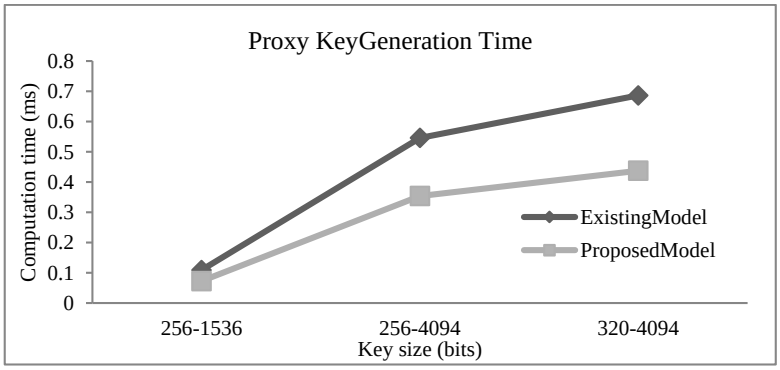

Figure 6. Computation time for Key Generation for varied key size

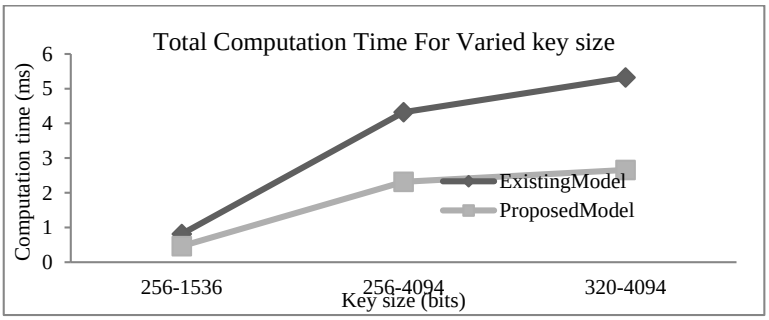

Figure 7. Total computation time for varied key size

To further evaluate robustness of our strategy the file size is varied and keeping the key size constant at (256-4094) and experiment are conducted. In Figure 8 the file sizes are varied and simulation is conducted for both proposed and existing method. The performance improvement of proposed model when file size is (128 bytes) is 57.86%, for (256 bytes) is 52.35% and for (512 bytes) is 52.35% and for (1024 bytes) is 54.76 over Existing model. An average improvement of 55.18% is achieved by Proposed Model over Existing Model in terms of total computation time.

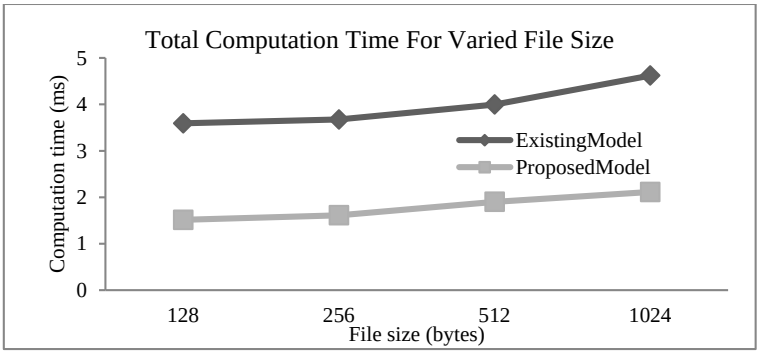

Figure 8. Total computation time for varied file size.

5. CONCLUSION

Providing security to data with least computation overhead is most desired. The existing technique adopts unidirectional based proxy re-encryption technique. To overcome the quantum security issue of public key cryptography many existing proxy re-encryption approaches have adopted lattice based cryptography mechanism which attained significant performance improvement but these techniques are unidirectional and induce decryption error for multiple re-encryption. Here we proposed a Bidirectional Proxy Re-encryption scheme by adopting lattice based cryptography technique which is multi-hop. The proposed model achieves significant performance improvement in terms of computation overhead over existing model. Simulation is conducted by varying key and file size an average improvement of 52.82% and 55.18 respectively is achieved by proposed Proxy Re-encryption model over existing model in term of computation overhead. In future we would extend our proxy Re-Encryption on to cloud environment and evaluate the performance.

REFERENCES

[1] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. "Improved Proxy Reencryption Schemes with Applications to Secure Distributed Storage". *ACM TISSEC*, 9(1):1-30, Feb 2006.
[2] Tony Smith. "DVD Jon: buy DRM-less Tracks from Apple iTunes March 18, 2005". Available at http://www.theregister.co.uk/2005/03/18/itunes_pymusique.
[3] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. "Improved Proxy Reencryption Schemes with Applications to Secure Distributed Storage". In *NDSS*, pages 29-43, 2005.
[4] M. Blaze, G. Bleumer and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography", *Proc. Advances* in *Cryptology- EUROCRYPT*' 98, Springer, Heidelberg, 1998, pp. 127-144.
[5] Matt Blaze and Martin Strauss. "Atomic proxy cryptography". *Technical report, AT&T Research*, 1997.
[6] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Advances in Cryptology–EUROCRYPT'98. Springer*, 1998, pp. 127–144.
[7] H. Xiong, Z. Chen, and F. Li, "Efficient privacypreserving authentication protocol for vehicular communications with trustworthy," *Security and Communication Networks*, vol. 5, no. 12, pp. 1441–1451, 2012.
[8] Neelambike S, Chandrika J, "An Efficent Distributed Medium Access Control for V2I VANET", *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS).* Vol. 9, No. 3, March 2018, pp. 742~751 ISSN: 2502-4752, DOI: 10.11591/ijeecs.v9.i3.pp742-751.
[9] S. Lee, H. Park, and J. Kim, "A secure and mutualprofitabledrm interoperability scheme," in *Proceedings of IEEE Symposium on Computers and Communications. IEEE*, 2010, pp. 75–80.
[10] G. Taban, A. A. C´ardenas, and V. D. Gligor, "Towards a secure and interoperable drm architecture," in *Proceedings of the ACM Workshop on Digital Rights Management*. ACM, 2006, pp. 69–78.
[11] Nur Hazwani Hussin, Azizan, M.M, Ali, A, Albreem, M. A. M, "Encryption Techniques and Wireless Power Transfer Schemes", *Indonesian Journal of Electrical Engineering and Computer Science(IJEECS)* Vol. 9, No. 1, January 2018, pp. 183~190 ISSN: 2502-4752, DOI: 10.11591/ijeecs.v9.i1.pp183-190.

[12] G. Ateniese, K. Fu, M. Green, and S. Hohenberger "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Transactions on Information and System Security (TISSEC'06)*, vol. 9, no. 1, pp. 1–30, 2006.
[13] Y.-R. Chen, J. Tygar, and W.-G. Tzeng, "Secure group key management using uni-directional proxy reencryption schemes," in *IEEE International Conference on Computer Communications. IEEE*, 2011, pp. 1952–1960.
[14] R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy re-encryption," in *Proceedings of the 14th ACM conference on Computer and communications security*. ACM, 2007, pp. 185–194.
[15] B. Libert and D. Vergnaud. "Unidirectional Chosen-Ciphertext Secure Proxy Re- encryption". In *Proc. of PKC'08, LNCS 4929*, pp. 360-379, Springer-Verlag, 2008.
[16] J. Baek, R. Safavi-Naini, and W. Susilo. "Certificateless Public Key Encryption without Pairing". In *Proc. of ISC'05. LNCS 3650*, pp. 134-148, Springer-Verlag, 2005.
[17] E. Kirshanova, "Proxy re-encryption from lattices," in *Public Key Cryptography–PKC'14. Springer*, 2014, pp. 77–94.
[18] Regev, "O. "On lattices, learning with errors, random linear codes, and cryptography". In: *Gabow, H.N., Fagin, R. (eds.) STOC*, pp. 84–93. ACM (2005).
[19] Brakerski, Z., Langlois, A., Peikert, C., Regev, O., Stehl´e, D. "Classical hardness of learning with errors". In: *Boneh, D., Roughgarden, T., Feigenbaum, J. (eds.) STOC*, pp. 575–584. ACM (2013).
[20] Rckert, M., Schneider, M. "Estimating the security of lattice-based cryptosystems". *Cryptology ePrint Archive*, Report 2010/137 (2010), http://eprint.iacr.org/.
[21] Micciancio, D., Regev, O. "Lattice-based cryptography". In: *Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.) Post-Quantum Cryptography*, pp. 147–191. Springer, Heidelberg (2009).
[22] Lindner, R., Peikert, C. "Better key sizes (and attacks) for LWE-based encryption". In: *Kiayias, A. (ed.) CT-RSA 2011*. LNCS, vol. 6558, pp. 319–339. Springer, Heidelberg (2011).
[23] T. Fei, L. Hongda, and J. Chang, "Multi-hop unidirectional proxy re-encryption from multilinear maps", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 98, no. 2, pp. 762–766, 2015.
[24] S. Garg, C. Gentry, and S. Halevi, "Candidate multilinear maps from ideal lattices." in *Advances in Cryptology–Eurocrypt'13*, vol. 7881. Springer, 2013, pp. 1–17.
[25] J. Shao, P. Liu, G. Wei and Y. Ling, "Anonymous proxy reencryption", *Security and Communication Networks*, vol. 5, no. 5, 2012, pp. 439-449.
[26] Boldyreva, M. Fischlin, A. Palacio and B. Warinschi, "A Closer Look at PKI: Security and Efficiency", Proc. PKC 2007 Springer, Heidelberg, 2007, pp. 458-475
[27] C.-K. Chu and W.-G. Tzeng, "Identity-Based Proxy Re-encryption without Random Oracles", *Proc. ISC 2007, Springer*, Heidelberg, 2007, pp. 189-202.
[28] T. Matsuo, "Proxy Re-encryption Systems for Identity-Based Encryption", *Proc. PAIRING 2007, Springer*, Heidelberg, 2007, pp. 247-267.
[29] M. Green and G. Ateniese, "Identity-Based Proxy Re-Encryption", *Proc. ACNS 2007, Springer, Heidelberg*, 2007, pp. 288-306.
[30] K. Liang, Z. Liu, X. Tan, D.S. Wong and C. Tang, "A CCA-Secure identity-based conditional proxy re-encryption without random oracles", *Proc. ICISC, 2012*, pp. 231-146.
[31] Mohammad Rasmi AL-Mousa, Fadi Al-salameen, Khaled Al-Qawasmi, "Using Encryption Square Key with One-dimensional Matrix for Enhancing RGB Color Image Encryption-Decryption", *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)* Vol. 9, No. 3, March 2018, pp. 771~777 ISSN: 2502-4752, DOI: 10.11591/ijeecs.v9.i3.pp771-777.
[32] T. Matsuda, R. Nishimaki and K. Tanaka, "CCA Proxy Re- Encryption without Bilinear Maps in the Standard Model", *Proc. PKC 2010 Springer*, Heidelberg, 2010, pp. 261-278.
[33] V. Kirtane and C.P. Rangan, "RSA-TBOS signcryption with proxy re-encryption", *Proceedings of the 8th ACM workshop on Digital rights management (DRM '08)*, 2008, pp. 59-66.
[34] Aono, Y., Boyen, X., Phong, L.T., Wang, L. "Key-private proxy re-encryption under LWE". In: *Paul, G., Vaudenay, S. (eds.) INDOCRYPT*, vol. 8250, pp. 1–18. Springer, Heidelberg, 2013.