Int. Jrl. of **Human Computations & Intelligence**
Vol. 02, Issue No. 01, 2023
ISSN: 2583-5696

ORIGINAL RESEARCH

Secure Public Key Cryptosystem for in Smart City using Algebraic Structure

V Muthukumaran[1] . S Vasudevan[2] . Syeda Ayesha Siddiqha[3]

[1]Department of Mathematics, SRM Institute of Science and Technology, Tamil Nadu, India.
[2]Department of Mathematics, REVA University, Bengaluru, India.
[3]School of Engineering, Presidency University, Bengaluru, India.

Received: 16 December 2022 / Revised: 02 January 2023 / Accepted: 03 February 2023

Abstract – Smart city areas have been distinguished as zones which are urbanized and use assorted sorts of electronic information assortment sensors that are used to supervise assets and resources effectively. Keen meters are a unit of brilliant urban communities, and they gather data about clients and their utilization designs. Thus, the Internet of Things (IoT) being at a consistent advancement has incited various clients into having their information gathered from shrewd meters, put away on cloud workers. This is a method of sparing expenses and time engaged with getting to the information. Despite that, the cloud helped IoT faces protection and security issues. This is because of the cloud workers having an untrusted nature. Because of this, it is basic for the information collected from the shrewd meters be encoded heretofore redistributing it to the cloud worker. In any case, having encoded information in the cloud worker prompts an intricacy with regards to getting to the information. For clients who are on an alternate public key framework, it gets nonsensical for the clients to initially download the whole information on the cloud so as to get to the necessary information. In this article we proposed efficient public key cryptosystem for Smart city using near-ring.

Index Terms – Cryptography, Secure Public Key, Smart Cities, Improved framework

I. INTRODUCTION

In light of the difficult new organization prospects, and on steerage intensity benefits and organization improvement e orts, the idea of "savvy" urban areas has appeared. Batamuliza, states that a ton of exertion has been placed in shrewd urban communities to comprehend and take part in a world that is progressively connected [9,10,11,12,12,14,15]. This obviously implies development in metropolitan situations regarding instruction, medical care, transportation, and so forth. Subsequently the idea of "savvy" has been grasped in all the previously mentioned regions so as to satisfy the requests that have developed because of their development. In view of the realities given by the correspondence advances, the development of these utilities will result to better, effective methods of living for their clients. The development of IoT anyway can be viewed as a supporter for the development of these utilities. Also, therefore development of information created from these utilities is experienced, for example, information

from shrewd watches, savvy medical care, keen vehicles, etc. This information accordingly requires handling and capacity and thus the cloud workers are answerable for these functionalities [16,17,18,19,20]. They anyway require an extraordinary degree of organization assets which comes full circle to the security and protection of this information is being undermined. This is on the grounds that the cloud workers have been delivered shaky placing the security and protection of clients into the spotlight. An a valid example is the place body sensors gather the wellbeing status of a client during an exercise and transfer to the cloud. This data is viewed as close to home and should be remained careful. What's more, hence, clients have taken to ensure the security of their information before putting away it to the cloud workers. The ceaseless development of such keen gadgets implies an ascent in requests for power utilization for these devices [3,4,5,6,21,22].

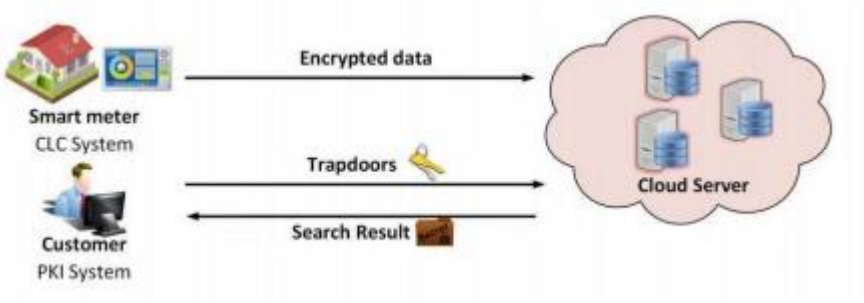

Fig. 1: A typical scenario of the smart meter

Furthermore, taking into account that the current force networks can't completely exposed the requests, shrewd lattice has been viewed as another answer for this test. Keen matrix targets guaranteeing solid computerized reactions to the rapidly changing power requests and simultaneously zeroing in on giving effective and dependable force frameworks. The way that the brilliant lattice has been placed into usage, much the same as some other advancements, it encounters security and protection difficulties [4,7,8]. Gadgets situated from homes, organizations, vehicles to individual contraptions gather data about their clients and utilization designs and from that point transfer them to the cloud. As prior referenced the data from these gadgets is secret and should be made sure about and to guarantee this, the information is consequently encoded before it's transferred to the cloud workers. Furthermore, along these lines, public-key encryption has end up being a productive method to guarantee that there is secrecy.

This is accomplished by the keen gadgets utilizing the public key of recipients inside the organization to scramble the clients' delicate information before transferring to the cloud worker. Elhabob et al. proposed a heterogeneous systems public key encryption with equality test in smart city[1]. With this, the information that is transferred to the cloud is made sure about. Hence in situations where an approved client needs to get to this information the client is needed to download the information and afterward utilize his/her own private key to decode the information so as to get to it. Anyway this is a serious tedious and tedious cycle in circumstances where the information is in immense sums. With this in thought, to guarantee that a client's data isn't uncovered at whatever point their information is looked; search usefulness is upheld in the ciphertexts that are put away in the cloud worker. This takes into consideration the hunt capacity, with no data identified with the ciphertexts being uncovered. In 2016 Valluri proposed public key cryptosystem based on Quaternion its secure many well-known attacks. In this article we proposed PKC for smart city.

II. NEARRING PUBLIC KEY ENCRYPTION SCHEME FOR SMART CITY

Key generation

Alice and Bob select randomly public elements, $z \in R$ and $v \in Z_p^*$ from a prime of the form $p = 3k + 5$. Then Alice selects randomly her private key $l, m \in Z$ such that $1 \le l \le p-1$ and $2 \le m \le p-1$ then calculate $f = v^l g^m v^{-l} \pmod p$. and publishes her public key $(\mathrm{f}, \mathrm{v}, \mathrm{g}, p)$.

Encryption

Given message $m \in R$ and Alice's public key $(\mathrm{f}, \mathrm{v}, \mathrm{g}, p)$. Bob chooses randomly $p, r \in Z$ such that $1 \le l \le p-1$ and $2 \le m \le p-1$ then computes $C_1 = v^p g^r v^{-p} \pmod p$, $C_2 = m.\mathrm{v}^p\ f^r g^{-p} \pmod p$ and finally outputs the ciphertext (C_1, C_2).

Decryption

Upon receiving the cipher text (C_1, C_2) Alice decrypts cipher text using her private key as follows:

$$\left[C_2 \left(v^l C_1^m v^{-l}\right)^{-1}\right] (\mathrm{mod}\ p) = m$$

Correctness

The correctness of the scheme is decided as follows.

$$\left[C_2 \left(v^l C_1^m v^{-l}\right)^{-1}\right] (\mathrm{mod}\ p)$$

$$\left[m.\mathrm{v}^l\ f^r v^{-l} \left(v^l C_1^m v^{-l}\right)^{-1}\right] (\mathrm{mod}\ p)$$

$$\left[m.\left(v^p f^r v^{-p}\right)\left(v^l (\mathrm{v}^p\ f^r v^{-p})^n v^{-l}\right)^{-1}\right] (\mathrm{mod}\ p)$$

$$\left[m.\left(v^p f^r v^{-p}\right)\left(v^p (\mathrm{v}^l\ f^m f^{-l})^r v^{-p}\right)^{-1}\right] (\mathrm{mod}\ p)$$

$$= m$$

Implementation of our Proposed Smart City Scheme

Let us demonstrate our method by using a special matrix nearring: $M_2(Z_n)$, where n to be a large secure prime.

Initial setup: Let

$$a = \begin{bmatrix} 1 & 6 \\ 0 & 1 \end{bmatrix}, z = \begin{bmatrix} 1 & 8 \\ 0 & 1 \end{bmatrix} \in M_2(\mathrm{Z}_n)$$

Key generation

Then Alice selects arbitrarily two natural number $l = 3, \mathrm{m} = 5$ m and n her private key of Alice. She then forms

$f = v^l g^m v^{-l} \pmod{23}.$

$$f = \begin{bmatrix} 1 & 6 \\ 0 & 1 \end{bmatrix}^3 \begin{bmatrix} 1 & 8 \\ 0 & 1 \end{bmatrix}^5 \begin{bmatrix} 1 & 6 \\ 0 & 1 \end{bmatrix}^{-3}$$

$$= \begin{bmatrix} 1 & 18 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 40 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -18 \\ 0 & 1 \end{bmatrix} \bmod 23$$

$$= \begin{bmatrix} 1 & 12 \\ 0 & 1 \end{bmatrix}$$

and announce $(\mathrm{f}, \mathrm{v}, \mathrm{g}, p)$.

Encryption: To send a message $m = \begin{bmatrix} 1 & 5 \\ 0 & 1 \end{bmatrix} \in M_2(Z_n)$ to Alice, Bob chooses $p = 2$ and $r = 3$. He then forms**,**

Let

$C_1 = v^p g^r v^{-p} \pmod{23},$

$$C_1 = \begin{bmatrix} 1 & 6 \\ 0 & 1 \end{bmatrix}^2 \begin{bmatrix} 1 & 8 \\ 0 & 1 \end{bmatrix}^3 \begin{bmatrix} 1 & 6 \\ 0 & 1 \end{bmatrix}^{-4} \bmod 23$$

$$= \begin{bmatrix} 1 & 17 \\ 0 & 1 \end{bmatrix}$$

$C_2 = m.\mathrm{v}^p \ f^r g^{-p} \pmod{23}$

$$C_2 = \begin{bmatrix} 1 & 5 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 6 \\ 0 & 1 \end{bmatrix}^2 \begin{bmatrix} 1 & 8 \\ 0 & 1 \end{bmatrix}^3 \begin{bmatrix} 1 & 6 \\ 0 & 1 \end{bmatrix}^{-2} \bmod 23$$

$$= \begin{bmatrix} 1 & 18 \\ 0 & 1 \end{bmatrix}$$

Decryption:

Upon receiving the cipher text (C_1, C_2) Alice decrypts cipher text using her private key as follows:

$$\left[C_2 \left(v^l C_1^m v^{-l} \right)^{-1} \right] (\bmod 23) = m$$

$$= \left[\begin{bmatrix} 1 & 18 \\ 0 & 1 \end{bmatrix} \left[\begin{bmatrix} 1 & 6 \\ 0 & 1 \end{bmatrix}^3 \begin{bmatrix} 1 & 17 \\ 0 & 1 \end{bmatrix}^5 \begin{bmatrix} 1 & 6 \\ 0 & 1 \end{bmatrix}^{-3} \right]^{-1} \right] \bmod 23$$

$$= \begin{bmatrix} 1 & 22 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -16 \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 5 \\ 0 & 1 \end{bmatrix}$$

$= m$

Security analysis

In this section, we briefly analyse the security aspects of the proposed public key encryption scheme in a detailed manner.

Chosen ciphertext attack

In the proposed scheme, the value of decrypting the ciphertexts $C_1 = v^p g^r v^{-p} \pmod{23}$ into the plain text m is equivalent to knowing $\left[m.\left(v^p f^r v^{-p}\right)\left(v^p (\mathrm{v}^l f^m f^{-l})^r v^{-p}\right)^{-1}\right] (\mathrm{mod}\ p)$. The attacker randomly selects a message $\overline{m} \in N$ and computes $\overline{m}C_2$ then forwards it to Alice for decryption process. Then, Alice computes $\overline{m}C_2\left(v^l C_1^m v^{-l}\right)^{-1}$. Such that, the adversary can recover the message m if he gets $\overline{m}m$.

Brute force attack

An attacker who has a prior knowledge on public parameters such as public key $f = v^l g^m v^{-l}$ makes an attempt to find the key values in Z_*^p. In such case, if the security parameters are larger than hidden semi-nearring conjugacy search problem then it is difficult to break the semi-nearring. In order to break the secret key using "Brute force attacks" $l, m \in Z$ it requires 2^{420} attempts.

Key recovers attacks

In the proposed approach, the public key is defined as $f = v^l g^m v^{-l}$. Such that the attacker can try to recover a conjugator Z_*^p if he knows the value of $n \in Z$. If we select a sufficiently large prime p over Z_*^p it is equivalent to solve CSP over Z_*^p. The other possible scenario is that if the attacker knows $n \in Z$ then he can solve DLP over Z_*^p.

III. CONCLUSION

Consequences of this article show that nearring speak to enthusiasm for planning quick open key understanding plans for savvy city. The idea of the heterogeneity in our plan takes into account a cloud worker to achieve a comparability test between ciphertexts that have been encoded under the PKI framework. Our theoretical examination and recreations from tests show our plan's practicability and reasonableness in contrast with other related works. Future works incorporate extension of the heterogeneous test to make arrangement for clients to designate a cloud worker rights to execute utilizing various kinds of approvals The security of our proposed convention dependent on twofold conjugacy search issue over nearring.

REFERENCE

1. Elhabob, R., Sella, I., Zhao, Y., Zhu, G., & Xiong, H. (2018). A heterogeneous systems public key encryption with equality test in smart city.
2. Mahesh, T. R., Kaladevi, A. C., Balajee, J. M., Vivek, V., Prabu, M., & Muthukumaran, V. (2022). An Efficient Ensemble Method Using K-Fold Cross Validation for the Early Detection of Benign and Malignant Breast Cancer. *International Journal of Integrated Engineering*, *14*(7), 204-216.
3. Krishnamoorthy, S., Muthukumaran, V., Yu, J., & Balamurugan, B. (2019, August). A secure privacy preserving proxy re-encryption scheme for IoT security using near-ring. In *Proceedings of the 2019 the International Conference on Pattern Recognition and Artificial Intelligence* (pp. 27-32).
4. Muthukumaran, V., Ezhilmaran, D., & Anjaneyulu, G. S. G. N. (2018). Efficient authentication scheme based on the twisted near-ring root extraction problem. In *Advances in Algebra and Analysis: International Conference on*

Advances in Mathematical Sciences, Vellore, India, December 2017-Volume I (pp. 37-42). Springer International Publishing.

5. Li, J., Wang, Q., Wang, C., Cao, N., Ren, K., & Lou, W. (2010, March). Fuzzy keyword search over encrypted data in cloud computing. In *2010 Proceedings IEEE INFOCOM* (pp. 1-5). IEEE.
6. Guptha, N. S., & Patil, K. K. (2017). Earth mover's distance-based CBIR using adaptive regularised Kernel fuzzy C-means method of liver cirrhosis histopathological segmentation. *International Journal of Signal and Imaging Systems Engineering*, *10*(1-2), 39-46.
7. Patil, K. K., & Ahmed, S. T. (2014, October). Digital telemammography services for rural India, software components and design protocol. In *2014 International Conference on Advances in Electronics Computers and Communications* (pp. 1-5). IEEE.
8. Boneh, D., Di Crescenzo, G., Ostrovsky, R., & Persiano, G. (2004). Public key encryption with keyword search. In *Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004. Proceedings 23* (pp. 506-522). Springer Berlin Heidelberg.
9. Al-Shammari, N. K., Alzamil, A. A., Albadarn, M., Ahmed, S. A., Syed, M. B., Alshammari, A. S., & Gabr, A. M. (2021). Cardiac stroke prediction framework using hybrid optimization algorithm under DNN. *Engineering, Technology & Applied Science Research*, *11*(4), 7436-7441.
10. Ahmed, S. T., & Basha, S. M. (2022). *Information and Communication Theory-Source Coding Techniques-Part II*. MileStone Research Publications.
11. Guptha, N. S., Balamurugan, V., Megharaj, G., Sattar, K. N. A., & Rose, J. D. (2022). Cross lingual handwritten character recognition using long short term memory network with aid of elephant herding optimization algorithm. *Pattern Recognition Letters*, *159*, 16-22.
12. Muthukumaran, V., Natarajan, R., Kaladevi, A. C., Magesh, G., & Babu, S. (2022). Traffic flow prediction in inland waterways of Assam region using uncertain spatiotemporal correlative features. *Acta Geophysica*, 1-12.
13. Fathima, A. S., Prakesh, D., & Kumari, S. (2022). Defined Circle Friend Recommendation Policy for Growing Social Media. *International Journal of Human Computations & Intelligence*, *1*(1), 9-12.
14. Yang, G., Tan, C. H., Huang, Q., & Wong, D. S. (2010). Probabilistic public key encryption with equality test. In *Topics in Cryptology-CT-RSA 2010: The Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010. Proceedings* (pp. 119-131). Springer Berlin Heidelberg.
15. Gothai, E., Muthukumaran, V., Valarmathi, K., Sathishkumar, V. E., Thillaiarasu, N., & Karthikeyan, P. (2022). Map-Reduce based Distance Weighted k-Nearest Neighbor Machine Learning Algorithm for Big Data Applications. *Scalable Computing: Practice and Experience*, *23*(4), 129-145.
16. Jayagopal, P., Muthukumaran, V., Koti, M. S., Kumar, S. S., Rajendran, S., & Mathivanan, S. K. (2022). Weather-based maize yield forecast in Saudi Arabia using statistical analysis and machine learning. *Acta Geophysica*, *70*(6), 2901-2916.
17. Merlin Linda, G., Sree Rathna Lakshmi, N. V. S., Murugan, N. S., Mahapatra, R. P., Muthukumaran, V., & Sivaram, M. (2022). Intelligent recognition system for viewpoint variations on gait and speech using CNN-CapsNet. *International Journal of Intelligent Computing and Cybernetics*, *15*(3), 363-382.
18. Wu, L., Zhang, Y., Choo, K. K. R., & He, D. (2017). Efficient and secure identity-based encryption scheme with equality test in cloud computing. *Future Generation Computer Systems*, *73*, 22-31.
19.
20. Vimala, B. B., Srinivasan, S., Mathivanan, S. K., Muthukumaran, V., Babu, J. C., Herencsar, N., & Vilcekova, L. (2023). Image Noise Removal in Ultrasound Breast Images Based on Hybrid Deep Learning Technique. *Sensors*, *23*(3), 1167.
21. Batamuliza, J. (2018). Certificateless secure anonymous key distribution scheme for smart grid. *International Journal of Computer Applications*, *975*, 8887.
22. Lee, H. T., Ling, S., Seo, J. H., & Wang, H. (2016). CCA2 attack and modification of Huang et al.'s public key encryption with authorized equality test. *The Computer Journal*, *59*(11), 1689-1694.