Fig. 5. Results of the communication cost of each transaction

system phase is 1.99 s. The average time needed to execute the register device phase is 0.89 s with a standard deviation of 0.23 s and the highest time to execute the register device phase is 1.37 s. The average time needed by the device to re-authenticate to the blockchain-fog node is 0.03 s with a standard deviation of 0.006 s and the highest time to execute the authentication device phase is 0.04 s.

TABLE VI
TIME NEEDED TO EXECUTE PHASE

| Phase | Time needed to execute phase | |
	AVG	STD
Registration system	1.26 s	0.38 s
Registration device	0.89 s	0.23 s
Authentication device	0.03 s	0.006 s

V. CONCLUSION

To overcome security problems in outdoor temperature monitoring problems, the authors proposed a decentralized IoT system and implement a blockchain-based authentication mechanism. The results of the evaluation that have been performed are that the time complexity for generating transactions is affected by the large number of processes contained in a transaction and the speed of the processing algorithm. Furthermore, communication costs are affected by the number of final process inputs per transaction. In addition, the time complexity of doing the three phases of authentication is affected by the number of blocks included in the blockchain and the rules that are owned by the smart contract. To ensure the security of blockchain, future work will be focused to evaluate the security of blockchain-based authentication mechanisms of IoT systems against various attack models.

REFERENCES

[1] U. Khalid, M. Asim, T. Baker, P. C. Hung, M. A. Tariq, and L. Rafferty, ""a decentralized lightweight blockchain-based authentication mechanism for iot systems"," *Cluster Computing*, vol. 23, no. 3, pp. 2067–2087, 2020.

[2] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, ""a survey of iot applications in blockchain systems: Architecture, consensus, and traffic modeling"," *ACM Computing Surveys (CSUR)*, vol. 53, no. 1, pp. 1–32, 2020.

[3] W. Viriyasitavat, T. Anuphaptrirong, and D. Hoonsopon, "When blockchain meets internet of things: Characteristics, challenges, and business opportunities," *Journal of industrial information integration*, vol. 15, pp. 21–28, 2019.

[4] M. Zhaofeng, M. Jialin, W. Jihui, and S. Zhiguang, ""blockchain-based decentralized authentication modeling scheme in edge and iot environment"," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2116–2123, 2020.

[5] Z. Tian, B. Yan, Q. Guo, J. Huang, and Q. Du, ""feasibility of identity authentication for iot based on blockchain"," *Procedia Computer Science*, vol. 174, pp. 328–332, 2020.

[6] I. Sibarani, E. S. Pramukantoro, and F. A. Bakhtiar, ""blockchain implementation based on bigchaindb and tendermint on iot data storage systems," "implementasi blockchain berbasis bigchaindb dan tendermint pada sistem penyimpanan data iot"," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN*, vol. 2548, p. 964X, 2019.

[7] A. Z. Ourad, B. Belgacem, and K. Salah, ""using blockchain for iot access control and authentication management"," in *International Conference on Internet of Things*. Springer, 2018, pp. 150–164.

[8] S. J. Basha, V. S. Veesam, T. Ammannamma, S. Navudu, and M. Subrahmanyam, ""security enhancement of digital signatures for blockchain using eddsa algorithm"," in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*. IEEE, 2021, pp. 274–278.

[9] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B.-Y. Yang, ""high-speed high-security signatures"," *Journal of cryptographic engineering*, vol. 2, no. 2, pp. 77–89, 2012.

[10] B. Bhat, A. W. Ali, and A. Gupta, ""des and aes performance evaluation"," in *International Conference on Computing, Communication & Automation*. IEEE, 2015, pp. 887–890.