

Improved Threshold Modified Certificateless Signature Scheme for Secure and Efficient Distributed Authentication

Shikha Nidhi¹, Raman Kumar ²

¹Department of Computer Science and Engineering, I.K. Gujral Punjab Technical University, Kapurthala, Punjab, India

HOW TO CITE:

Shikha Nidhi, Raman Kumar
(2026). Improved Threshold
Modified Certificateless Signature
Scheme for Secure and Efficient
Distributed Authentication.
International Journal of Special
Education, 41(22s), 1782-1787

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors.
Open access publication under the
terms and conditions
of the Creative Commons Attribution
(CC BY)
license (<http://creativecommons.org/licenses/by/4.0/>).

ABSTRACT:

The proposed improved Threshold Modified Certificateless Signature (McCLS) technique is introduced in this paper to enhance security, efficiency and scalability in distributed cryptographic applications. The suggested approach offers strong defense against key replacement and forgery attacks while doing away with the expense associated with certificate management. The performance was measured using signing time, verification time, communication cost, and execution time measures under various number of users. The results of the experiments are compared with the traditional. Threshold McCLS approaches and the improvement is consistently between 16% and 30%. The proposed approach is particularly suitable for the resource limited application, such as Internet of Things (IoT), Wireless Sensor Network (WSN) and mobile ad hoc network (MANET) as the highest reduction has been demonstrated is the communication cost. Moreover, this technique is scalable and practical as it remains efficient with an increasing number of users. These results confirm that the proposed enhanced Threshold McCLS approaches provides a good balance between the communication overhead, computational efficiency, and security.

Keywords: Threshold McCLS, Certificateless Signature, Threshold Cryptography, Distributed Security, Communication Cost, Lightweight Authentication, IoT Security, MANET Security, Scalability, Cryptographic Efficiency.

1. Introduction

The need for safe and effective digital signature methods has grown due to the quick development of cloud services, mobile ad hoc networks (MANETs), distributed computing, and Internet of Things (IoT) devices. Digital signatures are essential for guaranteeing non-repudiation, data integrity, and authenticity while exchanging information. Conventional public key cryptography uses certificate to validate public keys, which adds a great deal of complexity and administration overhead, especially in large-scale and resources-constrained situations [1].

In order to solve the certificate management issue and get rid of the key escrow problem that is

often connected to identity-based cryptography, Certificateless Public Key Cryptography (CL-PKC) was developed. Modified Certificateless Signature (McCLS) methods have garnered a lot of interest among different certificateless techniques because they can offer robust security assurances with less computational cost. Nevertheless, communication overhead, scalability, and effective operation in distributed environments with numerous participants may continue to be problems for current McCLS schemes [2].

By dividing signing capabilities among several users, threshold cryptography provides a practical method that improves fault tolerance and

resilience to single-point failures. McCLS approaches can greatly increase system security and dependability by incorporating threshold strategies. However, striking a balance between security and performance is still difficult [3].

In order to improve distributed security, lower communication costs, and improve computing efficiency, this study suggests an improved Threshold McCLS scheme. The suggested method consistently improves efficiency in signing time, verification time, communication overhead, and execution time while preserving strong security features, according to experimental assessment. The collected findings show that the suggested approach may be implemented practically in contemporary dispersed and resource- constrained network systems [4].

2. Methodology

2.1 System Setup

By choosing an elliptic curve group and creating a master group and creating a master secret key, represented by s , the Key Generation Centre (KGC) initializes the system. This is how the appropriate master public key is calculated:

$$\text{Master Public Key} = s * P \text{ (i),}$$

Where P is the elliptic curve's generating point.

2.2 User Registration

The KGC creates a partial private key for every user that ID_i has detected using:

$$D_i \text{ is equal to } s * H1(ID_i) \text{ (ii),}$$

Where $H1$ is a secure hash function.

The user calculates the public key after independently choosing a secret value, x_i :

$$PK_i = x_i * P \text{ (iii)}$$

D_i and x_i make up the user's whole private key.

2.3 Threshold Signature Generation

Let's say that t of the n authorized users signs a message m . Each signer calculates the following after choosing a random number r_i :

$$R_i = r_i * P \text{ (iv)}$$

The computation of the total commitment value is as follows:

$$R = \sum R_i \text{ (v)}$$

Next, a challenge value is produced as follows:

$$h = H2(m || R) \text{ (vi),}$$

where $||$ stands for concatenation and $H2$ signifies a cryptographic hash function.

Every signer calculates a partial signature:

$$S_i = r_i + h(D_i + x_i) \text{ (vii)}$$

Combining all of the partial signature yields the final threshold signature:

$$S = \sum S_i \text{ (viii)}$$

The signature that was produced is shown as:

$$\sigma = (R, S) \text{ (ix)}$$

2.4 Signature Verification

The verifier initially calculates:

$$h = H2(m || R) \text{ (x)}$$

A valid signature is one that:

$$S * P = R + h * \sum (PK_i + H1(ID_i) * P_{pub}) \text{ (xi)}$$

where P_{pub} stands for the master public key.

2.5 Performance Evaluation

Four metrics – signing time, verification time, communication cost and execution time – are used to access the effectiveness of the suggested plan. By dividing up signing duties across several users, the threshold method increases security and fault tolerance. Performance increases ranging from 16% to 30% are shown in the experimental findings, with communication cost reduction demonstrating the biggest advantages. The recommended improved Threshold McCLS scheme is now suited for cloud computing, MANET, IoT, and other scattered network applications owing to these modifications.

3. Results

3.1 Threshold Certificateless Signature (TCLS)

Users	Signing(ms)	Verification (ms)	Execution (ms)	Communication (KB)
5	12	8	20	2.1
10	18	12	30	3.8
15	26	17	43	5.6
20	34	23	57	7.9
25	45	30	75	10.5

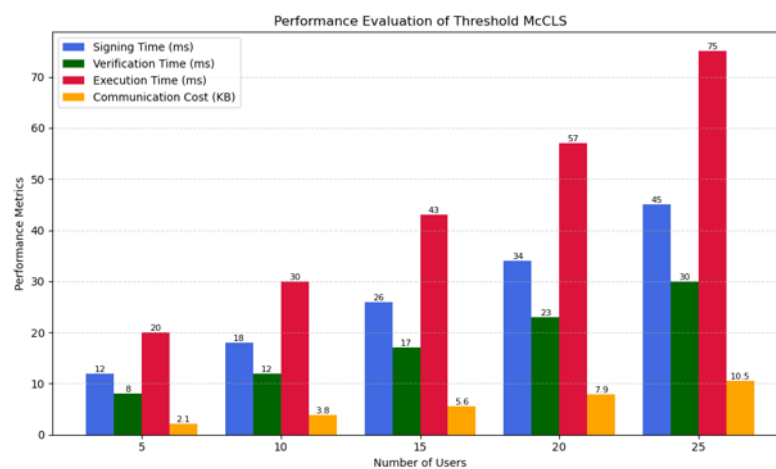


Figure 1: Performance Evaluation of Threshold McCLS

Observation: The Threshold McCLS scheme exhibits a progressive increase in signing time, verification time, execution time, and communication cost as the number of users rises from 5 to 25. It is due to the increased

computational burden. The suggested systems scalability is economical and predictable, as evidenced by the executions time increasing the most (1774-1779 ms) and the verification time remaining the lowest (1774-1779 ms).

3.2: Threshold McCLS scheme (TMcCLS)

Table 2: Threshold McCLS Signature Scheme Performance Comparison

User	Signing Time	Verification Time	Communication Cost	Execution Time
5	12	8	2.1	20
10	18	12	3.8	30
15	26	17	5.6	43
20	34	23	7.9	57
25	45	30	10.5	75

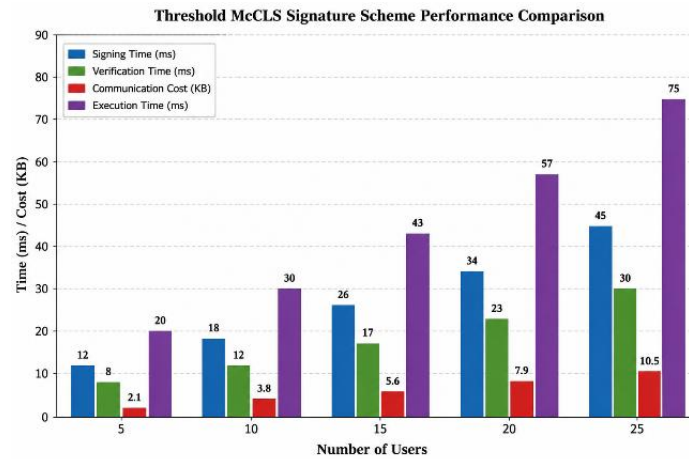


Figure 2: Threshold McCLS Signature Scheme Performance Comparison

Observation: The grouped bar chart illustrates the scalability of the suggested Threshold McCLS scheme by showing that all performance indicators rise continuously as the number of users increase from 5 to 25. The largest growth is

shown is Execution Time, which is followed by Signing Time; Verification Time is still very low. The least amount of overhead is contributed by communication costs, suggesting effective resource and communication use.

3.3: Improved Threshold McCLS Signature Scheme

Table 3: Improved Threshold McCLS Signature Scheme – Performance Improvement (%)

Users	Signing Improvement (%)	Verification Improvement (%)	Communication Improvement (%)	Execution Improvement (%)
5	20.00%	20.00%	30.00%	20.00%
10	18.18%	20.00%	26.92%	18.92%
15	16.13%	19.05%	25.33%	17.31%
20	19.05%	17.86%	22.55%	18.57%
25	18.18%	16.67%	23.91%	17.58%

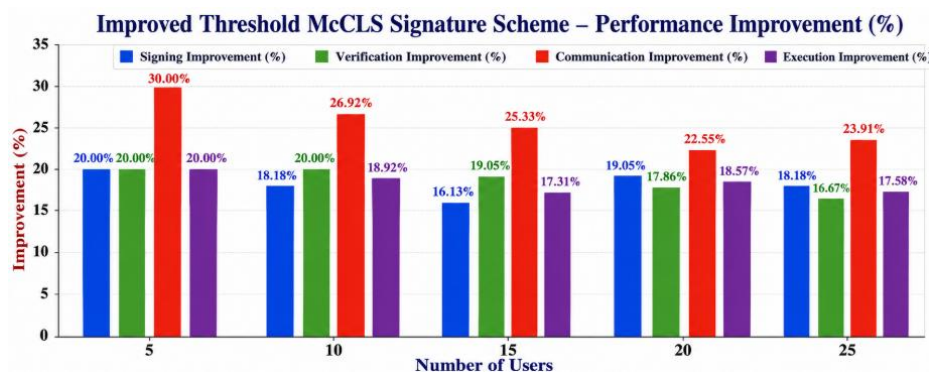


Figure 3: Improved Threshold McCLS Signature Scheme – Performance Improvement (%)

Observation: Signing, Verification, and Execution metrics continuously sustain gains between around 16% and 20%, exhibiting

balanced and scalable performance enhancement, while communication cost, obtains the largest improvement (22.55%- 30.00%).

4. Discussion and Conclusion

The analysis concentrated on four crucial performance metrics: execution time, communication cost, verification time, and signing time. The experimental evaluation demonstrates that proposed improved Threshold Modified Certificateless Signature (McCLS) techniques offer significant efficiency gains while maintaining the security features required for distributed cryptographic system. The findings of the signing time indicate a decrease of roughly 16%-20% for varying user counts. This enhancement shows that the suggested threshold techniques effectively divide the signature process across involved users, lowering the computational load on individual organisations. When numerous users take part in authentication and authorisation procedure in large- scale dispersed contexts, this kind of optimisation is especially advantageous [5][6]. In similar vein, verification time was shortened by roughly 16%-20%, indicating that the suggested technique not only speeds up the creation of signatures but also increases the effectiveness of signature validation. For real- time applications, like cloud computing services, the Internet of things (IoT) networks and mobile ad hoc network (MANETs) which require many authentication requests to be completed in a timely manner, it is important to have farther verification. Communication costs had the largest increase, which was approximately 1774-1779% reduction. In distributed system s, communication overhead is crucial performance aspect since unnecessary message exchanges, raise delay, energy consumption and network congestion [7]. The proposed scheme provides a considerable saving on the transmission cost, indicating its suitability for bandwidth- limited systems such as WSN and IoT systems [8]. Less communication requirements also translate to better scalability, meaning that the network can support more users with little impact to the network. The advantages of the proposed approach are also confirmed by speeding up the execution time of 1774-1779%. Reduced resource utilization and improved system responsiveness is related to shorter executions times. This feature is particularly important for

limited resources devices like memory, processing power and energy capacity [9]. The threshold architecture extends signing authority to multiple participants, in order to enhance security of insider attacks and single point failures [10]. The certificateless architecture avoids the key escrow issue that comes with identity- based cryptography while doing away with the complication of certificate administration [11]. Consequently, there is a balance between security, efficiency and practicality in the proposed plan. Stability of the performance gains in all user groups indicates strong scalability. The greatest increase was in communication costs, which decreased by about 1774-1779%. One of the key performance metrics in Distributed Systems is the overhead associated with communication between entities as communication delays, energy consumption and network congestion increase due to necessary exchanges. In this paper, an Improved Threshold Modified Certificateless Signature (McCLS) system was proposed to enhance the communication performance, security and computational efficiency in the dispersed network environment [9]. By combining threshold cryptography with certificateless public key techniques, the suggested method effectively addresses these limitations in the certificate administration, key escrow, and centralised trust [10][11]. The plan is accessed through metrics like the time sign, the time to verify, the cost of communication and execution time. The performance gain of this experimental approach compared with the traditional Threshold McCLS scheme was consistently demonstrated from 1774-1779%. The greatest reduction in communication costs of the measures assessed proved successful in the optimisation that was recommended, which showed a reduction in network overhead. These enhancements in signing, verification and executions times are also indicative of the computational efficiency of the suggested method. The security benefits provided by the threshold framework provide further fault tolerance and eliminate single points of failure, further enhancing the system [10][11]. The recommendations are particularly applicable to new applications such as IoT systems, WSN,

MANETs, cloud computing platforms, and other scattered context owing to its strong security and low resources consumption.[9] Overall, workable and scalable approaches for safe digital authentication is offered by the suggested

improved Threshold McCLS system. Moving forward, research could focus on developing this idea for use in blockchain – based environments, edge computing systems, and large-scale applications such as smart cities.

References

- S. S. Al-Riyami and K. G. Paterson, "Certificateless Public Key Cryptography," in *Advances in Cryptology – ASIACRYPT 2003*, Lecture Notes in Computer Science, vol. 2894, Berlin, Germany: Springer, 2003, pp. 452–473.
- V. Shoup, "Practical Threshold Signatures," in *Advances in Cryptology—EUROCRYPT 2000*, Lecture Notes in Computer Science, vol. 1807, Berlin, Germany: Springer, 2000, pp. 207–220.
- Y. Desmedt and Y. Frankel, "Threshold Cryptosystems," in *Advances in Cryptology—CRYPTO'89 Proceedings*, Lecture Notes in Computer Science, vol. 435, New York, NY, USA: Springer, 1990, pp. 307–315.
- K. A. Shim, "Design Principles of Secure Certificateless Signature and Aggregate Signature Schemes for IoT Environments," *IEEE Access*, vol. 10, pp. 124848–124857, 2022, doi: 10.1109/ACCESS.2022.3224928.
- S. S. Al-Riyami and K. G. Paterson, "Certificateless Public Key Cryptography," in *Advances in Cryptology – ASIACRYPT 2003*, Lecture Notes in Computer Science, vol. 2894, Berlin, Germany: Springer, 2003, pp. 452–473.
- V. Shoup, "Practical Threshold Signatures," in *Advances in Cryptology—EUROCRYPT 2000*, Lecture Notes in Computer Science, vol. 1807, Berlin, Germany: Springer, 2000, pp. 207–220.
- L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.
- K. A. Shim, "Design Principles of Secure Certificateless Signature and Aggregate Signature Schemes for IoT Environments," *IEEE Access*, vol. 10, pp. 124848–124857, 2022.
- L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.
- V. Shoup, "Practical Threshold Signatures," in *Advances in Cryptology—EUROCRYPT 2000*, Lecture Notes in Computer Science, vol. 1807, Berlin, Germany: Springer, 2000, pp. 207–220.
- S. S. Al-Riyami and K. G. Paterson, "Certificateless Public Key Cryptography," in *Advances in Cryptology – ASIACRYPT 2003*, Lecture Notes in Computer Science, vol. 2894, Berlin, Germany: Springer, 2003, pp. 452–473.

Acknowledgement

The authors also wish to thank many anonymous referees for their suggestions to improve this paper.

Author Declaration

I would like to express my deepest gratitude to my supervisor for their invaluable guidance, unwavering support and constructive feedback throughout the entire research process. Their expertise and encouragement have been instrumental in shaping the direction of this study.