An Effective Privacy-Preserving Blockchain-Assisted Security Protocol for Cloud-Based Digital Twin Environment

Arun Kumar K, Chandru T, Gunasekaran R, Harshavardhan B S, Janani.G
Dept. of IT., RMD Engineering College, Tiruvallur

***Abstract*: The DT environment involves the formation of a clone of the tangible object to perform simulations in the virtual space. The combination of conceptual development, predictive maintenance, real-time monitoring, and simulation characteristics of DT has increased the utilization of DT in different scenarios, such as medical environments, healthcare, manufacturing industries, aerospace, etc. However, these utilizations have also brought serious security pitfalls in DT deployment. Towards this, several authentication protocols with different security and privacy features for DT environments have been proposed. In this article, we first review a recently proposed two-factor authentication protocol for DT environments that utilizes the blockchain technology. However, the analyzed scheme is unable to offer the desirable security and cannot withstand various security attacks like offline password-guessing attack, smart card stolen attack, anonymity property, and known session-specific temporary information attack. We also demonstrate that an attacker can impersonate the analyzed protocol's legal user, owner, and cloud server. To mitigate these security loopholes, we devise an effective three-factor privacy-preserving authentication scheme for DT environments. The proposed work is demonstrated to be secure by performing the informal security analysis, the formal security analysis using the widely recognized Burrows-AbadiNeedham (BAN) logic, and the Real-or-Random (ROR) model. A detailed comparative study on existing competing schemes including the analyzed scheme demonstrates that the devised framework furnishes better security features while also having lower computation costs and comparable communication costs than the existing schemes.**

KEYWORDS: Burrows-AbadiNeedham (BAN) logic; Real-or-Random (ROR) model; DT environment;

I. INTRODUCTION

A Digital Twin is a real-time digital replica of a physical system that accurately reflects its features. The DT environment involves the formation of a clone of the tangible object to perform simulations in the virtual space. Grieves and Vickers first proposed the idea of performing simulations with a clone in a virtual environment in 2002, and National Aeronautics and Space Administration (NASA) in 2010 referred to the method as a DT [2]. The DT concept was developed to make it possible to reap the benefits of paradigms like Industry 4.0 and the industrial Internet of Things (IIoT). The idea is to make every product or process-related data source and control interface description accessible through a single interface for automatic communication establishment and auto-discovery. Without specific knowledge of each component, developers and engineers can determine, design, and construct the required interfaces, integrations, and communication links by analyzing the DTs of the incorporated components [3]. The devices may eventually be able to locate and communicate with one another without the need for a human engineer to stand in between them. With the assistance of DTs, this kind of auto-discovery and auto-established communication may eventually make IoT more scalable for currently unimaginable applications. The numerous fields in which DT technology is being studied are manufacturing, construction, healthcare, and space industries. IoT and mobile devices have recently been added to the DT technology's application range. For instance, autonomous driving can be achieved in a vehicular environment, and precise and detailed remote medical treatment can be carried out in a medical.

II. OBJECTIVE

A Digital Twin is a real-time digital replica of a physical system that accurately reflects its features. The DT environment involves the formation of a clone of the tangible object to perform simulations in the virtual space. Grieves and Vickers first proposed the idea of performing simulations with a clone in a virtual environment in 2002, and National Aeronautics and Space Administration (NASA) in 2010 referred to the method as a DT The DT concept was developed to make it possible to reap the benefits of paradigms like Industry 4.0 and the industrial Internet of Things (IIoT). The idea is to make every product or process-related data source and control interface description accessible through a single interface for automatic communication establishment and auto-discovery.

III. PROPOSED ALGORITHM

The proposed work is demonstrated to be secure by performing the informal security analysis, the formal security analysis using the widely recognized Burrows-Abadi Needham (BAN) logic, and the Real-or-Random (ROR) model. A detailed comparative study on existing competing schemes including the analyzed scheme

demonstrates that the devised framework furnishes better security features while also having lower computation costs and comparable communication costs than the existing schemes.

The goal of the suggested solution would be to guarantee that security measures that protect privacy and make use of blockchain technology don't adversely affect the functionality and effectiveness of the digital twin environment. This could entail decreasing computing cost, balancing trade-offs between security and performance, and optimizing algorithms.

Advantages of Proposed System

Enhanced Data Privacy

Immutable and Transparent Transactions

Decentralization and Trust lessness

Smart Contract Automation:

Improved Security

IV. MODULE DESCRIPTION

In this project have 3 modules:

1. Data Owner
2. Data User
3.Cloud Server
4.Network 1
5.Network 2

DATAOWNER

- Register the account with the basic information
- After authorized by cloud owner can login the account
- Make a request for key
- View key and upload the file with the encrypted format, If we need to select the network and node for file uploaded.
- View files
- Logout

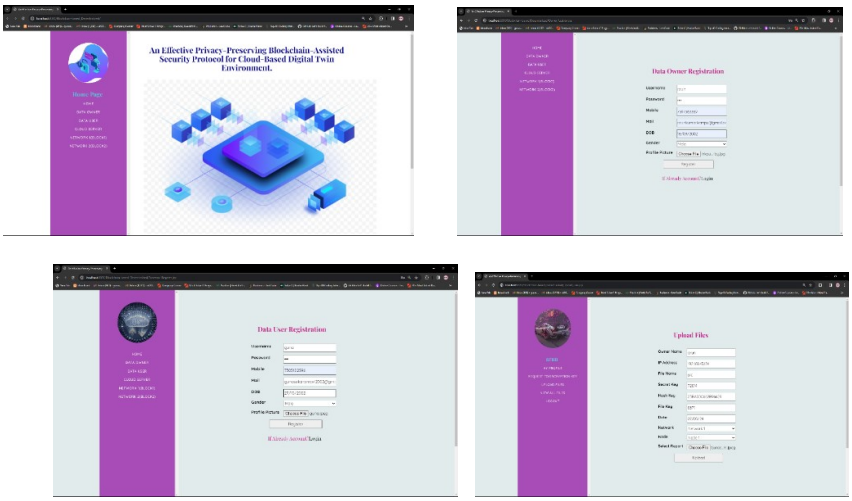
- DATAUSER
- Register the account with the basic information
- After authorized by cloud user can login the account
- View uploaded files with encrypted format
- Make a request for particular file
- If we enter the key correctly means, the file should be downloaded.
- After downloaded it should be decrypted format.
- Logout

- CLOUD SERVER
- Login the account with the correct credentials
- View owner and authorize them.
- View user and authorize them.
- View owner request and Send key for File upload
- Send Decryption Key
- View all uploaded files
- Graph
- Logout

- NETWORK1
- Login the account with correct credentials
- View network1 uploaded files
- Logout

- NETWORK2
- Login the account with correct credentials
- View network2 uploaded files
- Logout

V. RESULTS AND DISCUSSION



An user friendly page to get primary details of data owner during the first time registration of data owner and after the first time registration website host will accept the register form of data owner and accept it in the cloud server, then the data owner can able to login next time of getting into the page.

To get primary details of user data during the first time registration of user and after the first time registration website house will accept the register from of data user and accept it in the cloud server, then the user can able to login next time of getting into the page.

Cloud server where data owner can able to generate private and public key for the file and then they can send key to the user via g-mail. The website host can able to accept many data owners and and data users.

Data owner can only upload the files and user can able to access the files. The data owner will protect the file by giving only access to data to limited user by providing the key.

VI. CONCLUSION

In this work, we examined various design flaws and vulnerabilities of the scheme suggested in opposition to numerous cryptographic attacks, like user impersonation, KSSTIA, and offline password guessing attacks. By utilizing blockchain technology, we proposed an enhanced three-factor-based privacy-preserving authentication framework for the DT environment. The informal security analysis of the proposed scheme shows the efficiency and enhanced security against various wicked attacks. In addition, we would also like to develop a complete testbed experiment for practical aspects of the proposed scheme.

REFERENCES

[1] B.Piascik, J. Vickers, D. Lowry, S. Scotti, J. Stewart, and A. Calomino, ‘‘Materials, structures, mechanical systems, and manufacturing roadmap,’’ NASA, Washington, DC, USA, Tech. Rep. TA 12, 2012.

[2] H. Laaki, Y. Miche, and K. Tammi, ‘‘Prototyping a digital twin for real time remote control over mobile networks: Application of remote surgery,’’ IEEE Access, vol. 7, pp. 20325–20336, 2019.

[3] H. Wang and J. Zhang, ‘‘Blockchain based data integrity verification for large-scale IoT data,’’ IEEE Access, vol. 7, pp. 164996–165006, 2019.

[4] C.Nagarajan and M.Madheswaran - ‘Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter’ - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[5] C.Nagarajan and M.Madheswaran - ‘Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis’- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.

[6] C.Nagarajan and M.Madheswaran - ‘Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques’- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.

[7] C.Nagarajan and M.Madheswaran - ‘Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis’- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.

[8] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. “Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter” Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.

[9] C. Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya “Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay” Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022.

[10] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash “Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM” Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756

[11] G.Neelakrishnan, S.N.Pruthika, P.T.Shalini, S.Soniya, “Perfromance Investigation of T-Source Inverter fed with Solar Cell” Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:744-749

[12] C.Nagarajan and M.Madheswaran, “Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation” has been presented in ICTES’08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007

[13] M Suganthi, N Ramesh, “Treatment of water using natural zeolite as membrane filter”, Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022

[14] M Suganthi, N Ramesh, CT Sivakumar, K Vidhya, “Physiochemical Analysis of Ground Water used for Domestic needs in the Area of Perundurai in Erode District”, International Research Journal of Multidisciplinary Technovation, pp: 630-635, 2019

[15] P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, ‘‘Blockchain data-based cloud data integrity protection mechanism,’’ Future Gener. Comput. Syst., vol. 102, pp. 902–911, Jan. 2020.
[16] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, ‘‘Blockchain based data integrity service framework for IoT data,’’ in Proc. IEEE Int. Conf. Web Services (ICWS), Jun. 2017, pp. 468–475.
[17] S. Son, D. Kwon, J. Lee, S. Yu, N.-S. Jho, and Y. Park, ‘‘On the design of a privacy-preserving communication scheme for cloud-based digital twin environments using blockchain,’’ IEEE Access, vol. 10, pp. 75365–75375, 2022.
[18] T.-Y. Wu, Y.-Q. Lee, C.-M. Chen, Y. Tian, and N. A. Al-Nabhan, ‘‘An enhanced pairing-based authentication scheme for smart grid communications,’’ J. Ambient Intell. Humanized Comput., vol. 2021, pp. 1–13, Jan. 2021.
[19] S. Khatoon, S. M. M. Rahman, M. Alrubaian, and A. Alamri, ‘‘Privacypreserved, provable secure, mutually authenticated key agreement protocol for healthcare in a smart city environment,’’ IEEE Access, vol. 7, pp.
[20] A. Sengupta, A. Singh, P. Kumar, and T. Dhar, ‘‘A secure and improved two factor authentication scheme using elliptic curve and bilinear pairing for cyber physical systems,’’
[21] H. S. Grover and D. Kumar, ‘‘Cryptanalysis and improvement of a threefactor user authentication scheme for smart grid environment,’’ J. Reliable Intell. Environ., vol. 6, no. 4, pp. 249–260, Dec. 2020.