International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-10 Issue-5, June 2021

A Review on Secure Data Transmission for Banking Application using Machine Learning

Gurram Bhaskar, Motati Dinesh Reddy, Thatikonda Mounika

Abstract: ***Security on the Internet of Things (IoT) accentuates safeguarding the Internet-empowered devices that connect to remote networks. IoT Safety endeavors to shield IoT gadgets and frameworks against cybercrime, and it is considered a vital security element linked to the IoT. Conversely, banking applications are dynamically being regulated for their inability to give an adequate level of client assistance and insure themselves against and react to digital assaults. One of the primary components for this is the weakness of Fintech systems and organizations to breaking down. Therefore, wireless organizations covering these IoT items are incredibly unprotected. IoT is a lightweight framework, and it is ideal when utilizing lightweight and energy-effective cryptography for assurance. Deep learning is a proficient technique to examine dangers and react to assaults and security occurrences. So this business locales both security and energy productivity in IoT utilizing two novel strategies helped out through the deep learning. This work adds to the most inventive method of saving energy in IoT gadgets through diminishing the utilization of energy-costly '1' values in the interface of Dynamic RAM. This should be possible by utilizing Base + XOR encoding of information during information transmission. Utilizing Conditional Generative Adversarial Network (CGAN) based deep learning strategy, the Base + XOR encoding technique and C.X.E. are prepared or trained quite well in the banking/financial application. The information age in CGAN is done dependent on rules delivered utilizing the generator model. This work is ended up being burning-through less energy, less information transmission time, and gives greater security when thought about the existing frameworks.***

Keywords: Machine Learning (ML), Artificial Intelligence (A.I.), IoT, Data, Security, Banking

I. INTRODUCTION

In the current unprecedented times, digital transformation is very crucial. One of the critical difficulties is modernizing banks and inheritance business frameworks without disturbing the existing framework.

Manuscript received on June 01, 2021.
Revised Manuscript received on June 08, 2021.
Manuscript published on June 30, 2021.

***** Correspondence Author

Gurram Bhaskar*, Pursuing, Bachelor of Technology in Computer Science Engineering, SRM Institute of Science and Technology, Chennai (Tamil Nadu), India. Email: bhaskar.gurram2017@gmail.com

Motati Dinesh Reddy, Pursuing, Bachelor of Technology in Computer Science Engineering, SRM Institute of Science and Technology, Chennai (Tamil Nadu), India. Email: motatidineshreddy663@gmail.com

Thatikonda Mounika, Pursuing, Bachelor of Technology in Information Technology, Mallareddy College of Engineering and Technology, Hyderabad (Telangana), India. Email: mounikathatikonda77@gmail.com

ML and A.I. drove the way to deal with banking framework modernization and will empower organizations to connect with other Fintech administrations into accepting current customers' requests and guidelines while guaranteeing wellbeing and empowering security. In the financial business, with the developing pressure in overseeing risks alongside expanding administration and administrative necessities, banks should improve their administrations towards more unique and better client support. Fintech brands are progressively applying A.I. and ML in a broad scope of uses across a few channels to use all the accessible customer information to foresee how clients' prerequisites are developing. Furthermore, they are additionally hypothesizing what administrations will demonstrate gainful for them, what sort of false action has the most elevated chance to assault clients' frameworks.

IoT environment has re-imagined the term "network or connectivity", with novel standards like smart houses, clever towns, etc., and prompting up to this point concealed human-machine co-operations. Nonetheless, IoT sellers appear to relegate higher need to fast prototyping and deployment, which regularly prompts the creation of gadgets with different security vulnerabilities. Ramalingam and Venkatesan described banking as one of the critical spaces that can use IoT innovation's brilliant possibilities. As of now, Automated Teller Machine (A.T.M.), mobile banking and the Point of Service (P.O.S.) terminal has become the edge of the banking foundation. Banking IoT faces a number of difficulties, similar to information thickness and protection, security just as the need to protect client information. This work tackles the issue of information security through CGAN.

The Generative Adversarial Network (GAN) is by all accounts a deep learning, uncontrolled A.I. method. In this strategy, new information alongside the same insights that acts as a preparation set was produced through education if the preparation set was given. Generator-The Discriminator Model is a multi-facet perceptron (M.L.P.). The motivation behind the generator is to display or deliver information that is exceptionally near preparing the report. For circulation learning, GAN turns into another class of generative techniques. In this work, the GAN is acquainted with the information transmission measure alongside assurance, and furthermore, it identifies an assault during transmission; here, in the middle of the generator, G, and the Discriminator, D, min-max two player's game is presented. The discriminator additions information about the contrasts between the delivered information by genuine informational collection and created statement by the generator.

The generator also acquires information about making mistakes while making tests in prejudicial networks. In this work, the restrictive GAN configuration changes the molding data, m, into the generator (G) just as the Discriminator (D) as extra info. This work utilized two sorts of molding data which are included both generator and Discriminator. BASE + XOR is one of the encoding systems. It is acted as the generator of the proposed work, and it devours less energy during information transmission. By executing an essential XOR esteem activity inside an exchange, the Encoding of comparable information components is done through the Base +XOR encoding. C.X.E. is another sort of encoding component which encodes the information from BASE + XOR encoded result. It performs more grounded and quicker encryption utilizing XOR activity.

II. LITERATURE REVIEW

Farooq et al. proposed the two Generative Adversarial Network (GAN) based models to recognize dangers in IoT gadgets from the inside and outside the organization. They additionally broke down a utilization case for network work virtualization for widget the board once a malignant device has been distinguished on the organization. Their GAN based model planned the dormant space of appropriate dataset of IoT gadgets and hailed malevolent widgets found going amiss from their norm. Hao et al introduced a remote start to finish specialized method with the assistance of Deep Neural Networks (D.N.N.s). Following this, Conditional Generative Adversarial Network (GAN) was applied to address channel impacts. The molding data was acted by transmitter's sign which is encoded. Secure Wireless Sensor Network Middleware (SWSNM) was talked about by Remah et al and it is reliant upon the generative ill-disposed organization calculation which is a solo learning technique. This proposed network contains two sections: generator (G) and a discriminator (D). To confound aggressors and to shield information, the information was made counterfeit like unique information. This two information can be recognized utilizing D which have numerous layers. Zhaoqing et al discussed about most recent improvement of GANs. To start with, the examination of essential hypothesis of GANs and varieties among different generative models was completed. Following this, the order was completed in inferred models of GANs. The preparation stunts and assessment measurements were given, and execution was improved through point-by-point portrayal about GANs application. Xiaopu et al proposed a compelling seismic information obtaining technique. This strategy contains a Compressed Sensing Architecture in Generative Adversarial Network (CSA-GAN). This technique was proposed to beat colossal scale seismic information assortment issue. To diminish traffic just as to adjust the information transmission, packed detecting hypothesis was utilized, which depends on information assortment architecture. Decheng et al. named a novel methodology of bend reproduction through a contingent generative ill-disposed organization (GAN), CR-CGAN, and it was introduced to blend transmission line Galloping bends. By applying additional imperatives to achieve the total recreation of the running bends, they utilized the demonstrating abilities of the recently added GAN just as presented another arrangement in the generator-discriminator pair for acquiring great outcomes and likewise another refined misfortune capacity to enhance the information.

Zahangir et al. contemplated the advancement of the Convolution Neural Network (CNN), Deep Neural Network (D.N.N.), Recurrent Neural Network (R.N.N.), containing Long Short-Term Memory (LSTM) and Auto-Encoder (A.E.), Deep Belief Network (DBN), Generative Adversarial Network (GAN), Gated Recurrent Units (G.R.U.), and Deep Reinforcement Learning (DRL) in the field of Deep Learning (DL). Therefore, extraordinary headway has been tended to, as the latest variant DL methods rely on the DL method.

Akshay et al recommended an organization configuration propelled through profound remaining organizations, which allow a more expressive pairwise similarity focus to be figured proficiently. They likewise expressed that regularization is the key to learning with limited quantities of data and recommended an additional generator approach that depends on the Generative Adversarial Networks, whereby their lingering pairwise organization is by all accounts the Discriminator. Elhoseny and Hassanien presented another technique in W.S.N. named secure information preparing and transmission scheme. The most well-known safe grouping based steering calculations that have been made for W.S.N.s were considered and widely tended to. The directions and steps to make a legitimate answer for ensuring the intricate group network were n explained while utilizing less energy probably and acclimating to have less figuring power. Also, it proposed to build a W.S.N. stable grouping approach. Mohammed et al. suggested a new profound learning-centered data minimization calculation which 1) diminishes informational indexes while transmission through carrier channels; 2) forestalls man-in-the-center (MITM) information just as different assaults through altering the parallel portrayal over the equivalent dataset on numerous occasions: allocating different code words to a similar character in different portions of the dataset.

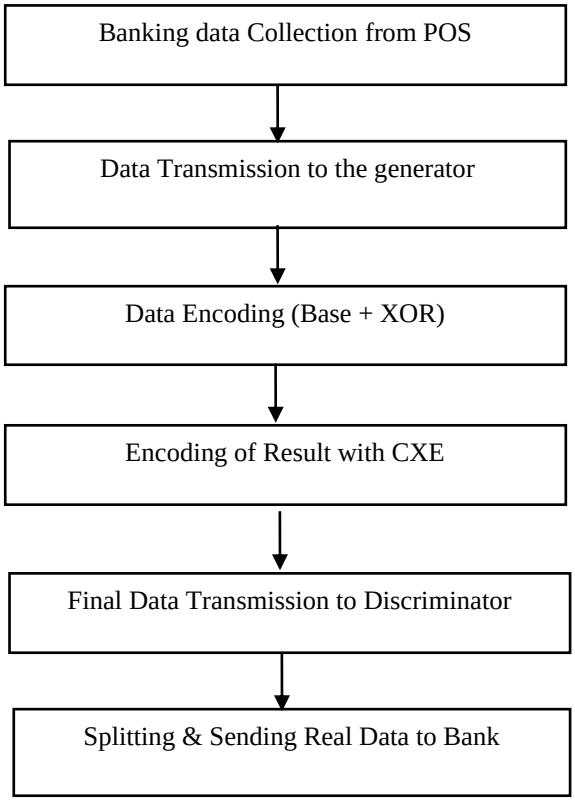
Bhavnesh et al. expressed the adequacy of error control codes just as various regulation systems for W.S.N. The investigation shows that a right option of tweak situation just as blunder control codes will limit the energy utilization in the W.S.N. While utilizing Forward Error Correction code termed Raptor codes, Bhanupriya et al introduced an energy-productive information transmission technique in the Binary Erasure Channel situation. Then changes are made in precoder and came about raptor codes was analyzed in parts of energy. Donghyuk et al examined about information move framework utilizing negligible energy dependent on Base and XOR strategy. Through conveying out XOR tasks among information components inside a one DRAM arrangement, the information like segment was moved. They handled two issues influencing the viability of their system which incorporates, I) the incessant presence in exchanges containing zero information components, (ii) the variety within an exchange utilizing the basic scope of information types. Two strategies like Zero Data Remapping just as Universal Base +XOR Transfer, were defined.

Ankur et al built up a new fast Encryption technique for delivering alternate code texts. The proposed cryptanalysis work outlined the security just as strength of keys and algorithm. The viability of the encryption scheme was dependent on the keys check that use the turbulent capacity produced.

Bassem et al presented another just as rapid encryption conspire named tumultuous encryption calculation RFCA. The proposed work involves turbulent code which comprises of two irritated guides piecewise straight tumultuous guide. In explicit, this calculation was adequate for encoding information in ZigBee networks whereby it requires vigor and continuous.

III. METHODOLOGY

The basic flowchart for working of the system has been shown in figure 1: The basic flowchart for working of the system has been shown in figure 1:



IV. CONDITIONAL GAN ARCHITECTURE

The conditional GAN architecture has been shown in figure 2. Initially, the banking data will be gathered from the P.O.S., which will be further transmitted to the generator. After this, the Encoding of data takes place, which is usually done using Exclusive OR operation. After encoding, the result is again encoded with C.X.E. and finally the data is transmitted to the Discriminator. After this the data is spitted and the actual data is sent to the bank, and fake data is sent to the intruder.

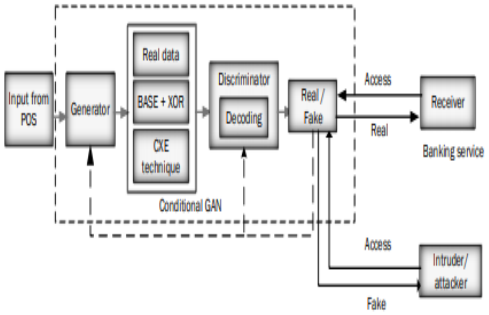


Figure 2: Conditional GAN Architecture

V. RESULTS & DISCUSSION

Mainly three parameters have been considered, i.e., data transmission time, the average consumption of energy and throughput.

Table 1: Data Transmission Time Vs Dataset for Base+ XOR and One hot Encoding

Dataset	Data Transmission Time (in Milliseconds)	
	Base +XOR	One hot Encoding
1 GB	0.3	0.9
3 GB	1.1	1.9
8 GB	1.9	2.8
13 GB	2.7	3.9
18 GB	3.5	4.2

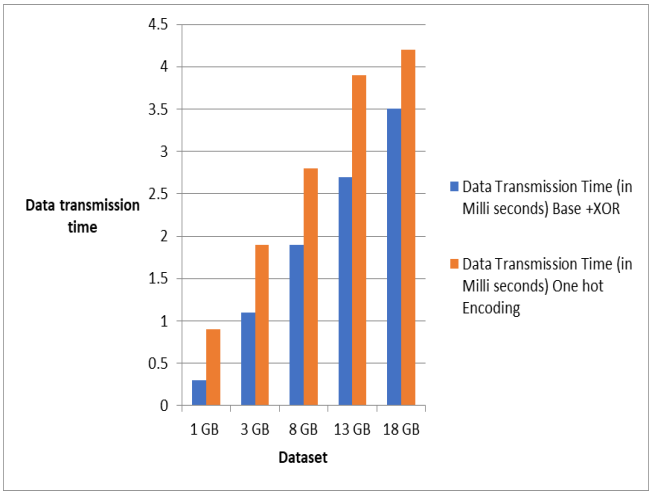


Figure 3: Data Transmission time comparison for two different techniques

Table 2: Average Energy Consumption Vs No. of Nodes for GAN & binary Encoding

No. of Nodes	Average Energy Consumption	
	GAN	Binary Encoding
10	0.2	0.9
25	1.3	1.8
40	2.5	3.2
55	3.4	4.2
70	4.2	4.9

Retrieval Number: 100.1/ijeat.E27460610521
DOI:10.35940/ijeat.E2746.0610521
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication

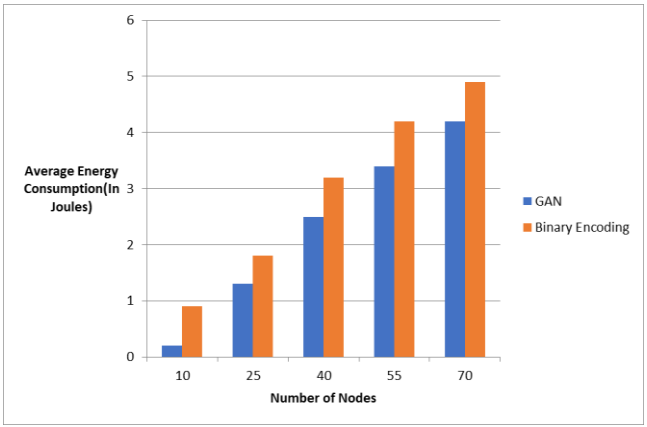


Figure 4: Average energy comparison for two different techniques

Table 3: Throughput Vs Dataset for CGAN & CNN

Dataset	Throughput (Kb/sec)	
	CGAN	CNN
1 GB	100	60
3 GB	170	120
8 GB	220	160
13 GB	320	250
18 GB	390	310

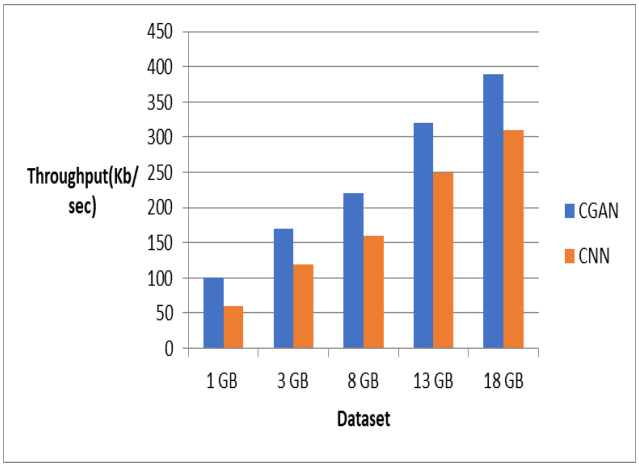


Figure 5: Throughput comparison for two different techniques

VI. CONCLUSION

From figures 3, it can be concluded that the data transmission time for the BASE+XOR technique is relatively lower as compared to the one-hot encoding technique. The dataset kept remained the same for both methods. From figures 4, it can be concluded that the average energy consumption in GAN is relatively low as compared to the binary encoding technique. Also, from figure 5, it can be revealed that the throughput for CGAN is higher than the CNN technique.

APPENDIX

It is optional. Appendixes, if needed, appear before the acknowledgement.

ACKNOWLEDGMENT

It is optional. The preferred spelling of the word "acknowledgement" in American English is without an "e" after the "g." Use the singular heading even if you have many acknowledgements. Avoid expressions such as "One of us (S.B.A.) would like to thank ... ." Instead, write "F. A. Author thanks" *Sponsor and financial support acknowledgements are placed in the unnumbered footnote on the first page.*

REFERENCES

1. Bhanupriya, Shereen, Sylvia Blossom & Malathy.: Energy efficient wireless Sensor networks using raptor codes: International Journal of Advanced Research in Electronics and Communication Engineering, 2017.
2. Donghyuk Lee, Mike O'Connor & Niladrish Chatterjee.: Reducing Data Transfer Energy by Exploiting Similarity within a Data Transaction: IEEE conference, 2018.
3. Ankur Khare Piyush, Kumar Shukla, Murtaza Abbas Rizvi and Shalini Stalin.: An Intelligent and Fast Chaotic Encryption Using Digital Logic Circuits for Ad-Hoc and Ubiquitous Computing: MDPI, vol.18.
4. Bassem Bakhache, Joseph M. Ghazal, and Safwan El Assad.: Improvement of the Security of ZigBee by a New Chaotic Algorithm: IEEE, 2013.
5. Ramalingam and V. P. Venkatesan.: Conceptual analysis of Internet of Things use cases in banking domain: TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), 2019, pp. 2034-2039.
6. Farooq Shaikh and Elias Bou-Harb.: IoT Threat Detection Leveraging Network Statistics and GAN: 2019.
7. Hao Ye, Geoffrey Ye Li, and Ling-Hwang Fred Juang.: Channel Agnostic End-to-End Learning-based Communication Systems with Conditional GAN: IEEE Globecom Workshops (GC Wkshps), 2018.
8. Remah a. Alshinina & khaled m. elleithy.: A Highly Accurate Deep Learning Based Approach for Developing Wireless Sensor Network Middleware: IEEE.
9. Zhaoqing Pan, Weijie Yu, Xiaokai Yi, Asifullah Khan, Feng Yuan, and Yuhui Zheng. : Recent Progress on Generative Adversarial Networks (GANs): A Survey: IEEE Access, 2019, Vol.7.
10. Xiaopu Zhang, Shuai Zhan, Jun Lin, Feng Sun, Xi Zhu, Yang Yang, Xunqian Tong, And Hongyuan Yang. : An Efficient Seismic Data Acquisition Based on Compressed Sensing Architecture with Generative Adversarial Networks: IEEE access, 2019, Vol. 7.
11. Decheng Wu, Hailin Cao, Dian Li, And Shizhong Yang.: Energy-Efficient Reconstruction Method for Transmission Lines Galloping With Conditional Generative Adversarial Network: 2020, Vol.8.
12. Md Zahangir Alom, Tarek M. Taha , Chris Yakopcic , Stefan Westberg , Paheding Sidike , Mst Shamima Nasrin , Mahmudul Hasan , Brian C. Van Essen , Abdul A. S. Awwal and Vijayan K. Asari.: A State-of-the-Art Survey on Deep Learning Theory and Architectures: MDPI, 2019.
13. Akshay Mehrotra and Ambedkar Dukkipati.: Generative Adversarial Residual Pairwise Networks for One Shot Learning: Computer Vision and Pattern Recognition, 2017.
14. M. Elhoseny & A. E. Hassanien.: secured data transmission in WSN: an overview: springer, 2019.
15. Bhavnesh Jaint, S.Indu & Neeta Pandey.: Energy Efficient Communication Techniques for Wireless Sensor Networks: International Journal of Innovative Technology and Exploring Engineering, 2019.

AUTHORS PROFILE

Gurram Bhaskar, is an aspiring data scientist who enjoys connecting the dots be it ideas from different disciplines, people from different teams, or applications from different industries. He is currently pursuing his Bachelor of Technology in Computer Science Engineering from SRM Institute of Science and Technology. He has strong technical skills and an academic background in engineering, statistics, and machine learning. Email: bhaskar.gurram2017@gmail.com

Motati Dinesh Reddy, is an aspiring learner. He has good knowledge of Data Science and Machine Learning with a strong inclination towards problem-solving and propelling data-driven decisions. He is currently pursuing his Bachelor of Technology in Computer Science Engineering from SRM Institute of Science and Technology. He has worked on multiple projects related to problem solving and Data science in his college. Academics. His field of research is machine learning and data science. Email: motatidineshreddy663@gmail.com

Thatikonda Mounika, an inquisitive technology enthusiast interested in data science ,Machine learning & a pragmatic learner who wants to implement new things .She is currently pursuing her Bachelor of Technology in Information Technology from Mallareddy College of Engineering and Technology. She has got great technical skills and academic excellence . Also , worked on multiple projects related to data science. Email: mounikathatikonda77@gmail.com