RESEARCH ARTICLE

Cryptanalysis of an Authentication Protocol for Edge-Centric Maritime Transportation Systems

Shuangshuang Liu[1,*], **Marko Hölbl**[2], **Renato R. Maaliw III**[3] and **Md. Solaiman Mia**[4]

[1] DISSec, College of Cyber Science, Nankai University, Tianjin 300071, China
[2] Faculty of Electrical Engineering and Computer Science, University of Maribor, Maribor 2000, Slovenia
[3] College of Engineering, Southern Luzon State University, Lucban 4328, Quezon, Philippines
[4] Department of CSE, Green University of Bangladesh, Dhaka, Bangladesh

Abstract

With the rapid development of edge computing and intelligent maritime transportation systems, secure authentication and key agreement protocols have become essential for protecting communications among maritime entities and edge devices. Recently, Mahmood et al. proposed an authentication protocol for edge-centric maritime transportation systems, claiming that their scheme can resist various security attacks while ensuring efficient communication. However, practical maritime environments still face many security threats. In addition, edge infrastructures usually have limited resources. Therefore, authentication protocols require rigorous security evaluation. In this paper, we perform a cryptanalysis of Mahmood et al.'s protocol and reveal several critical security weaknesses. We demonstrate that the protocol is vulnerable to temporary random-number leakage attacks and privileged insider attacks, which may enable adversaries to compromise authentication information and session security. Moreover, we show that the protocol fails to provide perfect forward secrecy, meaning that previously established session keys may be exposed once long-term secret credentials are compromised. These vulnerabilities reduce the security reliability and practical applicability of the original scheme in real-world maritime transportation environments. To address these issues, we discuss several measures for improvement and provide recommendations to strengthen the protocol's security. Our analysis provides useful guidance for the future design of secure authentication protocols in edge-centric maritime transportation systems.

Keywords: edge computing, intelligent maritime transportation systems, authentication protocol, temporary random number leakage attack, privileged insider attack, perfect forward secrecy.

1 Introduction

With the deep application of Internet of Things (IoT) technology in the maritime domain, modern maritime transportation systems gradually evolve toward intelligent and data-driven architectures. Various

Submitted: 19 May 2026
Accepted: 09 June 2026
Published: 14 June 2026

Vol. 2, **No.** 2, 2026.
10.62762/JRSC.2026.765456

***Corresponding author:**
✉ Shuangshuang Liu
shuangliu0309@163.com

Citation
Liu, S., Hölbl, M., Maaliw III, R. R., & Mia, M. S. (2026). Cryptanalysis of an Authentication Protocol for Edge-Centric Maritime Transportation Systems. *Journal of Reliable and Secure Computing*, 2(2), 104–110.

heterogeneous devices are deployed across ships, ports, and shipping infrastructure. These devices continuously generate multi-source data, including operational status, environmental monitoring, and business interactions. As data scales grow and real-time processing demands increase, traditional centralized architectures struggle to meet system requirements for latency and reliability. Consequently, distributed processing models centered on edge computing have become the mainstream solution. In this model, the system performs initial data processing at the edge near the source and then uploads information to cloud platforms for unified management and analysis. This approach reduces transmission burdens while improving overall processing efficiency.

However, this distributed architecture introduces new security challenges while enhancing performance [2–4]. Since edge nodes typically operate in open or semi-trusted environments, the system's attack surface expands significantly. During practical operation, maritime systems must frequently exchange information among multiple entities. This information often contains sensitive content, such as identity identifiers, navigation status, and control commands [5]. If attackers steal or manipulate this data during transmission or storage, it may lead to identity theft, data forgery, or even system control risks. Furthermore, privileged insiders abusing their authority further exacerbate overall security threats [6, 7]. Therefore, constructing a communication mechanism that balances security and efficiency in such complex environments remains a critical problem.

To address these issues, researchers widely consider identity authentication and key agreement mechanisms as fundamental technical tools for system security. By establishing a trusted authentication process between communicating parties and dynamically generating session keys, the system effectively prevents unauthorized access. Simultaneously, these mechanisms ensure the confidentiality and integrity of communication content during transmission, thereby providing basic secure communication guarantees for maritime transportation systems.

To address the security challenges in edge-centric maritime transportation systems, Mahmood et al. proposed an authentication and key agreement scheme aimed at securing interactions among communicating entities [1]. However, further security analysis reveals that their scheme still suffers from several potential vulnerabilities. Specifically, it fails to resist privileged insider attacks and temporary random number leakage attacks, and does not provide perfect forward secrecy. These weaknesses may allow the adversary to obtain sensitive information under certain attack models, thereby posing serious threats to the overall system security.

Based on the above analysis, this paper provides a detailed discussion of the security vulnerabilities in Mahmood et al.'s scheme [1] and presents several improvement recommendations regarding the identified flaws. These suggestions mainly include strengthening the protection mechanism of random numbers, enhancing the security design of verification information, and improving the session key generation process, in order to increase the protocol's resistance against relevant attacks and strengthen its forward secrecy. The analysis presented in this paper offers useful guidance for the design and optimization of future secure authentication protocols in edge-centric maritime transportation systems.

The main contributions of this paper are summarized as follows:

1. We conduct a systematic security analysis of the authentication scheme proposed by Mahmood et al. and identify several security weaknesses, including vulnerability to privileged insider attacks and temporary random number leakage attacks, as well as the lack of perfect forward secrecy.

2. We analyze the potential security risks caused by the above vulnerabilities in detail. We also show that an adversary can obtain sensitive information under specific attack models.

3. To address these security issues, we propose several improvement suggestions, including strengthening random number protection, improving the storage of verification information, and enhancing the session key agreement mechanism. These measures aim to improve the overall security of the protocol.

2 Review of Mahmood et al.'s Scheme

This section reviews Mahmood et al.'s protocol. Their protocol includes three entities: mobile edge computing (MEC) servers, mobile users, and a maritime cloud server (MCS). The protocol executes

across four phases: initialization, mobile user registration, MEC server registration, and mutual authentication. We outline the specific details below:

2.1 Initialization Phase

During system initialization, the MCS generates a system master key $MK \in Z_p^*$. Subsequently, the MCS selects a one-way hash function $h(\cdot)$ and publishes it as a public parameter. Meanwhile, the MCS securely stores MK to ensure system security.

2.2 Mobile User Registration Phase

Each user V_{ui} registers with the MCS before performing mutual authentication with the server MEC_{s_j}.

1. The user V_{ui} sends a registration request containing identity ID_{ui} to the MCS. Upon receiving the request, the MCS compares this identity against the database. If the identity does not exist, the MCS requests the user to select a new one. If the identity exists, the MCS generates a challenge C_{ui} and sends it to the user.

2. After receiving C_{ui}, V_{ui} generates a response $R_{ui} \leftarrow PUF(C_{ui})$ via their Physical Unclonable Function (PUF) and returns this response to the MCS.

3. MCS then assigns a temporary identity TID_{ui} to the user. Subsequently, MCS calculates $K_{ui} = h(ID_{ui} \parallel MK)$. The MCS stores the user identity ID_{ui} and the corresponding challenge-response pair $\langle C_{ui}, R_{ui} \rangle$ in the database. It also binds this data to TID_{ui} and protects the record using the master key MK.

4. Finally, the MCS sends $\langle TID_{ui}, K_{ui} \rangle$ to the user. V_{ui} securely stores this information in a trusted device.

2.3 MEC Server Registration Phase

MEC_{s_j} sends a registration request message to the MCS. Upon receiving the request, the MCS assigns an identity ID_{s_j} and a pseudonym SID_{s_j} to MEC_{s_j}. Subsequently, the MCS calculates $K_{s_j} = h(ID_{s_j} \parallel MK)$. The MCS stores the mapping between K_{s_j} and SID_{s_j} in the database and encrypts this record using MK. Finally, the MCS returns $\langle K_{s_j}, SID_{s_j} \rangle$ to MEC_{s_j}. MEC_{s_j} saves the received information securely in its memory.

2.4 Mutual Authentication Phase

1. First, V_{ui} generates a random number r_{ui} and calculates $T_{ui} = ID_{ui} \oplus r_{ui}$ and $Ver_{ui} = h(ID_{ui} \parallel K_{ui} \parallel SID_{s_j} \parallel r_{ui})$. Subsequently, V_{ui} sends the message $\{TID_{ui}, T_{ui}, Ver_{ui}\}$ to MEC_{s_j}. Upon receiving the message, MEC_{s_j} stores the relevant information and forwards $\{TID_{ui}, SID_{s_j}\}$ to the MCS to request user authentication.

2. The MCS receives the request and matches the temporary identity TID_{ui} within its database. It checks whether the identity belongs to the current or previous session record to enhance resistance against desynchronization attacks. After a successful match, the MCS retrieves the corresponding user identity and challenge-response data. The MCS also obtains the server key K_{s_j} via SID_{s_j} and generates a new temporary identity TID_{ui}^{new}. Subsequently, the MCS recomputes the user's long-term key $K_{ui} = h(ID_{ui} \parallel MK)$. It then constructs the encrypted message $\alpha = Enc_{K_{s_j}}(ID_{ui}, \langle C_{s_j}, R_{s_j} \rangle, TID_{ui}^{new}, K_{ui})$, updates the local TID record, and sends α to MEC_{s_j}.

3. Upon receiving α, MEC_{s_j} decrypts α to obtain the user information and recovers the random number $r_{ui} = T_{ui} \oplus ID_{ui}$. It then verifies the validity of the user identity. MEC_{s_j} terminates the session if the verification fails. Otherwise, it generates a random number r_{s_j} and calculates the session parameter T_{s_j}, parameter β, and session key $SK = h(ID_{ui} \parallel SID_{s_j} \parallel r_{ui} \cdot r_{s_j} \parallel \beta)$. After generating the verification value Ver_{s_j}, MEC_{s_j} sends $\{T_{s_j}, Ver_{s_j}\}$ to V_{ui}.

4. Finally, V_{ui} recovers the relevant parameters, recomputes the session key SK, and validates Ver_{s_j}. If the verification fails, V_{ui} assumes an active attack and terminates the session immediately. Otherwise, both parties accept SK as the shared session key for the current communication.

3 Cryptanalysis of Mahmood et al.'s Scheme

3.1 Attack Model

By referring to the adversarial capabilities defined in the Dolev-Yao (DY) model [8] and the Canetti-Krawczyk (CK) model [9], we assume that the attacker A possesses the following abilities.

- A can fully control all communication messages

transmitted over public channels. They can perform passive eavesdropping and active attacks on messages during transmission, including interception, modification, and deletion [10–12].

- A can obtain the long-term private keys or master keys held by a legitimate communication entity (e.g., users, edge nodes, or cloud servers). This assumption is solely used to analyze whether the scheme satisfies perfect forward secrecy [13, 14].
- Given that servers are typically deployed in unattended or weakly physically protected environments, A may gain access to sensitive information stored on the server side [15–18].
- A may obtain temporary random numbers or ephemeral secret values generated by a communication entity during scheme execution, enabling temporary random number leakage attacks [19, 20].

3.2 Analysis of Mahmood's scheme

In this section, we conduct a security vulnerability analysis of Mahmood's scheme [1] and find that it is vulnerable to temporary random-number leakage attacks and privileged insider attacks. Additionally, the scheme lacks perfect forward secrecy. Below are the specific details of the analysis.

Temporary Random Number Leakage Attack: The temporary random number leakage attack refers to the process by which an attacker A can obtain random numbers generated by a single entity and exploit them in combination with information transmitted over a public channel to compromise the scheme. Suppose A acquires the random number r_{ui} generated by V_{ui} and combines it with the message T_{ui} transmitted over the public channel.

(1) A can compute

$$ID_{ui} = T_{ui} \oplus r_{ui}$$

(2) A can compute

$$(C_{ui} \parallel TID_{ui}^{new} \parallel r_{sj}) = r_{ui} \oplus T_{sj}$$

based on r_{ui} and message T_{sj} transmitted over the public channel.

(3) A can compute

$$\beta = Gen(ID_{ui} \parallel TID_{ui}^{new})$$

(4) A can obtain the session key

$$SK = h(ID_{ui} \parallel SID_{sj} \parallel r_{ui} \parallel r_{sj} \parallel \beta)$$

Therefore, Mahmood et al.'s scheme cannot resist temporary random number leakage attacks.

Privileged Insider Attack: The privileged insider attack refers to a process where an attacker A, acting as an insider with access to a server, physically obtains information stored on the server and then combines it with messages transmitted over public channels to attack the scheme. Assume A, acting as a privileged insider, can obtain $\{K_{sj}, SID_{sj}\}$ stored on the server and also intercept the message α transmitted over public channels.

(1) A can compute

$$Dec_{K_{sj}}(\alpha) = (ID_{ui}, \langle C_{sj}, R_{sj} \rangle, TID_{ui}^{new}, K_{ui})$$

(2) A can compute

$$r_{ui} = T_{ui} \oplus ID_{ui}$$

(3) Based on the obtained r_{ui} and T_{sj} transmitted via the public channel, A computes

$$(C_{ui} \parallel TID_{ui}^{new} \parallel r_{sj}) = r_{ui} \oplus T_{sj}$$

(4) Based on the acquired ID_{ui} and TID_{ui}^{new}, A can compute

$$\beta = Gen(ID_{ui} \parallel TID_{ui}^{new})$$

(5) Finally, A can compute the session key:

$$SK = h(ID_{ui} \parallel SID_{sj} \parallel r_{ui} \parallel r_{sj} \parallel \beta)$$

Therefore, Mahmood et al.'s scheme cannot resist the privileged insider attack.

Perfect Forward Secrecy: Perfect forward secrecy means that even if the long-term keys of both communication parties are compromised at some future point, A cannot recover previously established session keys. Here we assume A can obtain the long-term key K_{sj} of MEC and combine it with messages α transmitted over the public channel.

(1) A can compute

$$Dec_{K_{sj}}(\alpha) = (ID_{ui}, < C_{sj}, R_{sj} >, TID_{ui}^{new}, K_{ui})$$

(2) Based on the obtained information ID_{ui} and the message T_{ui} transmitted via the public channel, A can compute

$$r_{ui} = T_{ui} \oplus ID_{ui}$$

(3) Based on the obtained r_{ui} and T_{sj} transmitted via the public channel, A can compute

$$(C_{ui} \parallel TID_{ui}^{new} \parallel r_{sj}) = r_{ui} \oplus T_{sj}$$

(4) Based on the acquired ID_{ui} and TID_{ui}^{new}, A can compute

$$\beta = Gen(ID_{ui} \parallel TID_{ui}^{new})$$

(5) Combining the message SID_{sj} transmitted over the public channel, A can compute the session key:

$$SK = h(ID_{ui} \parallel SID_{s_j} \parallel r_{ui} \cdot r_{s_j} \parallel \beta)$$

Therefore, Mahmood et al.'s scheme does not have perfect forward secrecy.

4 Discussion of Defense Attacks

In this section, we propose further improvement directions from a system design perspective, targeting the primary security vulnerabilities in the protocol Mahmood et al. developed. We provide specific defense strategies against three typical attacks to enhance the security and robustness of the protocol in practical maritime edge computing environments.

1. Regarding the privileged insider attack, attackers typically attempt offline analysis or forge authentication processes after obtaining verification information from the server database. To mitigate this risk, edge servers should avoid storing sensitive authentication parameters in plaintext or with weak protection. If the system must store verification data, it should employ strong encryption mechanisms. For instance, encrypting the verification table using symmetric or public-key encryption ensures that attackers cannot directly perform identity forgery or password guessing even after a database breach.
2. Regarding the perfect forward secrecy, the current protocol maintains a link between long-term keys and session keys. Consequently, a compromise of the long-term key threatens the security of historical sessions. To address this issue, we suggest introducing a one-time ephemeral key pair or a temporary random key generation mechanism during each session initialization. This ensures that each session key remains independent. Through this method, attackers cannot backtrack or recover historical communication content even if they compromise the long-term system key in the future, effectively strengthening the protocol's forward security.
3. Regarding the temporary random number leakage attack, which exploits the short-term exposure of random numbers to derive sensitive information, the authors recommend a Multi-Factor Authentication (MFA) mechanism. This approach combines random numbers with additional security factors, such as biometric data or device-binding information. Even if an attacker obtains a temporary random number, they cannot complete identity forgery or session recovery using only a single factor. This significantly improves the overall security and attack resistance of the protocol.

In summary, comprehensive optimization of storage mechanisms, key generation methods, and authentication processes effectively alleviates these three security issues. These improvements provide a reliable reference for designing secure authentication protocols in maritime edge computing environments.

5 Conclusion

In this paper, we presented a cryptanalysis of Mahmood et al.'s authentication protocol for edge-centric maritime transportation systems. Despite its claimed provable security, we identified three critical weaknesses: vulnerability to temporary random number leakage attacks, susceptibility to privileged insider attacks, and the lack of perfect forward secrecy. We further suggested several improvement directions, including strong encryption for verifier storage, the use of ephemeral key pairs, and the integration of multi-factor authentication. Our findings underscore the necessity of rigorous security evaluation and provide a useful reference for designing more secure authentication protocols in maritime edge computing environments. In future work, we plan to construct an improved protocol that addresses these weaknesses while remaining efficient for resource-constrained maritime edge devices.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

Marko Hölbl served as an Associate Editor of the *Journal of Reliable and Secure Computing* at the time of manuscript submission. To ensure the integrity of the peer-review process, Marko Hölbl was not involved in the editorial handling, peer review, or decision-making process for this manuscript, which was handled independently by another editor. The remaining authors declare no conflicts of interest.

AI Use Statement

The authors declare that no generative AI was used in the preparation of this manuscript.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Mahmood, K., Shamshad, S., Ayub, M. F., Ghaffar, Z., Khan, M. K., & Das, A. K. (2023). Design of provably secure authentication protocol for edge-centric maritime transportation system. *IEEE Transactions on Intelligent Transportation Systems, 24*(12), 14536-14545. [CrossRef]

[2] Liu, J., Li, C., Bai, J., Luo, Y., Lv, H., & Lv, Z. (2021). Security in IoT-enabled digital twins of maritime transportation systems. *IEEE Transactions on Intelligent Transportation Systems, 24*(2), 2359-2367. [CrossRef]

[3] Gyamfi, E., Ansere, J. A., Kamal, M., Tariq, M., & Jurcut, A. (2022). An adaptive network security system for iot-enabled maritime transportation. *IEEE transactions on intelligent transportation systems, 24*(2), 2538-2547. [CrossRef]

[4] Jakob, M., Vaněk, O., & Pěchouček, M. (2011). Using agents to improve international maritime transport security. *IEEE Intelligent Systems, 26*(1), 90-96. [CrossRef]

[5] Gupta, B. B., Gaurav, A., Hsu, C. H., & Jiao, B. (2021). Identity-based authentication mechanism for secure information sharing in the maritime transport system. *IEEE Transactions on Intelligent Transportation Systems, 24*(2), 2422-2430. [CrossRef]

[6] Chen, C. M., Hao, Y., Kumari, S., & Amoon, M. (2025). An intelligent blockchain-enabled authentication protocol for transportation cyber-physical systems. *IEEE Transactions on Intelligent Transportation Systems, 26*(9), 14053-14066. [CrossRef]

[7] Wu, T. Y., Wu, H., Kumari, S., & Chen, C. M. (2025). An enhanced three-factor based authentication and key agreement protocol using PUF in IoMT. *Peer-to-Peer Networking and Applications, 18*(2), 83. [CrossRef]

[8] Dolev, D., & Yao, A. (1983). On the security of public key protocols. *IEEE Transactions on information theory, 29*(2), 198-208. [CrossRef]

[9] Canetti, R., & Krawczyk, H. (2001, April). Analysis of key-exchange protocols and their use for building secure channels. In *International conference on the theory and applications of cryptographic techniques* (pp. 453-474). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[10] Chen, C. M., Liu, S., Li, X., Islam, S. H., & Das, A. K. (2023). A provably-secure authenticated key agreement protocol for remote patient monitoring IoMT. *Journal of Systems Architecture, 136*, 102831. [CrossRef]

[11] Thakur, G., Prajapat, S., Kumar, P., & Chen, C. M. (2024). A privacy-preserving three-factor authentication system for IoT-enabled wireless sensor networks. *Journal of Systems Architecture, 154*, 103245. [CrossRef]

[12] Kumar, P., Pal, A. K., & Islam, S. H. (2024). 2F-MASK-VSS: Two-factor mutual authentication and session key agreement scheme for video surveillance system. *Journal of Systems Architecture, 153*, 103196. [CrossRef]

[13] Xu, M., & Wang, D. (2025). Practical two-factor authentication protocol for real-time data access in WSNs. *IEEE Transactions on Dependable and Secure Computing, 22*(5), 5215-5230. [CrossRef]

[14] Zhang, Y., He, D., Vijayakumar, P., Luo, M., & Huang, X. (2023). SAPFS: An efficient symmetric-key authentication key agreement scheme with perfect forward secrecy for industrial Internet of Things. *IEEE Internet of Things Journal, 10*(11), 9716-9726. [CrossRef]

[15] Wang, D., Li, W., & Wang, P. (2018). Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. *IEEE Transactions on Industrial Informatics, 14*(9), 4081-4092. [CrossRef]

[16] Wang, C., Wang, D., Tu, Y., Xu, G., & Wang, H. (2020). Understanding node capture attacks in user authentication schemes for wireless sensor networks. *IEEE Transactions on Dependable and Secure Computing, 19*(1), 507-523. [CrossRef]

[17] Wang, D., Wang, N., Wang, P., & Qing, S. (2015). Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity. *Information Sciences, 321*, 162-178. [CrossRef]

[18] Liu, S., & Wang, Z. (2025). Security analysis on a two-factor privacy-preserving protocol for efficient authentication in Internet of Vehicles networks. *IEEE Internet of Things Journal, 12*(16), 34623-34632. [CrossRef]

[19] Moghadam, M. F., Nikooghadam, M., Al Jabban, M. A. B., Alishahi, M., Mortazavi, L., & Mohajerzadeh, A. (2020). An efficient authentication and key agreement

scheme based on ECDH for wireless sensor network. *IEEE Access*, *8*, 73182-73192. [CrossRef]

[20] Kwon, D. K., Yu, S. J., Lee, J. Y., Son, S. H., & Park, Y. H. (2021). WSN-SLAP: Secure and lightweight mutual authentication protocol for wireless sensor networks. *Sensors*, *21*(3), 936. [CrossRef]

Shuangshuang Liu received the B.S. degree in computer technology from Shandong University of Science and Technology, China, in 2023. She is currently pursuing a Ph.D. degree in DISSec, College of Cyber Science, Nankai University, China. (Email: shuangliu0309@163.com)

Marko Hölbl is an associate professor in Computer Science and Vice-Dean for Research at the University of Maribor, Faculty of Electrical Engineering and Computer Science. His research focuses on cybersecurity, including cryptography, network and internet security, data protection, digital forensics, blockchain technology, and user aspects of information security and privacy. He has been involved in numerous national and international research and development projects in cybersecurity. He coordinated the H2020 project CyberSec4Europe – Cybersecurity for Europe- and a national project on cyber resilience for the Slovenian Armed Forces' ICT and weapon systems. He is currently involved in the Digital Europe project AKADIMOS, supporting the development of the European Cybersecurity Skills Academy, and the ESA RPA project PQC Key Management. He has published a broad range of scientific work, including journal articles, conference papers, and book chapters, in respected international venues. His work is widely cited in major scientific databases, and he is also active as an editor, guest editor, reviewer, and conference organizer in cybersecurity and information systems.(Email: marko.holbl@um.si)

Renato R. Maaliw III is a full-fledged Professor and the former Dean of the College of Engineering in Southern Luzon State University, Lucban, Quezon, Philippines. He has a doctorate in Information Technology with specialization in Machine Learning, a Master's degree in Information Technology with specialization in Web Technologies, and a Bachelor's degree in Computer Engineering. His area of interest is in computer engineering, web technologies, and software engineering, data mining, machine learning and analytics. He has published original research in various domains involving data analytics & visualizations, won best paper awards at international conferences, and served as a technical reviewer for conferences and reputable journals.(Email: rmaaliw@slsu.edu.ph)

Md. Solaiman Mia received the B. Sc. (Hons.) and M. S. in Computer Science and Engineering (CSE) from University of Dhaka, Bangladesh. He is currently working as an Assistant Professor in the Dept. of CSE, Green University of Bangladesh. Before this, he worked as an Assistant Professor in the Dept. of CSE in Shanto-Mariam University of Creative Technology and Dhaka International University. He also worked as a Lecturer in the Dept. of CSE in Hamdard University Bangladesh and Asian University of Bangladesh. Solaiman received the MOICT Fellowship from Bangladesh Government for his research works. He is currently serving as a Professional Member of IEEE, IEEE Computer Society, Life Time Member of Bangladesh Computer Society and ISOC Bangladesh Dhaka Chapter. He has some experiences as a Reviewer in some international journals and conferences. Some of his research works have been published in some reputed national and international journals and conferences. An international research book is also published by him. His research interests include Reversible Logic Synthesis, Machine Learning, Quantum Computing, Data Mining, etc.(Email: solaiman@cse.green.edu.bd)