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

ORIGINAL RESEARCH

Proxy Re-encryption for Internet of Things (IoT) over Seminear-ring

V Muthukumaran[1] . B Vidyashree[2]

[1]Department of Mathematics, College of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur - 603203, Tamilnadu, India.
[2]Department of Mathematics, REVA University, Bangalore, Karnataka, India.

Received: 05 December 2022 / Revised: 02 February 2023 / Accepted: 13 February 2023

Abstract – The assembly of distributed computing and Internet of Things (IoT) is halfway because of the logical requirement for conveying stretched out administrations to a more extensive client base in various circumstances. Be that as it may, distributed computing has its impediment for applications requiring low-idleness and high portability, especially in antagonistic settings. Somewhat, such constraints can be moderated in a mist registering worldview since the last overcomes any barrier between far off cloud server farm and the end gadgets. This work we suggested established key arrangement agreement reliant on seminear-ring. The confidence of our agreement reliant on Double Decomposition Problem in non-commutative seminear-ring.

Index Terms – Seminear-ring, Double Decomposition Problem, IoT

I. INTRODUCTION

Distributed computing is generally adult and has been used in various applications, including those including Internet of Things (IoT) gadgets. IoT gadgets are Internet associated gadgets (likewise alluded to as articles or things) intended to gather information (for example sense natural information, for example, dampness and air temperature) before sending the information to a preparing focus (for example the cloud) for capacity, handling, investigation, and so on As such, the majority of the handling is attempted at a far off server farm site that might be truly situated in another nation. Such an organization model may not be appropriate for applications that have explicit necessities [4], for example, the accompanying: Inertness/defer delicate applications Latency/postpone touchy applications, for example, video conferencing and mechanical computerization may request a very short dormancy so as to keep up a high ability of experience. Other idleness touchy applications, for example, combat zones, brilliant traffic signals and crisis reaction administrations may require a considerably more limited inactivity as any deferral can have genuine outcomes (for example fatalities).

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

Organization availability obliged applications in a distributed computing model, all information and solicitations are sent to and handled at the cloud worker. The huge increment in the quantity of IoT gadgets likewise brings about a comparing increment in the measure of information to be sent, prepared, put away, and so forth In any case, IoT gadgets ordinarily have restricted organization (and registering) limits. Consequently, it is trying to convey ceaseless and dependable help in an obliged network climate. Topographically appropriated applications IoT applications can be geologically circulated, for instance, in brilliant frameworks, railroads, and pipeline checking, and the separation between IoT gadgets and far off cloud community influences inertness and thus the nature of administration.

Continuous versatile applications Cloud workers are sent in a static area, however IoT applications, for example, those conveyed in brilliant transportation and ecological observing are dynamic and have high portability. Current years in crypto coherent examination have seen a few proposition for secure cryptographic plans utilizing noncommutative gatherings; specifically Artin's interlace bunches [1, 2, 3, 4, 5,6,7,8,9,10]. Applying interlace bunch a stage on behalf of cryptosystems was presented in [11]. Twist gatherings, from one perspective, are more convoluted than Abelian gatherings and, then again, are not very muddled to work with. These two attributes make mesh bunch a helpful and valuable decision to pull in the consideration of analysts. In [23-32] suggested a mesh bunch variant of D-H protocol [6-12]. They recover the exceeding plan by suggesting another validated key understanding convention dependent on CSP in interlace gatherings. We utilize CSP to recommend another key arrangement conspire. The above problem in twist bunches is troublesome and therefore gives single direction capacities. In [7-22] author suggested protocol trade convention dependent on disintegration issue in centralizer near-rings and secure the men-in-center assaults.

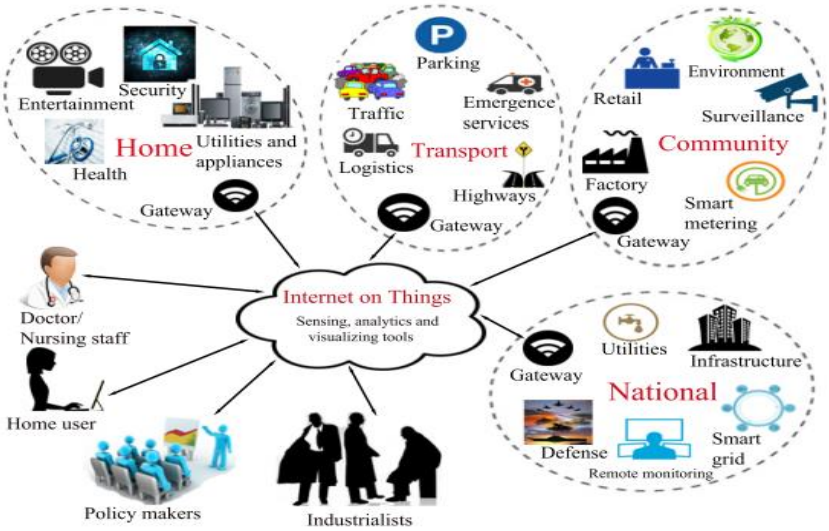

Fig. 1: Authentication model for IoT applications

This work is organized as monitors: Section 1 delivers outline toward the suggested system. Section 2 we description to the proposed method based on IoT. Section 3 provides the security investigation of the suggested method. In the Section 5 we discuss about performance analysis of the scheme and section 5 provides conclusion.

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

II. PROPOSED METHOD FOR IOT SYSTEM

Complexity Assumptions over Seminear-ring

Double Decomposition Problem over Seminear-ring

Given $(f_1, f_2) \in R \times R$ and $\alpha, \beta \in End(\mathrm{R}), w \in R$ the problem is to find $f_1, f_2 \in S$ such that $z = \alpha(f_1) w \beta(f_2)$. Furthermore, let $H_1 :\to \{0,1\}^{\lambda+2\mu}, H_2 : \mathrm{R}^2 \to \{0,1\}^{\lambda+2\mu}, H_1 : \{0,1\}^{\lambda} \to N(R)$.

Key Generation:

Proceeding effort for safety boundary λ, procedure Key Gen arbitrarily picks $f_1, f_2 \in N(R)$ and $w \in R$ formerly productions the PK $L = \alpha(f_1) w \beta(f_2)$ and private key (f_1, f_2).

Encryption:

Proceeding contribution a communication $m \in \{0,1\}^{\lambda}$ and PK L procedure Encryption builds the $(h_1, u_1) \in R \times \{0,1\}^{\lambda+2\mu}$

- Randomly picks $f_1^{'}, f_2^{'} \in R$ and let $e = \alpha(f_1^{'}) \mathrm{L} \beta(f_2^{'})$.
- Let $v_1 = H_1(e) \oplus m$.
- Let $\alpha(f_1^{''}), \beta(f_2^{''}) = H_2(v_1)$.
- Let $s_1 = \alpha(f_1^{''}) e \beta(f_2^{''})$
- Let $h_1 = \alpha(f_1^{''}) \beta(f_1^{'}) w \alpha(f_2^{'}) \beta(f_2^{''})$.
- Let $u_1 = H_3(s_1) \oplus v_1$.

Decryption:

The ciphertext $(h_1, u_1) \in N \times \{0,1\}^{\lambda+2\mu}$, procedure Decryption the text as following way.

- Assume the $\overline{s_1} = L = \alpha(f_1) h_1 \beta(f_2)$
- Let $\overline{v_1} = H_3(\overline{s_1}) \oplus u_1$.
- Assume the $(\overline{\alpha(f_1)}, \mathrm{w}, \overline{\beta(f_2)}) = H_2(\overline{v_1})$.
- Assume the $\overline{L} = I_L(\overline{\alpha(f_1)}).\overline{s_1}.I_R(\overline{\beta(f_2)})$
- Assume the $\overline{m} = H_1(\overline{e}) \oplus \overline{v_1}$.

Re-encryption key generation:

The operator *A*'s PK (f_1, f_2) and operator B's PK (f_3, f_4), send to $K = (y_1, \mathrm{y}_2)$

$y_1 = (\alpha(f_3))^{-1} w(\beta(f_1)), y_2 = (\alpha(f_4))^{-1} w(\beta(f_2))$

Re-encryption:

Arranged contribution a ciphertext $(h_1, u_1) \in N \times \{0,1\}^{\lambda+2\mu}$, calculation re-encryption computes $\overline{h_1} = y_1.h_1.y_2$ and afterward yields another ciphertext $(\overline{h_1}, u_1)$.

Theorem

Demonstrate that the suggested IoT helped intermediary re-encryption plot be situated steady trendy environment.

Proof.

Initially, the stability of unscrambling cycle is approved regarding encryption measure. For a substantial ciphertext pair $(h_1, u_1) \in N \times \{0,1\}^{\lambda+2\mu}$, we have that $\overline{w}$ is properly proportional to its partner utilized over the encryption, i.e.,

$$\begin{aligned}
\overline{s_1} &= \alpha(f_1) h_1 \beta(f_2) \\
&= \alpha(f_1)\alpha(f_1'')\alpha(f_1')w\beta(f_2)\beta(f_2')\beta\alpha(f_2'') \\
&= \alpha(f_1'')\alpha(f_1)\alpha(f_1')w\beta(f_2'')\beta(f_2)\beta(f_2') \\
&= \alpha(f_1'')\beta(f_1')w\alpha(f_2')\beta(f_2'') \\
&= h_1.
\end{aligned}$$

Thus, we have

$$\begin{aligned}
\bar{v}_1 &= H_3(\overline{s_1}) \oplus u_1. \\
&= H_3(w) \oplus s \\
&= s_1.
\end{aligned}$$

and

$$\begin{aligned}
\left(\overline{\alpha(f_1)}, \mathrm{w}, \overline{\beta(f_2)}\right) &= H_2(\overline{v_1}). \\
&= H_2(\overline{s_1}) \\
&= \alpha(f_1''), \beta(f_2'').
\end{aligned}$$

$$\begin{aligned}
\overline{L} &= I_L\left(\overline{\alpha(f_1)}\right).\overline{s_1}.I_R\left(\overline{\beta(f_2)}\right) \\
&= \overline{L} = I_L\left(\overline{\alpha(f_1)}\right).\alpha(f_1)h_1\beta(f_2).I_R\left(\overline{\beta(f_2)}\right) \\
&= s_1
\end{aligned}$$

and

$$\begin{aligned}
\overline{m} &= H_1(\bar{e}) \oplus \overline{v_1}. \\
&= H_1(e) \oplus v_1 \\
&= m
\end{aligned}$$

Next, we play out the approval of the decoding cycle regarding its encryption cycle. For a sensible re-scrambled ciphertext pair $(h_1', u_1') \in N \times \{0,1\}^{\lambda+2\mu}$ it is now realized that it originates from a substantial ciphertext (h_1, u_1)encoded under client An's open key $K = (y_1, \mathrm{y}_2)$ and a re-encryption key in agreement to $\overline{h_1} = y_1.\mathrm{h}_1.\mathrm{y}_2$, $\overline{u_1} = u_1$. Where, $y_1 = (\alpha(f_3))^{-1} w(\beta(f_1))$ and $y_2 = (\alpha(f_4))^{-1} w(\beta(f_2))$ while (f_1, f_2) and (f_3, f_4) keeping in mind that and are client have PK and client B's Pk, distinctly. Presently, with realizing B's Pk (f_3, f_4) one can from the start recuperate.

At that point, resulting ascertaining on message m must be right.

$$\begin{aligned}\overline{\overline{s_1}} &= \alpha(f_3).\overline{h_1}.\alpha(f_4)\\ &= \alpha(f_3).y_1.\mathrm{h}_1.\mathrm{y}_2.\alpha(f_4)\\ &= \alpha(f_1'')\beta(f_1')w\alpha(f_2')\beta(f_2'')\\ &= h_1\end{aligned}$$

III. SECURITY ANALYSIS

Security Against Equivalent Private Key Attack:

Presently, let us study the connection that is among the public key $n \in R$ and the Pk $(f_3, f_4) \in R_1 \times R_2$ is straightforward: $L = \alpha(f_1) w \beta(f_2)$, here we should must know about the security danger called proportionate private key assault. That is, if an enemy A can discover with the end $\alpha(f_1), \beta(f_2) \in R$ goal that

$$L = \alpha(f_1) w \beta(f_2) \qquad (1)$$

Grips, then for each assumed ciphertext (h_1, u_1) encryption is done by the Pk L, the opponent *A* might stab to improve the info around the original message m using $\alpha(f_1), \beta(f_2)$. Such that the initial step related with An's unscrambling cycle is given as follows:

$$\begin{aligned}\overline{s_1} &= \alpha(f_1) h_1 \beta(f_2)\\ &= \alpha(f_1'')\beta(f_1')w\alpha(f_2')\beta(f_2'').\end{aligned}$$

Now, only if

$$\alpha(f_1') \in N(R_1) \text{ and } \alpha(f_2') \in N(R_2) \quad (2)$$

$$\begin{aligned}\overline{s_1} &= \alpha(f_1) h_1 \beta(f_2)\\ &= \alpha(f_1)\alpha(f_1'')\alpha(f_1')w\beta(f_2)\beta(f_2')\beta\alpha(f_2'')\\ &= \alpha(f_1'')\alpha(f_1)\alpha(f_1')w\beta(f_2'')\beta(f_2)\beta(f_2')\\ &= \alpha(f_1'')\beta(f_1')w\alpha(f_2')\beta(f_2'')\\ &= h_1.\end{aligned}$$

with the end goal that the foe can recoup the whole message *m*. Otherwise, assuming either $\alpha(f_1') \in N(R_1)$ and the cycle of decoding will be fizzled, aside from with immaterial likelihood, in thought to the way that are $\alpha(f_1''), \alpha(f_1'), \beta(f_2''), \beta(f_2')$ haphazardly appropriated in R . Presently, through joining the conditions, PK(h_1, u_1) , we have that $\alpha(f_1) w \beta(f_2) \in N(R_2)$ concerning the condition $\beta(f_2') \in N(R_2)$, we have that Therefore, $\alpha(f_1)\overline{\alpha(f_1')} = 1_R$, i.e. $\alpha(f_1) = \alpha(f_1')$ for example So also, we have $\beta(f_2) = \beta(f_2')$. That is, over the subseminear-ring and, the response for the gathering condition of (1) is characterized in special route under the state of $\mathrm{N}(\mathrm{R}_1) \cap N(\mathrm{R}_2) = \{1_R\}$. Thusly, the enemy A's likelihood to perform a productive

assault is least, under the presumption over seminear-ring N is recalcitrant. At the end of the day, the retreat of Pk is established in the stability of the turned RP issue in seminear-ring.

Security Against Chosen Plaintext Attack:

In agreement to the encryption cycle, A realizes that $\alpha\left(f_1^{''}\right)\beta\left(f_1^{'}\right)w\alpha\left(f_2^{'}\right)\beta\left(f_2^{''}\right)$ for some obscure what's more, $\alpha\left(f_1^{''}\right),\beta\left(f_1^{'}\right),w,\alpha\left(f_2^{'}\right),\beta\left(f_2^{''}\right)\in R.$ A have the earlier information on the seminear-ring condition $e=\alpha\left(f_1^{'}\right)\mathrm{L}\,\beta\left(f_2^{'}\right)$, where is the open key with no attention to the worth u. Assume that A from the start makes a speculation on . At that point, $\alpha\left(f_1^{'}\right),\beta\left(f_2^{'}\right)\in R$ A can attempt the accompanying attack:

The attack we canister watch, the foe container approve his/her estimate by testing the correspondence $u_1^{*}=H_3\left(\overline{s_1}\oplus\overline{v_1}\right)$, or equity $h^{*}_{1}=\alpha\left(f_1^{''}\right)\beta\left(f_1^{'}\right)w\alpha\left(f_2^{'}\right)\beta\left(f_2^{''}\right)$ rather than them two. Actually, one of them is genuine just with unimportant likelihood if the other is bogus, and for arbitrarily choosing them $\alpha\left(f_1^{'}\right),\beta\left(f_2^{'}\right)$ two are bogus with a nearly higher measure of likelihood, in thought to the way that is sufficiently enormous. Along these lines, making an arbitrary supposition on $\alpha\left(f_1^{'}\right),\beta\left(f_2^{'}\right)\in R$ likelihood for making a fruitful assault is irrelevant:

IV. PERFORMANCE ANALYSIS

Security

The proposed approach utilize seminear-ring based information sharing technique that keeps pernicious outsider substances from catching the information substance, even with the instance of wiretapping between the customer and the worker. Additionally, the $u_1^{*}=H_3\left(\overline{w}\oplus\overline{v}\right)$ and $h^{*}_{1}=\alpha\left(f_1^{''}\right)\beta\left(f_1^{'}\right)w\alpha\left(f_2^{'}\right)\beta\left(f_2^{''}\right)$ re-encryption key got during the client element An's encryption cycle couldn't be utilized constantly through the additional client B. In this way, the suggested method protects in reverse mystery.

Computation amount

The suggested framework agreements effective information imparting offices to smaller value intricacy processes. The explanation it does calculation tasks athwart workers. Table 1, calculation capacity examination with the current methodologies and it is seen that the suggested attitude is additional productive than current procedures by methods for expanded information sharing postpone time during calculation.

Table 1 Comparison of proposed scheme

Schemes	Data accessing	Data collection	Nodes cost	Amount of Sharing
Zuo et al. [16]	S_E+6T_p	3S_E+6T_p	S_E+T_p	O(m(m-1)/2)
Lu at al. [18]	2S_E	3S_E+6T_p+S_m	3S_E+6T_p	O(m(m-1)/2)
Yang et al. [21]	3S_E+6T_p+S_m	3S_E+6T_p+S_m	3S_E+6T_p+S_m	O(m(m-1)/2)
Our	S_E+2T_p+3S_m	O	S_E+2T_p+S_m	O(m)

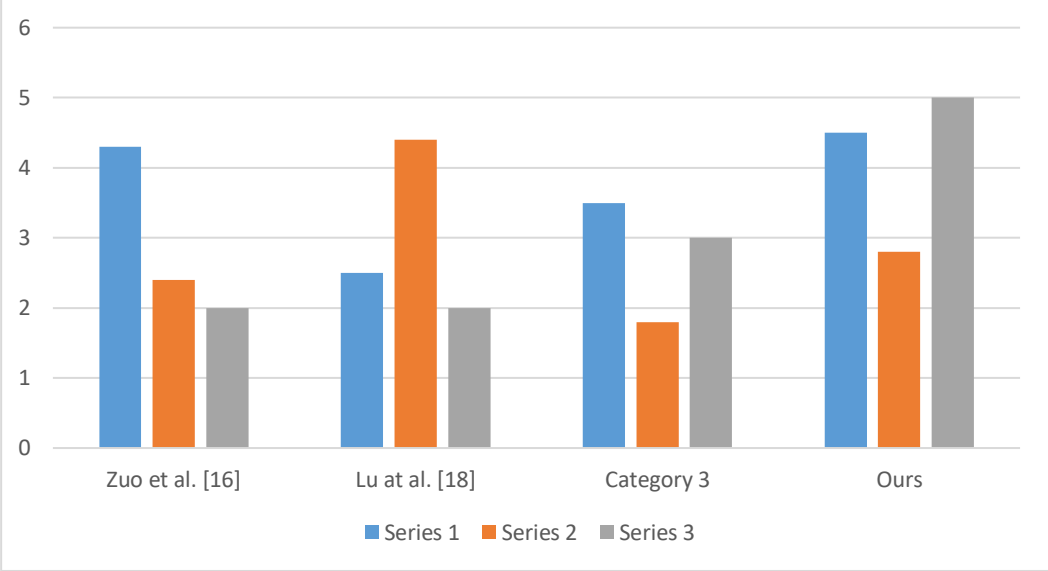

Fig. 2: Comparative diagram

Forward and backward secrecy

Adaptable membership and unsubscription of clients in information distribution between gatherings. Bought in bunch individuals ought not have a clue about the mystery bunch key utilized already, and withdrew individuals ought not have a clue about the new mystery bunch key. The proposed technique depends on the gathering mark, and subsequently gives security.

V. CONCLUSIONS

Propose method benevolences an actual technique for enhanced security and protection gauges across IoT frameworks. It presents a protected information sharing dependent on intermediary re-encryption for web of vehicles utilizing seminear-ring. It gives a powerful answer for Double Decomposition Problem utilizing seminear-ring. This further increases the refuge of the framework. The safety analyzing of the suggested plot expresses that the suggested approach gives improved security and protection measures. We foresee that the suggested show ought to be by and large and capably used in the circulated processing condition.

REFERENCES

1. Gerla, M., Lee, E. K., Pau, G., & Lee, U. (2014, March). Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. In *2014 IEEE world forum on internet of things (WF-IoT)* (pp. 241-246). IEEE.
2. Alam, K. M., Saini, M., & El Saddik, A. (2015). Toward social internet of vehicles: Concept, architecture, and applications. *IEEE access*, *3*, 343-357.
3. 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.
4. Rajaram, R. N., Ohn-Bar, E., & Trivedi, M. M. (2016). Refinenet: Refining object detectors for autonomous driving. *IEEE Transactions on Intelligent Vehicles*, *1*(4), 358-368.
5. 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.

6. Kumari, S., Khan, M. K., & Atiquzzaman, M. (2015). User authentication schemes for wireless sensor networks: A review. *Ad Hoc Networks*, *27*, 159-194.
7. 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.
8. Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015, June). Security and privacy challenges in industrial internet of things. In *Proceedings of the 52nd annual design automation conference* (pp. 1-6).
9. Xiong, H., Zhang, H., & Sun, J. (2018). Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing. *IEEE Systems Journal*, *13*(3), 2739-2750.
10. Diffie, W., & Hellman, M. E. (2022). New directions in cryptography. In *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman* (pp. 365-390).
11. Sangeetha, S. K. B., Muthukumaran, V., Deeba, K., Rajadurai, H., Maheshwari, V., & Dalu, G. T. (2022). Multiconvolutional Transfer Learning for 3D Brain Tumor Magnetic Resonance Images. *Computational Intelligence and Neuroscience*, *2022*.
12. Xiong, H. (2014). Cost-effective scalable and anonymous certificateless remote authentication protocol. *IEEE Transactions on Information Forensics and Security*, *9*(12), 2327-2339.
13. 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.
14. 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.
15. Ahmed, S. T., Kumar, V., & Kim, J. (2023). AITel: eHealth Augmented Intelligence based Telemedicine Resource Recommendation Framework for IoT devices in Smart cities. *IEEE Internet of Things Journal*.
16. 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.
17. Ma, S. (2016). Identity-based encryption with outsourced equality test in cloud computing. *Information Sciences*, *328*, 389-402.
18. Ling, Y., Ma, S., Huang, Q., Li, X., & Ling, Y. (2020). Group public key encryption with equality test against offline message recovery attack. *Information Sciences*, *510*, 16-32.
19. Duong, D. H., Fukushima, K., Kiyomoto, S., Roy, P. S., & Susilo, W. (2019). A lattice-based public key encryption with equality test in standard model. In *Information Security and Privacy: 24th Australasian Conference, ACISP 2019, Christchurch, New Zealand, July 3–5, 2019, Proceedings 24* (pp. 138-155). Springer International Publishing.
20. 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.
21. Ahmed, S. T., Basha, S. M., Ramachandran, M., Daneshmand, M., & Gandomi, A. H. (2023). An Edge-AI enabled Autonomous Connected Ambulance Route Resource Recommendation Protocol (ACA-R3) for eHealth in Smart Cities. *IEEE Internet of Things Journal*.
22. 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.
23. 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).
24. Ramaiah, N. S., & Ahmed, S. T. (2022). An IoT-Based Treatment Optimization and Priority Assignment Using Machine Learning. *ECS Transactions*, *107*(1), 1487.
25. 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.