International Journal of Data Science and Artificial Intelligence (IJDSAI)
Volume 02, Issue 03, May – June (2024)

RESEARCH ARTICLE

BLOCK CHAIN ENABLED DATA SECURITY USING BLOWFISH ALGORITHM IN SMART GRID NETWORK

R.C. Ilambirai [1,*], S. Lourdu Jame [2] and P.U. Poornima [3]

[1] Department of Electrical and Electronics Engineering, SRMIST, Kattankulathur, Chennai, Tamil Nadu, 603203 India.
[2] Department of Electrical and Electronics Engineering, SRMIST, Kattankulathur, Chennai, Tamil Nadu, 603203 India.
[3] Department of Electrical and Electronics Engineering, SRMIST, Kattankulathur, Chennai, Tamil Nadu, 603203 India.

[*]*Corresponding e-mail: ilambirai12@gmail.com*

Abstract – Smart Grid provides a reliable and efficient end-to-end delivery system. Data on each user's unique electricity consumption is given in real time. It also enables utilities to control and monitor the electrical system in real-time, helping them to reduce power outages. Users' privacy is a significant issue in addition to the usual security issues. Data about power usage may be used to infer private information about users by entities with access to the data. To solve these problems, a Block-Chain-based Secure Smart Grid Network (BCS-SGN) has been created, utilizing group signatures and covert channel permission to guarantee user validity. Initially, the data from the smart grid network will be collected and encrypted using blowfish techniques. After encryption, the encrypted data will be stored in the block chain network, which also stores the transmission logs. In order to utilize the security controller, smart contracts are analyzed using smart grid devices. DES, AES, and BCS-SGN are widely used. Symmetric key algorithms are properly compared in this study. Additionally, the metrics of encryption/decryption time, computational time, and throughput are also compared. The percentage of the proposed method, BCS-SGN, is 20%, AES is 15%, and DES is 12%. These outcomes demonstrate that the proposed BCS-SGN outperforms other techniques.

Keywords *– Smart grid, Smart contract, Blowfish Algorithm, Block chain.*

1. INTRODUCTION

The recent blooming expansion of the network, in both wired and wireless environments, has been the primary driver of the smart grid as an emerging technology. As a result of the interconnection-based environment, there are many different types of edge infrastructure or devices available for energy service offers [1–3]. All electrical devices, smart meters, and other embedded systems with an energy-related focus are connected on the Smart Grid Network (SGN) platform [4]. A basic SGN can be set to have network nodes that are multiple electric sources and different user kinds [5–7]. As a result, network characteristics and service model usage might result in governance and optimization.

In order to guarantee sufficient confidentiality, integrity, and availability, researchers are encouraged to look into viable methods while using such a large-scale network. Users' privacy is a significant issue in addition to the usual security issues [8]. Data about power usage may be used to infer private information about users by entities with access to the data. Detecting household gadgets and people [9], profiling electric vehicles (EVs), and human location and activity patterns [10] are a few examples of this information.

Differential privacy is a notable and commonly used concept for formalizing data privacy [11]. It ensures that the presence or absence of an individual has no effect on the result by adding controlled randomness to the data. Moreover, "local" differential privacy is widely employed since it doesn't need a trustworthy data curator. Since blockchain doesn't save information on the identities of ENs or group signatures, the model protects privacy from the standpoint of the signature.

These methods have significantly advanced the protection of the privacy of power usage data [12]. Other techniques, such as homomorphic encryption and blockchain-based systems, have been utilized to protect the anonymity of energy usage [13]. This work makes an effort to offer a comprehensive system that secures and maintains user privacy in smart grids without relying on a centralized or reliable authority. The following list of contributions might be used to summarize this work.

- Initially the data from the smart grid network will be collected and encrypted using blowfish technique.
- After Encryption the encrypted data will be stored in the block chain network, which also stores the transmission logs. Smart contracts provide the most secure approach because they operate on the blockchain.
- This paper focused on privacy concerns related to smart grids and offered an alternative that would

enhance data security while maintaining smart grid performance.

- Additionally, the metrics of encryption/decryption time, computational time, and throughput are compared in order to evaluate the proposed method.

The remaining sections of the paper are arranged as follows. Section 2 offers a review of related work. The model design and the main suggested algorithms are then presented in Sections 3 and 4, respectively. Additionally, Section 5 provides analysis and evaluation outcomes. The profession is concluded in Section 6 lastly.

2. LITERATURE SURVEY

The literature on privacy-preserving smart grid systems has been reviewed. To deal with this problem, scholars have employed a variety of methods and resources.

In 2022 S., Jha, et.al [14] proposed a secure technique, in which the availability of energy, financial and environmental security has been interconnected that also affects the development of people. The electric power industry should place a strong emphasis on comprehensive energy security, which is based on the security of power grids. As a result, the conversion of energy for both essential and end uses is intricately interwoven, necessitating a large-scale energy plan.

In 2022 Subhash, P., et.al [15] proposed a big data framework, in the area of energy usage which has been influenced by the smart grid. The end-to-end, two-way delivery method offered by Smart Grid is effective and dependable. Real-time data on a user's individual electricity usage is provided. In order to get the star rating for each particular appliance, the study first determine the potential number of appliances used by a single user.

In 2021 Xiao, L., et.al [16] suggested a simple identity authentication technique, which uses elliptic curve encryption (ECC) technology, suitable for smart grid environments. In the suggested protocol, the identity and key information are encrypted using ECC, and the session's validity is checked using the timestamp. The cost analysis concludes by demonstrating that the suggested protocol is appropriate for implementation in large-scale intelligent smart grid setups since it has lower communication and calculation costs than other relevant protocols.

In 2021 Zainab et al [17] suggested big data management, in which order to handle the data in the grid. In order to comprehend the sources and types of data in the grid, data management tools and procedures have been used. The report highlights the shortcomings of the current approaches geared toward using large amounts of data from the smart grid.

3. BLOCK CHAIN-BASED SECURE SMART GRID NETWORK

In this study a novel Block Chain based Secure Smart Grid Network (BCS-SGN) has been proposed. Initially the data from the smart grid network will be collected and encrypted using blowfish techniques. After Encryption the encrypted data will be stored in the block chain network, which also stores the transmission logs. The proposed BCS-SGN protects and upholds user privacy without depending on a centralized authority. The overall planned workflow is shown in Figure 1.

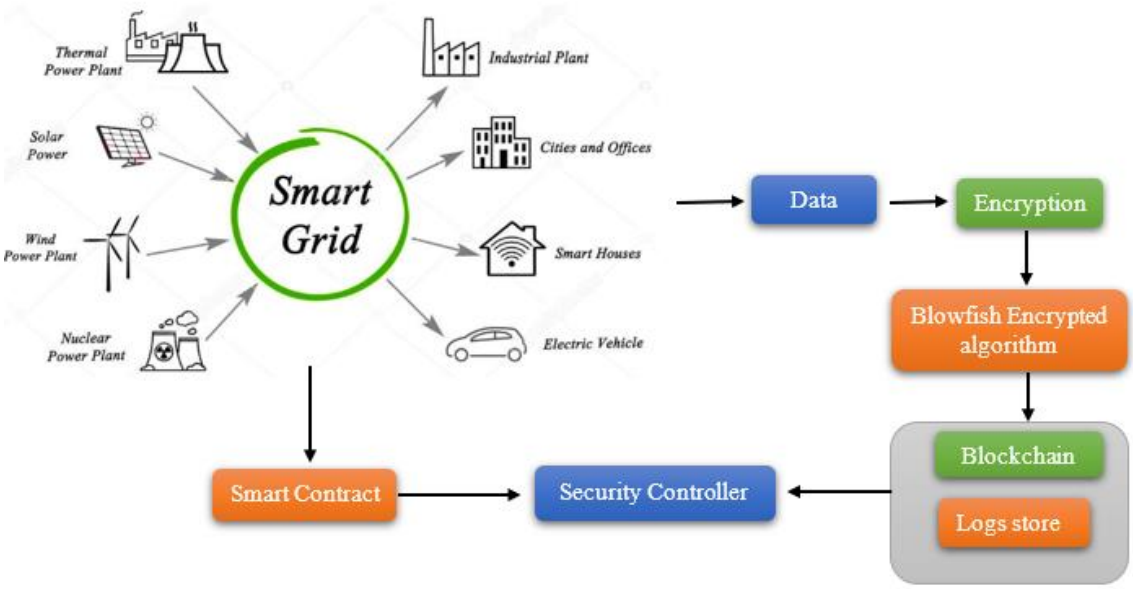

Figure 1. BCS-SGN framework

3.1 Blowfish Encrypted Algorithm

Using the same secret key for both encryption and decryption, Blowfish is a symmetric encryption method. Another block cipher is Blowfish, which separates a message into blocks of a predetermined length for encryption and decoding. Data encryption and protection are made possible with the help of the symmetric block cipher known as the Blowfish.

3.1.1 Data Encrypted Algorithm

The procedure repeats fifteen times, exchanging the two 32-bit segments (L and R) as the XOR operation is completed. The ciphertext is generated by performing an XOR calculation with the remaining P array and computing the cipher function following the fifteenth iteration. This algorithm, which uses S-boxes, is thought to have its most complicated component in the computation of the cipher function. The following algorithms are shown Table 1.

Table 1. Data Encrypted Algorithm

Algorithm 1: Data Encryption
Divide 64 bits in to two 32bit
Halves:1to 16
For i=1 to 16
XL=XL XOR Pi
XR=F(XL)XOR XR
Swap XL and XR
Swap XL and XR
XR=XR XOR P17
XL=XL XOR P18
Concatenate XL and XR

3.2 Block chain Smart Contract

The blockchain server where smart contracts are deployed is called the smart contract. Our model takes into account the practicality of applying blockchain technology so that a smart contract will determine the best course of action for energy allocations. We create dynamic programming in order to generate the best possible solution for the distribution of energy resources while taking into account three factors: communication security, latency time, and energy consumption. The smart contract is used to broadcast the operations, allowing each edge node to inform the node operator about how well it predicts it will handle the next request.

3.3 Block chain

A blockchain system that uses a layer of authorization to establish the scope of users or voters and grant access to the system to that target group is known as a permissioned blockchain. The platform for data storage that our model chooses is a permissioned blockchain for two main reasons. A key factor in the development of our approach is the potential of blockchain to protect privacy. According to our observations, a permissionless blockchain is not ideal considering that the user groups in the smart grid energy trading scenario are mostly internal entities connected via SGNs with a very constant identification state.

4. RESULT AND DISCUSSION

The performance of the Novel BlockChain-based Secure Smart Grid Network (BCS-SGN) has been discussed in this section. Matlab is one program that can be used to simulate the blockchain process. This can be used to spread the blockchain and mine blocks with incorrect hashes for testing, as multiple nodes can carry out the activity in the simulation. With Matlab, one gigabyte of RAM at minimum and sixty gigabytes of disk space at most are available for each worker. mimic procedures and perform MatLab algorithms on historical blockchain data. one gigabyte of RAM at minimum and sixty gigabytes of disk space at most for each worker. The assessment of the suggested methods performance is provided in this part. DES is a well-known algorithm, and the performance of AES was compared to the previously recommended methods, BCS-SGN.

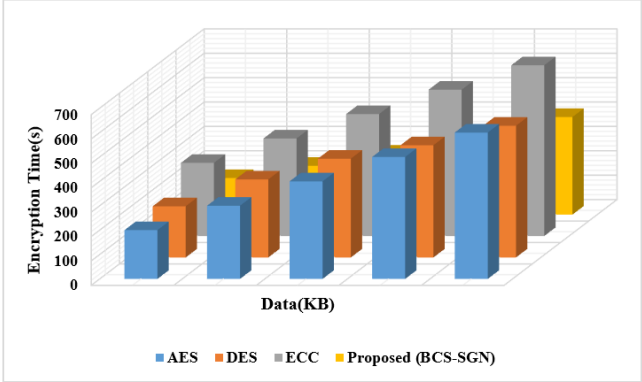

Figure 2. Encryption time

A graph comparing the encryption times the encryption part's graphical comparison is shown in Figure. 2. A nearly proposed approach from the Blowfish algorithm.

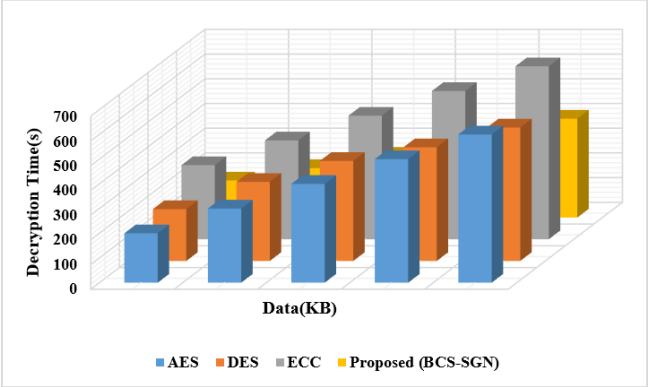

Figure 3. Decryption time

Figure 3 displays a graphical comparison of the decryption section. The suggested method outperforms the Blowfish algorithm.

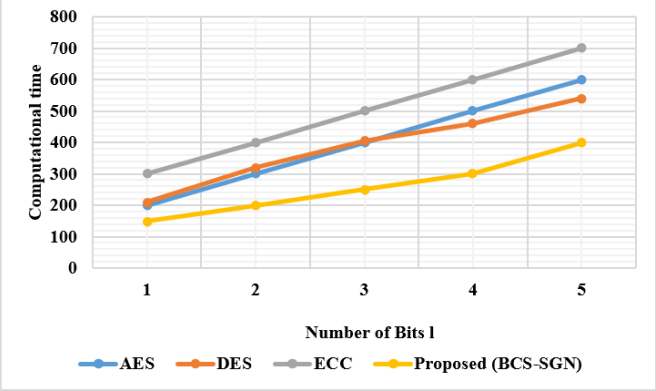

Figure 4. Computational time comparison

In Figure. 4, the bit number of the relevant characteristic, l, is directly correlated with the computational overheads of Extension.

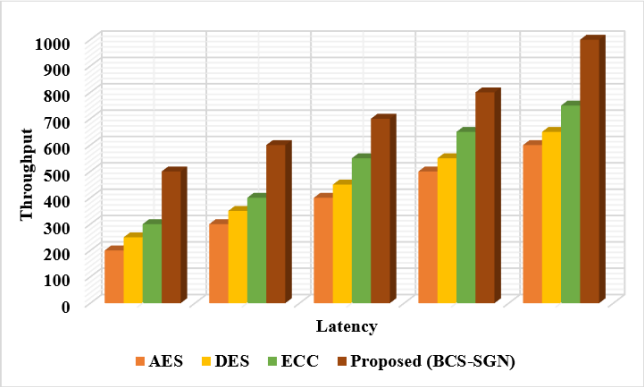

Figure 5. Throughput

In Figure. 5, the quantity of data or information moving from one location to another is known as throughput. By combining the total number of plaintexts in megabytes by the entire amount of time needed to complete each encryption step, the throughput of an encryption system can be computed.

5. CONCLUSION

In this paper, a novel blockchain-based smart grid network (BCS-SGN) has been created, utilizing group signatures and covert channel permission to guarantee user validity. Initially, the data from the smart grid network will be collected and encrypted using blowfish techniques. After encryption, the encrypted data will be stored in the block chain network, which also stores the transmission logs. In order to utilize the security controller, smart contracts are analyzed using smart grid devices. DES, AES, BCS-SGN, and the other four widely used symmetric key algorithms are properly compared in this study. Additionally, the metrics of encryption/decryption time, computational time, and throughput are also compared. The percentage of the proposed method, BCS-SGN, is 20%, AES is 15%, and DES is 12%. These outcomes demonstrate that the proposed BCS-SGN outperforms other techniques. This study concludes with a number of recommendations for additional research. The suggested algorithm needs to be improved upon or supported by additional research.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

FUNDING STATEMENT

Not applicable.

ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

REFERENCES

[1] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5g beyond", *IEEE Network*, pp. 99, no. 1, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[2] S. Wang, X. Zhang, Y. Zhang, L. Wang, J. Yang, and W. Wang, "A survey on mobile edge networks: Convergence of computing, caching and communications", *IEEE Access*, vol. 5, pp. 6757–6779, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[3] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Basar, "Dependable demand response management in the smart grid: A stackelberg game approach," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 120–132, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[4] N. Nikmehr and S. Ravadanegh, "Optimal power dispatch of multimicrogrids at future smart distribution grids", *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1648–1657, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[5] Y. Zhang, R. Yu, M. Nekovee, Y. Liu, S. Xie, and S. Gjessing, "Cognitive machine-to-machine communications: visions and potentials for the smart grid", *IEEE Network*, vol. 26, no. 3, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[6] K. Wang, Y. Wang, X. Hu, Y. Sun, D. Deng, A. Vinel, and Y. Zhang, "Wireless big data computing in smart grid", *IEEE Wireless Communications*, vol. 24, no. 2, pp. 58–64, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[7] Y. Zhang, R. Yu, S. Xie, W. Yao, Y. Xiao, and M. Guizani, "Home M2M networks: architectures, standards, and QoS improvement", *IEEE Communications Magazine*, vol. 49, no. 4, pp. 44–52, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[8] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks", *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 530– 538, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[9] K. Gai, M. Qiu, Z. Ming, H. Zhao, and L. Qiu. Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks. IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2431– 2439, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[10] G. Liang, J. Zhao, F. Luo, S. Weller, and Z. Dong, "A review of false data injection attacks against modern power systems", *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[11] K. Gai, M. Qiu, Z. Ming, H. Zhao, and L. Qiu, "Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks", *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2431– 2439, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[12] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid", *IEEE Security & Privacy*, vol. 3, no. 75–77, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[13] M. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges", *Future Generation Computer Systems*, vol. 82, pp. 395– 411, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[14] S. Jha, H.A. Abdeljaber, M.K. Imam Rahmani, M.M. Waris, A. Singh, and M. Yaseen, "An Integration of IoT, IoC, and IoE towards building a green society", *Scientific Programming*, 2022 [CrossRef] [Google Scholar] [Publisher Link]

[15] P. Subhash, K.S. Surya, and A.B. Reddy, "Analysis of Smart Grid Data for Appliance Prediction and Efficient Power Consumption", *In 2022 International Conference on Recent Trends in Microelectronics, Automation, Computing and*

Communications Systems (ICMACC) pp. 1-5, 2022. IEEE. [CrossRef] [Google Scholar] [Publisher Link]

[16] L. Xiao, J. Cai, M. Qiu, and M. Liu, "A Secure Identity Authentication Protocol for Edge Data in Smart Grid Environment", *In 2021 8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2021 7th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, pp. 188-193, 2021. IEEE. [CrossRef] [Google Scholar] [Publisher Link]

[17] A. Zainab, A. Ghrayeb, D. Syed, H. Abu-Rub, S.S. Refaat, and O. Bouhali, "Big data management in smart grids: Technologies and challenges", *IEEE Access*, vol. 9, pp.73046-73059, 2021. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

R.C. Ilambirai completed her B.E degree in the Department of Electrical and Electronics Engineering in 2002, M.Tech in Power Electronics in 2004 and her research in 2022 all from Tamilnadu, India.She is working as an Assistant Professor in the Department of Electrical and Electronics Engineering, SRM Institute of Science and Technology, Chennai, Tamilnadu, India.She has a good expertise in the field of inverters, dc-dc power converters, integration of converters with renewable energy sources, their applications etc. Overall, she has published 18 papers in International Journals and 8 Conference publications. She is a life member of MISTE, MIEI and member of IEEE.

S. Lourdu Jame is working as an Assistant Professor in the Department of Electrical and Electronics Engineering in SRM Institute of Science and Technology. She completed her B.E Electrical and Electronics Engineering in the year 2010, M.Tech in the year 2012 and Ph.D in the year 2023. The total professional experience is 11 years. Her areas of specialization are Thermoelectric Generator, Energy storage, Energy conservation. She has published 12 international publications among which 2 are SCI indexed journals. She is a life member of IEEE.

P.U. Poornima obtained her B.Tech in the Electrical and Electronics Engineering in 2003 under JNTU, Hyderabad and M.Tech in Power Electronics in 2005 from VIT University, Vellore and Ph.d in 2022 from SRMIST, Tamilnadu, India. She is working as an Assistant Professor in Electrical &Electronics Engineering, SRM Institute of Science and Technology, Chennai. Her research areas of interests are Integration of renewable energy sources, Inverters, Converters, Drives applications etc. She has published 10 research papers in international journals and presented four papers in International and National conferences. She is a life member of IEI and member of IEEE.

Arrived: 05.05.2024
Accepted: 17.06.2024