frontiers in Blockchain

HYPOTHESIS AND THEORY
published: 08 December 2021
doi: 10.3389/fbloc.2021.770074

Asymmetric Confidentiality in Blockchain Embedded Smart Grids in Galois Field

Bannishikha Banerjee, Ashish Jani and Niraj Shah*

School of Engineering, PP Savani University, Surat, India

Economic growth requires a sharp increase in the utilization of energy. Since the initial mechanical era, financial development has been driven by industrialization, transportation, and, most important of all, electrification, majorly achieved by petroleum product ignition. This way of development has had malicious and abusive aftershocks on the environment since the beginning. Smart grids are an idea to slightly diminish the burden on our Mother Nature, but this idea is getting tainted by the anticipation of ferocious technophiles who may try to get the grid down using quantum computers in the coming years. Thus, security becomes one of the major concerns for the smart grid. In this paper, we propose a quantum-resistant framework for associating smart grids and blockchain embedded with a permutation-substitution-based public-key cryptosystem in Galois Field to prevent unauthorized access and perform encryption of the private information of the user and consumption statistics. Permutation and substitution are performed to increase the diffusion and confusion of the data. Expenditures are quantified from the dissipation particulars, and the payment of electricity bill is performed using our blockchain wallet. The prediction model of consumption data is generated availing stochastic gradient descent. The performance analysis of the proposed cryptosystem is predicted after a simulation of the smart grid.

Keywords: blockchain, smart grid, cryptography and smart city, quantum computing, simulation

OPEN ACCESS

Edited by:
Mohammad Jabed Morshed Chowdhury,
La Trobe University, Australia

Reviewed by:
Shahriar Badsha,
University of Nevada, Reno, United States
Narayan Ranjan Chakraborty,
Daffodil International University, Bangladesh
Khalid Hasan,
Victoria University, Australia

****Correspondence:***
Bannishikha Banerjee
bannishikha.banerjee@ppsu.ac.in

Specialty section:
This article was submitted to Blockchain in Industry, a section of the journal Frontiers in Blockchain

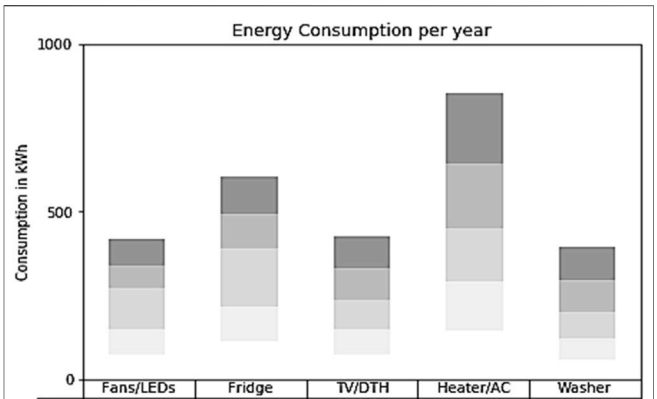
Received: *03 September 2021*
Accepted: *04 October 2021*
Published: *08 December 2021*

Citation:
Banerjee B, Jani A and Shah N (2021) Asymmetric Confidentiality in Blockchain Embedded Smart Grids in Galois Field. Front. Blockchain 4:770074. doi: 10.3389/fbloc.2021.770074

INTRODUCTION

In the last few decades, economic growth has demanded an exponential rise in energy consumption, be it industrialization, transportation, or merely electrification of households. The economy is thriving at the expense of fossil product-based energy frameworks, which indeed have been facing up to some difficulties, *viz*., fossil combustion consequences, climate contamination, and energy overuse (Liwen et al., 2012). Lately, many organizations have been working together to recompute the utilization of power sources and mitigate the energy extremity (Greenstone et al., 2019). The entire global framework relies on electricity apparatus built traditionally; this is resulting in exceeding ineffectiveness. Currently, in the existing electricity grid structure, resources are utilized blindly to meet the societal requirements (Kunmin et al., 2008). The extravagant use of resources and energy leads to the excessive release of carbon dioxide into the atmosphere, which is the major cause of global temperature rise. The worldwide carbon dioxide expulsion in the impending years is contemplated to outstretch at many gigatons. Almost half of the pollutants come from the electricity domain through the ignition of non-renewable energy sources like coal, oil, and petroleum gas to create the required energy. Consuming these exhaustible resources brings

about the creation of carbon dioxide, the essential warmth-catching, ozone-harming substance answerable for an unnatural weather change, notwithstanding other nitrogen and sulfur oxides liable for different natural effects (Adkins et al., 2010). The consequences of the current energy strategy in environmental contamination are self-evident (Aklin et al., 2017). Resulting from the immense utilization of energy, which applies a genuine effect on the presence of humankind and annihilates the recovery flow and surpasses the decontamination capacity of nature, numerous ecological issues have happened (Allcott and Rogers, 2014). Usage of non-restorable, life-suffocating sources makes the presently available electricity arrangement the worst choice. However, these electrical corporations could be made authentic and acceptable. A little commitment can be made for the assurance of the climate by disposing of the conventional power matrices and changing to futuristic frameworks. The Smart Grid can be visualized as a design or system for a modernized, extraordinary, and forefront step of our electrical power structure (Kai et al., 2008). A completely working Smart Grid will include sensors all through the transmission and conveyance network to gather information. A thorough arrangement of Smart Grid with renewables would be a major step to address environmental crashes (Hassan et al., 2021). The worldwide organizations are now coordinating together to develop a grid that is efficient and productive. Controlling authorities are effectively teaming up on inventive ways to deal with the making of Smart Grid (DayoAlowolodu et al., 2018). Furthermore, research shows that private buyers will pay more to reduce the half-life span of ozone-depleting substances (Biermann, 2003). Smart Grid is a desideratum for the diminution of environmental catastrophes. It will likewise require clear norms for interconnection measurements. This seems like a great idea, but security issues will always remain a major challenge. The rival countries or organizations would try to get the grid of each other down using several attacks. Especially in the presence of high-tech resources, breaking traditional cryptographic algorithms becomes fairly easy (Banerjee and Patel, 2016; Banerjee, 2019; Banerjee et al., 2020; Banerjee et al., 2021). Blockchain might be able to help us in this context. Electricity units or monetary transactions can be performed in the blockchain environment. Consumers can buy extra units of electricity or sell surplus units to potential buyers. Grids connected with this blockchain would be used to transfer the bought units to the legitimate consumer. This would enable equity in the distribution of electricity in urban as well as rural areas and reduce wastage, which would further increase cost-effectiveness. The consumers can perform monetary transactions using cryptocurrency as simulated by us in this paper, but the confidentiality and privacy of the personal information of the consumer along with transaction still remains an issue. Therefore, a security framework is the need of the hour that would protect the grid from getting compromised. In this paper, we propose an asymmetric cryptographic framework implanted with blockchain, simulated on OpenDSS, that would proficiently transmit the electricity consumption statistics and private information of the consumer over a network and would incorporate financial transactions among the consumers and providers of our hypothetical smart grid.



	Fans/LEDs	Fridge	TV/DTH	Heater/AC	Washer
2019	79.2	115.3	83.5	185.7	76.5
2018	68.3	109.8	82.8	183.1	74.9
2017	81.8	121.7	80.6	177.9	73.8
2016	79.6	118.3	78.7	170.3	71.2
2015	74.4	114.3	75.1	169.4	67.4

FIGURE 1 | Energy consumption.

ENERGY PROJECTION

To get an idea about the energy consumption of an average household, we performed a prediction analysis on the overall electricity consumption data, acquired from the Indian Institute of Technology, Bombay (Smart Energy Informatics, 2018), and equipment-wise electricity consumption, borrowed from[1]. Prediction is performed to understand the rate at which resource depletion is transpiring. Forecasts dependent on the current datasets are performed utilizing stochastic gradient descent AI-based meta-calculation (Johnson and Zhang, 2013)[2]. Stochastic gradient descent helps in consolidating different weak classifiers into a solitary solid classifier (Mahdavi et al., 2012). Stochastic gradient descent works by putting more weight on hard-to-group occasions and less on those "generally dealt with well" (Mahdavi et al., 2012) by using logistic regression. **Figure 1** demonstrates the prediction of energy consumption data.

Figure 1 shows the electricity consumption in a common household. This model is generated to understand the rate at which energy consumption and resource depletion is occurring because of the traditional grids; this helps us in understanding the importance of smart grids. Here we have computed the energy utilization of the individual units. Stochastic gradient descent is utilized to perform predictions dependent on the current dataset. Cutting edge energy framework is moving towards environmentally friendly power which will produce energy from photovoltaic boards, cell-based power modules,

[1]https://www.e-education.psu.edu/egee102/node/1915

[2]https://www.indigoadvisorygroup.com/blog/2017/3/6/global-energy-utilitiesBlockchain-pilots-and-use-cases

hydroelectric force, wind turbines, and other sources. Global organizations should deal with renewable energy and will require smart matrices for better and proficient transmission. Smart grids can react to dynamic changes in energy supply, which help normalize the changes. Despite having such countless favorable circumstances of smart matrices, there are still difficulties in its transformation with regards to the protection and security of clients and their information. For protection and security, blockchain is a potential idea. Blockchain can be utilized as a public record to follow the exchanges in the smart grid by utilizing virtual currency. Blockchain can likewise be utilized to share consumption information and track the carbon impression. Blockchain, as an innovation, guarantees the protected exchange of virtual cash and utilization information. Blockchain is not restricted to get an exchange of digital money; it can likewise be utilized to keep the record of energy utilization as well.

BLOCKCHAIN MODEL

Blockchain is an explicit type of database (Banerjee et al., 2020). It varies from a characteristic database in the way it stores information in a decentralized manner. Blockchains store data in blocks that are then chained together (Banerjee et al., 2020). As new data comes in, it is entered into a new block (Cui et al., 2020). Once the block is filled with data, it is chained onto the previous block, which makes the data chained together in a chronological fashion. Dissimilar types of information can be stored on a blockchain, but the most common use so far has been as a ledger for transactions. However, this is not the only place where blockchain can show its capabilities (Zhaofeng et al., 2020). Smart technology is another broad area where blockchain may thrive. The smart grid alludes to a high-level correspondence and data foundation that empowers enhancement in energy creation and transmission. The attributes of smart matrices include the entire energy management framework, from generators or energy providers to end-customers (Sikeridis et al., 2020). Savvy frameworks incorporate the capacity to empower dynamic client cooperation and encourage renewable energy alternatives. A viewpoint perspective on the smart lattice shows one grid performing tremendously well in different areas (Zoican et al., 2018). These areas can be power administration, beginning from energy creation and finishing with the client. Nonetheless, these areas are combined with the assistance of sensors and IoT devices that include numerous parts of information. Safeguarding the framework while providing flexibility and effectiveness becomes one of the major tasks of the smart grid (Dong et al., 2014). Kabalci et al. (2019) have proposed the Energy Internet, correspondingly known as the Internet of Energy (IoE). It has been bestowed by incorporating a smart lattice fixture with Internet innovation. Conversely, with the brilliant lattice, the energy internet is a rejoinder for energy kindred proceedings by obliging with IoT, progressed data and correspondence innovations, power framework parts, and other energy establishments (Agung and Handayani, 2020). The point of this creative methodology is to guarantee the association of energy anyplace whenever required. Power is distributed between the production entities and the consumption entities (Vishwakarma and Das, 2020). Entities like wind power plants, solar power plants, fossil fuel-based power plants, and similar factories are producers. Conversely, entities like homes, universities, gas stations, shopping malls, etc., are consumers. Connecting these entities in a secure blockchain fashion provides efficiency, confidentiality, and transparency in the smart grid. To secure the data of the above-mentioned organizations in a blockchain-based smart grid, we propose a permutation–substitution-based framework. Statistics gathering is conducted using sensors, IoT devices, and paraphernalia. Then, confidentiality is provided using the proposed approach, and authentication is bestowed using hashing algorithms. Finally, the data is shared on the blockchain. This would increase protection against quantum computing attacks. The model starts from data collection and then progresses to sharing the data on the blockchain framework. The data is collected using IoT devices. Filtering and cleaning of the collected data are performed. Later, the consumption data is encrypted. To provide authentication, the

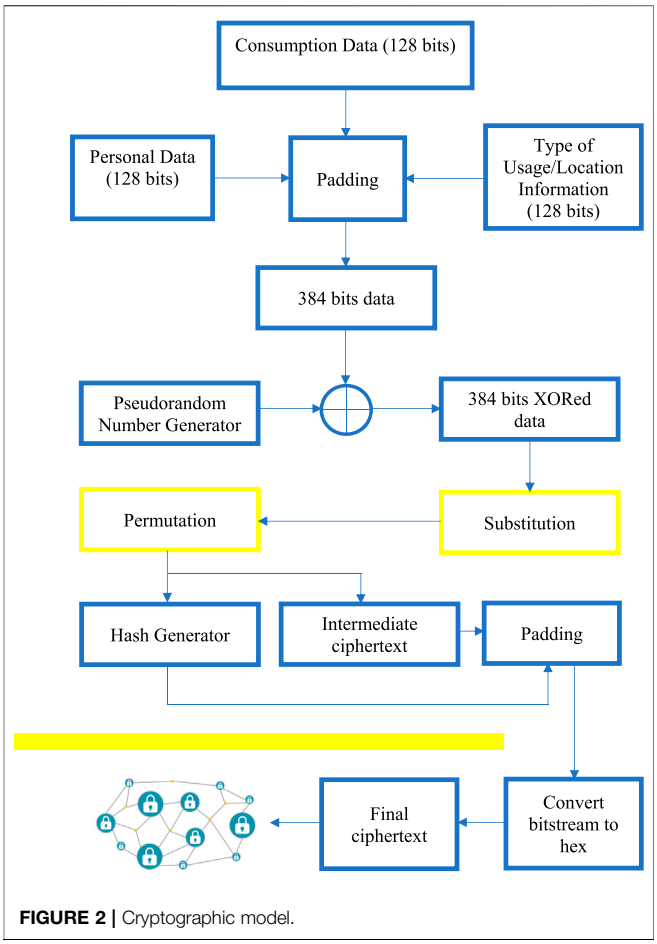


FIGURE 2 | Cryptographic model.

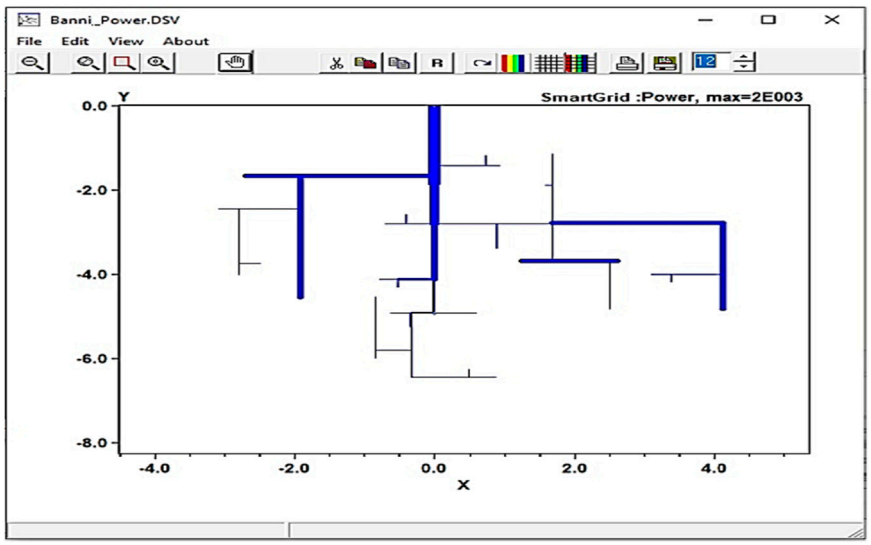


FIGURE 3 | Smart grid lines.

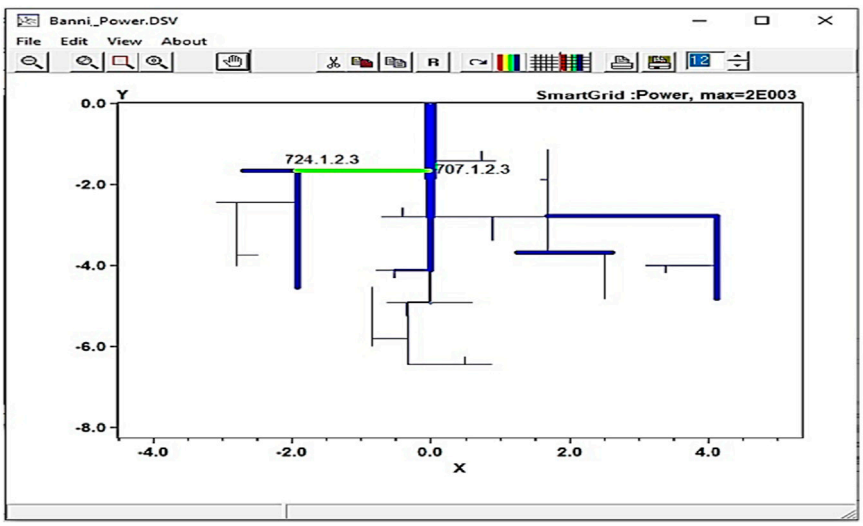


FIGURE 4 | Phase line.

hash value is computed and appended with the data. Then, it is shared on the blockchain framework. We devised a security framework for the securitization of smart grids. In the proposed flow, the consumption data is calculated using gamma function Γ(Z). It helps in modeling scenarios with uncertainty and continuous changes. Then, Gaussian integral is used to calculate the consumption data C_d over a particular time duration t. To generate a key pair from the pseudorandom generator, we used the extended Euclidean algorithm for Galois Field GF (n m).

$$p_r = Rn - 1 mod\, n$$

Rn is the public key generated by the pseudorandom generator. It is used in the encryption process. Subsequently, pr is the private key, and it is computed using Rn in field n of Galois Field. Pr is used in the decryption process. The following flow chart (**Figure 2**) demonstrates the securitization of smart grids using blockchain.

In the following equations, P_{d} is personal data, T_{u} is type of usage, R_{n} is random number generated, S is the hexadecimal number from substitution box; x is power consumption, z is auxiliary power consumed by the meter or sensor, etc., and k is the power wastage rate due to the deterioration of the panel or grid with passing time.

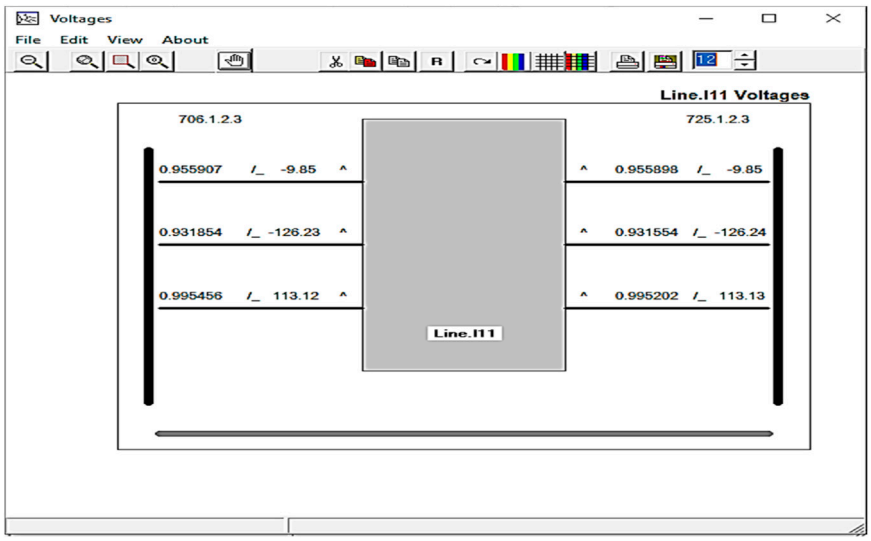


FIGURE 5 | Line voltage.

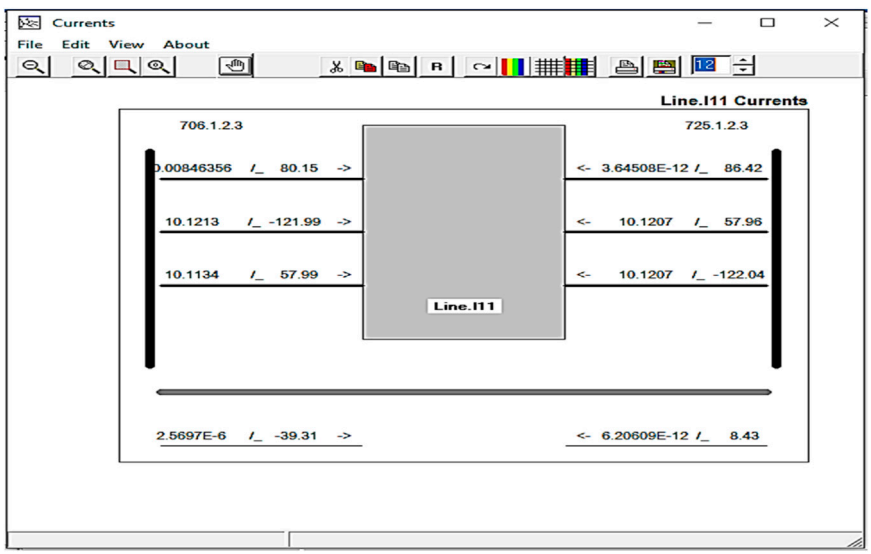


FIGURE 6 | Line current.

$$\Gamma(z) = \int_0^{\infty} t^{z-1} e^{-t} dt = \frac{e^{-\gamma z}}{z} \prod_{k=1}^{\infty} \left(1 + \frac{z}{k}\right)^{-1} e^{z/k}, \ \gamma \approx 0.577216$$

$$C_d = \int_{-\infty}^{\infty} e^{-x^2} dx = \left[\int_{-\infty}^{\infty} e^{-x^2} dx \int_{-\infty}^{\infty} e^{-t^2} dt\right]^{1/2} + \Gamma(z)$$

$$C_d = \int_{-\infty}^{\infty} e^{-x^2} dx = \left[\int_0^{2\pi} \int_0^{\infty} e^{-r^2} r dr d\theta\right]^{1/2} + \Gamma(z)$$

After calculating the consumption data, padding is performed between consumption data, personal data, and type of consumption. Personal data is padded on the most significant side of the consumption data. The type of consumption is padded on the least significant side of the same.

$$X = P_{\mathrm{d}} + C_{\mathrm{d}} + T_{\mathrm{u}}$$

Thereafter, XOR operation was performed between the resulting padded data and pseudo-random number generated from the random number generator.

$$Y = R_n \hat{} X$$

$$Y = Y_0 \ldots Y_n$$

The least significant half of the XORed data is stored as an integer in i, and the most significant half of the same is stored in j.

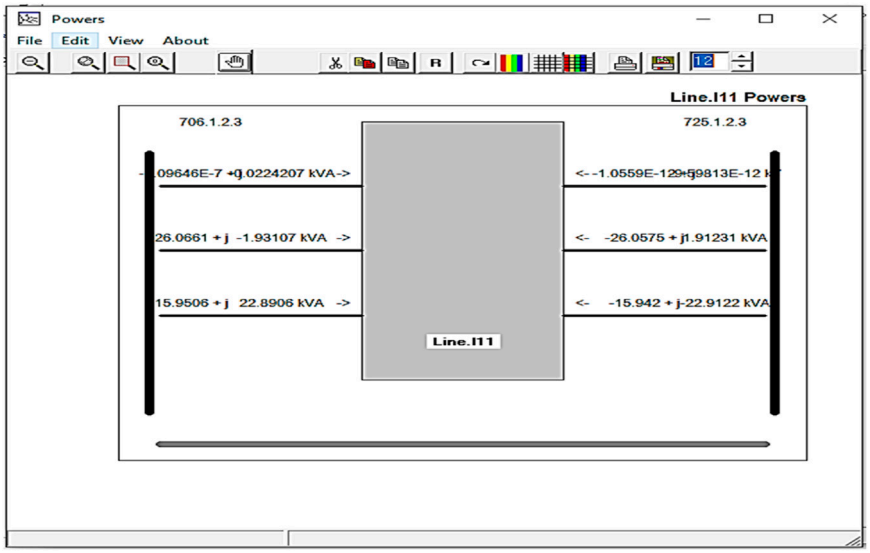


FIGURE 7 | Line power.

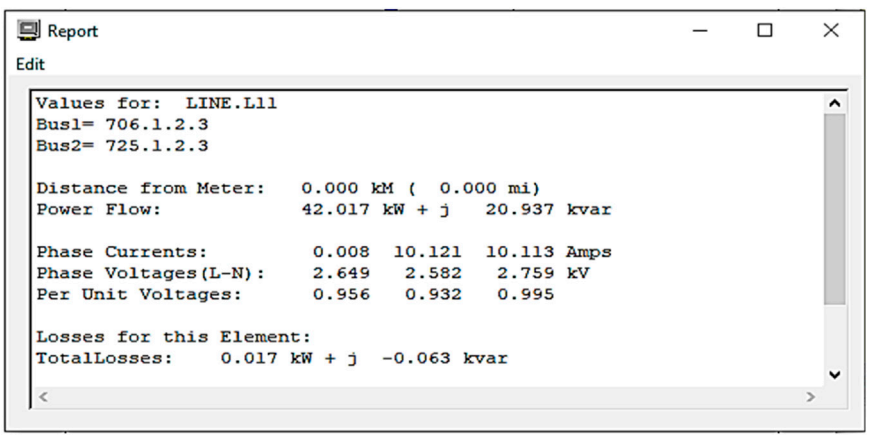


FIGURE 8 | Line.L11.

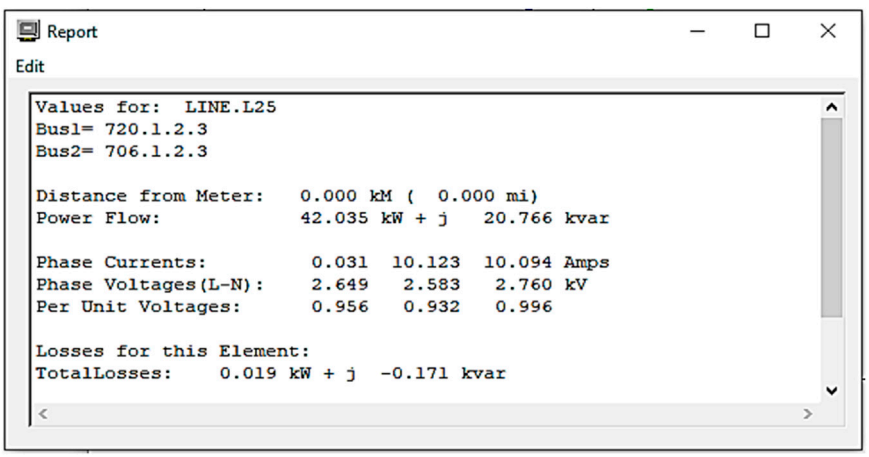


FIGURE 9 | Line.L25.

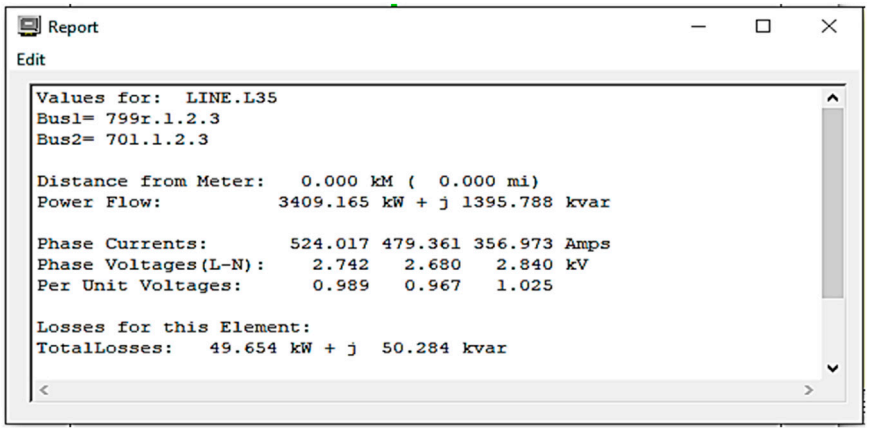


FIGURE 10 | Line.L35.

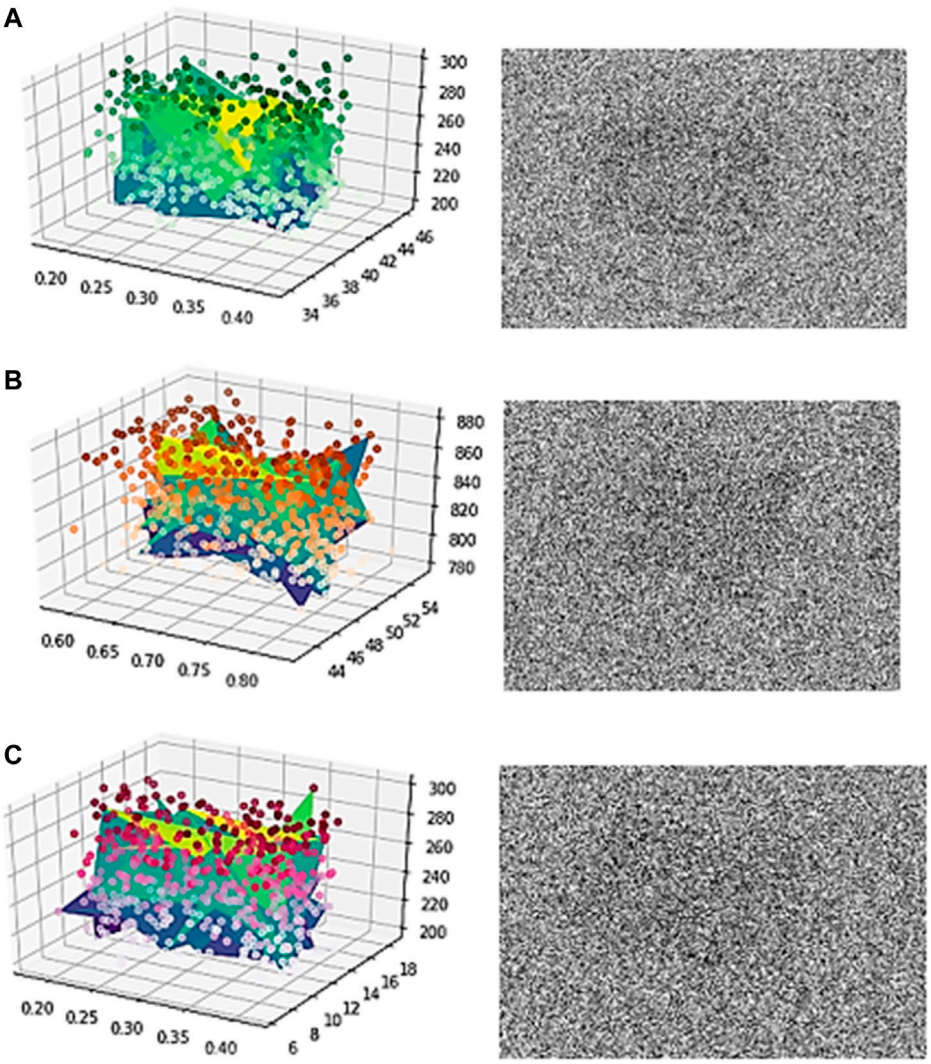


FIGURE 11 | (A, B, C) Consumption data encryption.

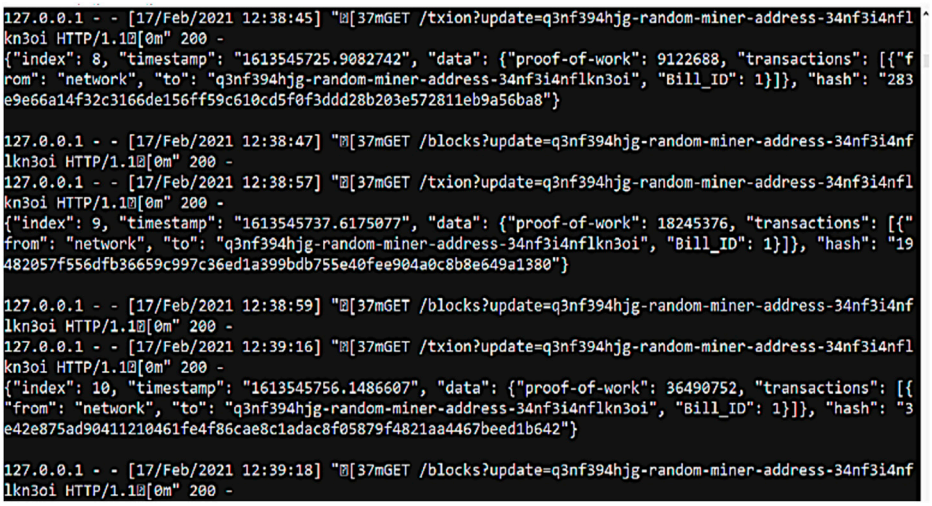


FIGURE 12 | Generating blocks.

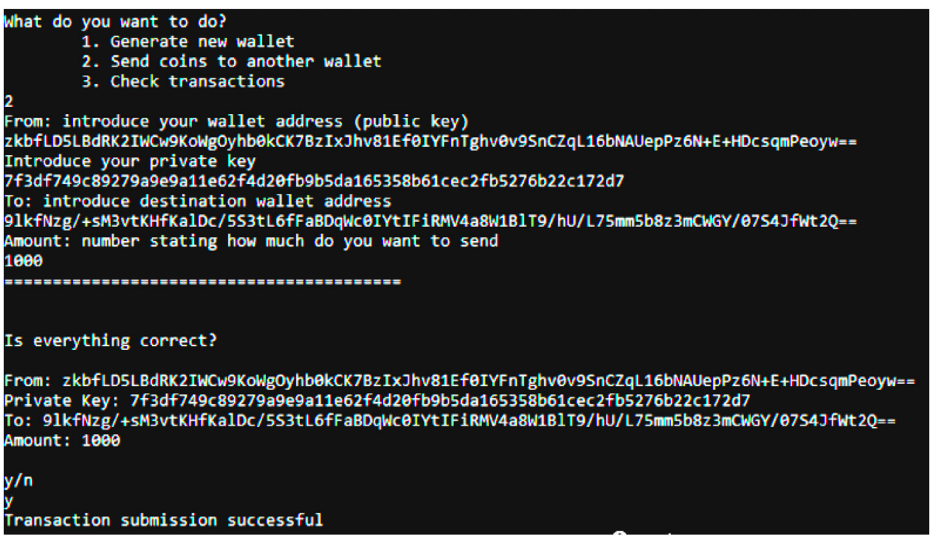


FIGURE 13 | Sending coins.

$$i = int\left(Y_0 \ldots Y_{\frac{n}{2}-1}\right)$$
$$j = int\left(Y_{n/2} \ldots Y_n\right)$$

Subsequently, we perform the substitution operation using the advanced encryption standard substitution table. The substitution table consists of 16 rows, namely, $R_0 \ldots R_F$ and 16 columns, namely, $C_0 \ldots C_F$. The row number and column number are fetched from the values of i and j, and the hexadecimal value of the corresponding row and column is stored in Z.

$$Z = S[i][j]$$

After substituting the bits, we perform permutation by considering n as the total number of bits and r as the number of 1s in the total bits. Thereafter, we perform left circular shift nP_r times on the least significant half and right circular shift nP_r times on the most significant half.

$$nP_r = \frac{n!}{(n-r)!}$$
$$\lim_{n\to\infty}\left(Z_0 \ldots Z_{\frac{n}{2}-1}\right) \ll nP_r$$
$$\lim_{n\to\infty}\left(Z_{\frac{n}{2}} \ldots Z_n\right) \gg nP_r$$

After performing circular shift on the bitstream, we swap each bit with the consecutive bit.

$$Q = Swap\left(Z_n, Z_{n+1}\right)$$

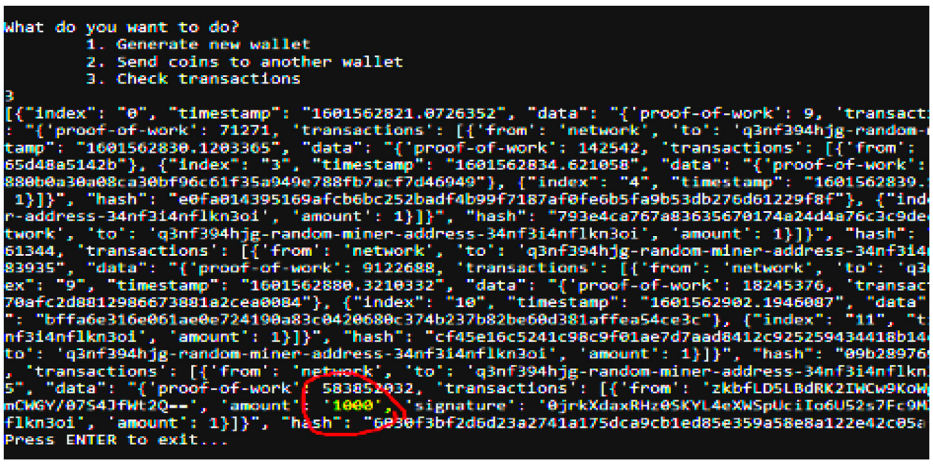


FIGURE 14 | View Transactions.

TABLE 1 | Entropy value comparison.

Image	Original grayscale	Ciphertext	Decrypted
Figure 11A	3.34	7.95	3.35
Figure 11B	3.39	7.92	3.38
Figure 11C	3.30	7.98	3.30

Hashing operation is performed on the resulting block of bits.

$$T = H(Q)$$

The hash value is appended to the swapped bit, resulting in the intermediate ciphertext. Later, the intermediate ciphertext or bitstream is converted to hexadecimal blocks of data. This hexadecimal data is shared over blockchain.

$$I_C = Q + T$$
$$C = hex(I_C)$$

SMART GRID SECULARIZATION

Smart grid simulation is performed using OpenDSS and Anaconda-Jupyter. In OpenDSS, we have taken phase lines and buses to simulate the electric grid. The following lines show the phases, buses, line code, and length of the phase line. The phase line connectivity of the grid is demonstrated in **Figure 3**.

$$New\ Line.L1\ Phases = 3\ Bus1 = 701.1.2.3\ Bus2 = 702.1.2.3\ LineCode = 722\ Length = 0.96$$

$$New\ Line.L2\ Phases = 3\ Bus1 = 703.1.2.3\ Bus2 = 705.1.2.3\ LineCode = 724\ Length = 0.4$$

Here the phases are connected in a delta model of 1 kV, which has a power consumption of 4.800 kW.

$$New\ Load.S701a\ Bus1 = 701.1.2\ Phases = 1\ Conn = Delta\ Model = 1kV = 4.800\ kW$$
$$New\ Load.S701a\ Delta\ Model = 140.0\ kV\ AR = 70.0$$
$$New\ Load.S701b\ Bus1 = 701.2.3\ Phases = 1\ Conn = Delta\ Model = 1kV = 4.800\ kW$$
$$New\ Load.S701b\ Delta\ Model = 350.0\ kV\ AR = 175.0$$

Selecting a particular phase line is highlighted in **Figure 4**.

Figure 5 demonstrates a potential difference or voltage difference between the two nodes of a particular phase line.

Figure 6 demonstrates the current flowing between the two nodes of a particular phase line.

Figure 7 demonstrates power consumption between the two nodes of a particular phase line.

Figure 8–10 show the overall phase current, voltage, and power flow of pseudorandom lines.

The first 3D graph (**Figure 11A**) is of power, voltage, and current. The second graph is of power factor, frequency, and energy. The third graph is of energy, current, and time. Time taken was from 6 to 18 months. The figure shows the encryption results of the consumption data. The graphs are generated using Numpy and Matplotlib in Python, Jupyter-Anaconda. The encryption is also performed using Python in Jupyter-Anaconda.

As demonstrated in **Figure 11**, plaintext and key sensitivity are checked to predict the diffusion and confusion in the ciphertext as compared to the plaintext. We can observe that almost 90% of the plaintext is jumbled, denoting high diffusion and confusion. Therefore, the security provided is of acceptable range. After calculating the power consumption, we created our blockchain cryptocurrency wallet in Anaconda-Python for electricity bill payment. The upcoming screencaps show transactions of bill amounts on blockchain. The sender uses his public–private key pair to send the money to the wallet of the receiver's. Implementation is done using Python in Jupyter-Anaconda.

TABLE 2 | Security model.

Security model: Standard model			
Algorithm	**Key size (bits)**	**Signature size (bits)**	**Complexity**
PQB	256	256	$O(N^2.log(N))$
QKD	256	256	$O(N.log(N))+O(N^2.log(1/N))$
QC	256	256	$O(log(N))+O(N^2)$

TABLE 3 | Avalanche effect.

Algorithm	Bits change	Sensitivity%
PQB	232/256	90.6251
QKD	195/256	76.1718
QC	139/256	54.2968

The following image (**Figure 12**) demonstrates that our blockchain is up and online and the blocks are getting generated.

We are generating wallets by providing our ID. The ID is used to compute private and public addresses which are then stored in .txt format. After that, we perform the transaction using coins. Both the public key and private key of the sender are used for debiting the coins from the wallet of the sender. The public key of the receiver is needed to credit the amount in their wallet. The following screenshot (**Figure 13**) demonstrates the transaction for bill payment.

After the payment is completed, we check the transactions to see if the coin has been successfully credited to the wallet of the receiver. The following figure (**Figure 14**) highlights the accomplished transaction.

RESULTS

Information entropy has a magnitude in the range (0 1). When the metadata entropy of a system is 1, it suggests that the system has no predictability at all. When the information entropy is zero, the system is free of unpredictability and imperfection. The valuation of information entropy can be exploited to represent the outcome of plaintext and ciphertext exclusivity. The higher the evidence entropy, the more secure the data (Banerjee and Patel, 2016). Following is the mechanism for predicting information entropy:

$$H(s) = \sum_{i=0}^{2^{N-1}} p(s_i) log_2 p(s_i)$$

When there is no pixel association, the entropy is 8 because each pixel has 24 potential values. However, because the digital image cannot be fully random, the actual information entropy is less than 8. The information entropy of photographs depicting data is usually between 3 and 4. The information entropy of the above-mentioned 3D graphical picture (**Figure 10**) is determined. **Table 1** shows the entropy values of the original grayscale image, ciphertext, and decrypted image.

It has been observed in the image that the entropy of the grayscale and decryption figures before encryption is about 3.3, indicating that there is a strong correlation between the various elements of the graph, but the information entropy of the ciphertext is very close to the extreme value of 8, indicating that the encrypted images are close to random distribution, and the security is higher, hence assuring the security of the proposed double-crossover scheme.

The implementation of the two algorithms is performed in Python, Anaconda Jupyter Notebook. Time complexity and avalanche effect are noted. PQB is post-quantum blockchain, which is our work. QKD is quantum key distribution approach of Yin et al. (2020), and QC is quantum cryptography approach of DayoAlowolodu et al. (2018).

Another parameter selected for performance measurement is complexity of block addition and encryption. Blockchain is simulated using Hyperledger fabric in ubuntu. The results achieved are as follows: PQB is our approach, whereas QKD (Yin et al., 2020) and QC (DayoAlowolodu et al., 2018) are existing approaches (**Table 2**).

The third parameter is avalanche effect (**Table 3**). It is a measure of sensitivity or bit flip ratio. Whenever we changed one bit of the plaintext, almost 90% of bits changed. This ensures high sensitivity. This means that, even if we change just one bit of the plaintext, the entire ciphertext changes. It becomes almost impossible for the attacker or intruder to find a pattern between different ciphertexts.

The results clearly show that the proposed approach provides appropriate sensitivity in polynomial time in the given context. Hence, we can assume that, for the given dataset, the asymmetric approach performs quite well.

CONCLUSION

Smart grids are necessary to restrict the carbon footprint in the coming years. However, implementing smart grids leaves the privacy of the consumers at the mercy of attackers. Hence, the secularization of the smart grid against several attacks is the need of the era. Our security framework embedded with blockchain does the task in the given context. We encrypt the consumer data and the consumption data using our approach. The strength analysis is done using the statistical plaintext sensitivity test and key sensitivity test. Almost 90% avalanche effect is observed in the generated ciphertext. Therefore, it is concluded that the permutation–substitution-based blockchain embedded public key cryptographic approach in Galois Field is providing the

necessary security in the smart grids against attacks for the tested set of data.

DATA AVAILABILITY STATEMENT

Publicly available datasets were analyzed in this study. This data can be found here: (Smart Energy Informatics, 2018) Smart Energy Informatics Lab—http://seil.cse.iitb.ac.in/residential-dataset.

AUTHOR CONTRIBUTIONS

All authors listed have made a substantial, direct, and intellectual contribution to the work and approved it for publication.

REFERENCES

Adkins, E., Eapen, S., Kaluwile, F., Nair, G., and Modi, V. (2010). Off-grid Energy Services for the Poor: Introducing LED Lighting in the Millennium Villages Project in Malawi. *Energy Policy* 38 (2), 1087–1097. doi:10.1016/j.enpol.2009.10.061

Agung, A. A. G., and Handayani, R. (2020). Blockchain for Smart Grid. *J. King Saud Univ. - Comp. Inf. Sci.* doi:10.1016/j.jksuci.2020.01.002

Aklin, M., Bayer, P., Harish, S. P., and Urpelainen, J. (2017). Does Basic Energy Access Generate Socioeconomic Benefits? A Field experiment with Off-Grid Solar Power in India. *Sci. Adv.* 3 (5), e1602153. doi:10.1126/sciadv.1602153

Allcott, H., and Rogers, T. (2014). The Short-Run and Long-Run Effects of Behavioral Interventions: Experimental Evidence from Energy Conservation. *Am. Econ. Rev.* 104 (10), 3003–3037. doi:10.1257/aer.104.10.3003

Banerjee, B. (2019). Avalanche Effect: A Judgement Parameter of Strength in Symmetric Key Block Ciphers. *Int. J. Eng. Dev. Res.* 7 (2), 116–121.

Banerjee, B., Jani, A., and Shah, N. (2020). Post Quantum Security Enhancement Scheme in IoT Blockchain Framework. *GIS Sci. J.* 7 (6), 664–672.

Banerjee, B., Jani, A., and Shah, N. (2021). Traditional and Quantum Approaches against Shor's Algorithm: A Review. *Int. J. Res. Publ. Rev.* 2 (2), 6.

Banerjee, B., and Patel, J. (2016). A Symmetric Key Block Cipher to Provide Confidentiality in Wireless Sensor Networks. *INFOCOMP J. Comp. Sci.* 15 (1), 12–18.

Biermann, A. (2003). Distributed Generation: Institutional Change in the UK2000~2003[J]. *Proceedings of Summer Study*. Berlin, Germany: European Council.

Cui, Z., Xue, F., Zhang, S., Cai, X., Cao, Y., Zhang, w., et al. (2020). A Hybrid Blockchain-Based Identity Authentication Scheme for Multi-WSN. *IEEE Trans. Serv. Comput.* 13 (2), 241–251. doi:10.1109/tsc.2020.2964537

Dayo Alowolodu, O., K Adelaja, G., K Alese, B., and Catherine Olayemi, O. (2018). Medical Image Security Using Quantum Cryptography. *Iisit* 15, 057–067. doi:10.28945/4008

Dong, Z., Zhao, J., and WenXue, Y. (2014). From Smart Grid to Energy Internet: Basic Concept and Research Framework. *Automation electric Power Syst.* 38 (15), 1–11.

Greenstone, M., Reguant, M., Ryan, N., and Dobermann, T. (2019). *Energy and Environment*. Aukland, New Zealand: International Growth Centre.

Hassan, M., Rehmani, M., and Chen, J. (2021). *Optimizing Blockchain Based Smart Grid Auctions: A Green Revolution*. Boston, MA: arXiv - CS - Cryptography and Security. arxiv-2102.02583.

Johnson, R., and Zhang, T. (2013). "Accelerating Stochastic Gradient Descent Using Predictive Variance Reduction, NIPS'13," in Proceedings of the 26th International Conference on Neural Information Processing Systems - Volume 1, 315–323. doi:10.5555/2999611.2999647

Kabalci, Y., Kabalci, E., Padmanaban, S., Holm-Nielsen, J. B., and Blaabjerg, F. (2019). Internet of Things Applications as Energy Internet in Smart Grids and Smart Environments. *Electronics* 8 (9), 972. doi:10.3390/electronics8090972

Kai, X., Qi, L., Zhong, Z., and Keng, Y. (2008). The Vision of Future Smart Grid[J]. *Electric Power* 06, 19–22.

Kunmin, Z., Jiahua, P., and Dapeng, C. (2008). *Study on Low-Carbon Economy*. China: China Environmental Science Press.

Liwen, F., Huiru, Z., and Sen, G. (2012). An Analysis on the Low-Carbon Benefits of Smart Grid of China. *Phys. Proced.* 24, 328–336. doi:10.1016/j.phpro.2012.02.049

Mahdavi, M., Yang, T., Jin, R., Zhu, S., and Yi, J. (2012). Stochastic Gradient Descent with Only One Projection. *Adv. Neural Inf. Process. Syst.* 25 (NIPS 2012).

Shafie-khah, M. (2020). *Blockchain-based Smart Grids*. London: Academic Press.

Sikeridis, D., Bidram, A., Devetsikiotis, M., and Reno, M. J. (20202020). "A Blockchain-Based Mechanism for Secure Data Exchange in Smart Grid protection Systems," in IEEE 17th Annual Consumer Communications & Networking Conference (CCNC) (NV, USA: Las Vegas), 1–6. doi:10.1109/CCNC46108.2020.9045368

Smart Energy Informatics Lab (2018). Available at: http://seil.cse.iitb.ac.in/residential-dataset.

Vishwakarma, L., and Das, D., (2020), Science and Education MagazineTechScape: IIT Jodhpur, Vol. 01, Issue 02, 2020.

Yin, J., Li, Y.-H., Liao, S.-K., Yang, M., Cao, Y., Zhang, L., et al. (20202020). Entanglement-based Secure Quantum Cryptography over 1,120 Kilometres. *Nature* 582, 501–505. doi:10.1038/s41586-020-2401-y

Zhaofeng, M., Xiaochang, W., Jain, D. K., Khan, H., Hongmin, G., and Zhen, W. (2020). A Blockchain-Based Trusted Data Management Scheme in Edge Computing. *IEEE Trans. Ind. Inf.* 16 (3), 2013–2021. doi:10.1109/tii.2019.2933482

Zoican, S., Vochin, M., Zoican, R., and Galatchi, D. (2018). in Blockchain and consensus algorithms in internet of things, 2018 International Symposium on Electronics and Telecommunications (ISETC 2018) (Timisoara), 1–4.

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Copyright © 2021 Banerjee, Jani and Shah. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.