International Journal of Communication Networks and Information Security
ISSN: 2073-607X, 2076-0930
Volume 14 Issue 03 Year 2022 Page 110:122

Intelligent Mobile Edge Computing Integrated with Blockchain Security Analysis for Millimetre-Wave Communication

Priyadarsini K
Department of Data Science and Business Systems, School of Computing, College of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur, Chennai- 603203, Tamil Nadu, India
priyadak@srmist.edu.in
Sri Lakshmi Chandana
Assistant Professor, Department of Electronics and Communication Engineering, Prasad V Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada, Andhra Pradesh, India
chsrilakshmi@pvpsiddhartha.ac.in
Severo Simeón Calderón Samaniego
Professor, Universidad Peruana los Andes, Perú, South America
d.scalderon@upla.edu.pe
Dr. Megha Gupta Chaudhary
Assistant Professor, Department of Physics, SRM Institute of Science and Technology NCR Campus, Delhi-NCR Campus, Ghaziabad, Uttar Pradesh, India
tomeghag@gmail.com
Dr. Vipul Vekariya
Dean and Principal, Faculty of Engineering & Technology, Parul University, Vadodara, Gujarat, India
piet@paruluniversity.ac.in
Mr. Abhay Chaturvedi
Associate Professor, Department of Electronics and Communication Engineering, GLA University, Mathura, Uttar Pradesh- 281406, India
abhaychat@gmail.com

Article History

Received: 11 August 2022
Revised: 22 October 2022
Accepted: 10 November 2022

Abstract

With the increase in number of devices enabled the Internet of Things (IoT) communication with the centralized cloud computing model. With the implementation of the cloud computing model leads to increased Quality of Service (QoS). The cloud computing model provides the edge computing technologies for the real-time application to achieve reliability and security. Edge computing is considered the extension of the cloud computing technology involved in transfer of the sensitive information in the cloud edge to increase the network security. The real-time data transmission realizes the interaction with the high frequency to derive improved network security. However, with edge computing server security is considered as sensitive privacy information maintenance. The information generated from the IoT devices are separated based on stored edge servers based on the service location. Edge computing data is separated based in edge servers for the guaranteed data integrity for the data loss and storage. Blockchain technologies are subjected to different security problem for the data integrity

through integrated blockchain technologies. This paper developed a Voted Blockchain Elliptical Curve Cryptography (VBECC) model for the millimetre wave application. The examination of the blockchain model is evaluated based on the edge computing architecture. The VBECC model develop an architectural model based Blockchain technology with the voting scheme for the millimetre application. The estimated voting scheme computes the edge computing technologies for the estimation of features through ECC model. The VBECC model computes the security model for the data transmission in the edge computing-based millimetre application. The experimental analysis stated that VBECC model uses the data security model ~8% increased performance than the conventional technique.

Keywords: Elliptical Curve Cryptography, Edge Computing, Blockchain, Voting scheme, Cloud Computing

1. Introduction

Internets of Things have brought connected billion of things to communicate via the internet. The key features of IoT devices are to connect analysis and integrate. Optimization of Technology, improving customer engage, analytics with reducing waste and collecting the enhanced data that is collected are the advantage of IoT. The IoT Security and Privacy, Complexity due to heterogenous environments, Flexibility due to integration, Compliance with regulation is difficulties that IoT faces. The security accompanied with privacy could not be maintained as connected devices was constantly communicating and exchanging information over networks. The users have no control on them once personal data was sent on the network. Sometime these devices we open to Botnets attack, DOS attack, Smurf attack Man-in the-middle attacks, data and identity theft, DOS. There are tailored made tooled to help in the provided IoT security solutions which are currently available or an open source in the market. A prototype model of a Smart Home is developed on which experiments are implemented to test, collect data and breach the edge devices working on the designed proposed system A blockchain is developed and examined on the edge IoT device of the prototype to give an improved security for edge devices of the IoT.

Blockchain model comprises of peer-to-peer communication for the distributed ledger with secure cryptographic scheme those are immutable and updatable through consensus model. The cryptography model uses the ledger with consideration of different location for the failure estimation. The control parameters are distributed based on transaction. New block uses the ledger version for the immutable chain model for the blockchain model. It uses the integrity blockchain model based previous blocks for the new block entities for the ledger.

Cryptography scheme focused on management of private information in the open network for data transmission. The information security model is evaluated based on fields in the network for the processing. However, the cryptography model scheme provides the vast range of services through authentication, integrity, non-repudiation, accessibility, and confidentiality. The edge computing-based model uses the intelligent processing system for the millimetre wave application. The proposed VBECC model uses the blockchain model based on edge computing technology. To improve the security in the millimetre-based edge computing model ECC model is implemented. With the VBECC model voting scheme is implemented over the blockchain model for the processing of the data collected from the millimetre model. The simulation analysis expressed that proposed VBECC model exhibits the improved performance ~8% compared with the conventional technique.

This paper is organized as follows: the related works based on blockchain technology is presented in Section 2. The VBECC model methodology is presented in Section 3 and simulation results are included in Section 4. Finally, the overall conclusion obtained from VBECC model is presented in Section 5.

2. Related Works

In [10] reviewed approximately down the focal homes of deterministic, secluded and restricted of a mind-blowing simultaneousness with the circumstance that have an impact on them and approach to make sure its homes endure. The author depicts Ethereum and their insects withinside the plan which can be associated with quantity goof, language rendition and execution irritates. The EVM bytecode is coordinated earlier than a plan is executed. The Strength language is applied critically anyhow includes insects which the coder will later clean out with time. The author advice that ERC-20 must be satisfactory with a normal define of regulations for Ethereum token. The savvy knowledge assistance is the maintenance of these requirements and reduces sincerity of the insects.

In [11] said that permissionless placing in Blockchain is in which the normally untrusting humans makes a look at an agreement on circumstance of the conveyed and decentralized report. The manufacturer's opinions on picked blockchain degree like Bitcoin, Ethereum and Particle which suggests availability, statistics shape recording and its size. By prudence of Particle logging turns into risky and it's far sincerely reliant facilitator. The author then choices a blockchain primarily based totally Logging blueprint of Name coin, commit coin, Shape and Catena that is portrayed in an actual graph and relies upon instructions of naming, assist, logs, statistics, key straightforwardness. The paper closes with problems of strong timestamps with assist and cryptographic statistics shape for proscribing on chain or off chain statistics correctly with the proof which could verify by purchaser. In this way Blockchain trade version finishes safety and gets entry to control.

In [12] proposed that the File System based on Merkle Tree as a first-rate response for non-public constraint of blockchain that may be confided in a plan thinking about institution primarily based totally community without focal regulator. This is made heads or tails of in the sport plan on a excellent deal of servers with inside the server farm that makes use of a P2P tree-primarily based totally broadcast association and it's far essential contemplated the MTFS shape which applied open bits of get-collectively apparent affirmation publicity of connecting focuses, placing of a hexadecimal hash string for the centre factor ID. The PRE lopsided evaluation accomplishes parent textual content document and a case report that is < 1MB.The manufacturer blanketed every other alternate for coping with record objects „_mt" and root hash data as „_capsule". The enormous philosophy at the purchaser and of the data at the report framework close by replications and tests of the non-public placing away report institutions are on blockchain improvement.

In [13] offered taken into consideration first rate comprehension new traits and conservativeness which permits any purchaser to transport wondering with inside the blockchain cap in a position recreation plan and EVM. Each block of the Ethereum maintain the positive Merkle tree for trade, states, and receipts. The wise comprehension sends as it's far applied on chain A and is redone thinking about the relocation cycle on chain B. The qualification in nation is keep as key or well worth with the important key to stable ultimate greedy nation. The paper combines the deliver code, knowledge and

3. Voted Blockchain Model

The blockchain model comprises of the distributed peer to peer communication in the distributed environment in the Internet network as illustrated in figure 1. The blockchain model VBECC model uses the HTTP, SMTP and TCP/IP scheme at the bottom layer of Internet to offer the effective communication in the network. Conventional peer to peer network uses the Internet topology with the VBECC model comprises of the Blockchain model comprises of the state machine and smart contract.

Within the peer-to-peer communication between nodes the blockchain model uses the validation model to evaluate peer-to-peer connection between nodes. The evaluation is examined with the features in the blockchain features for the secure data communication between nodes.

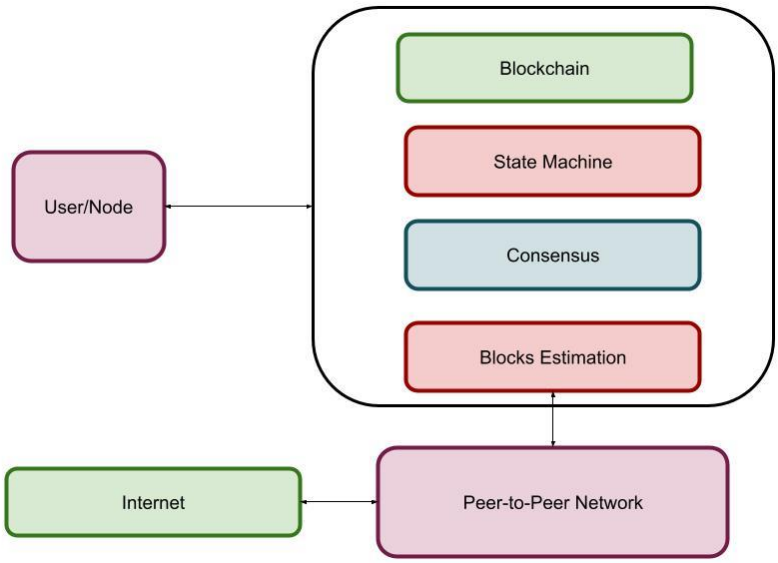


Figure 1. Architecture of VBECC Block chain

. The VBECC model uses the single box features to perform connection between nodes such as transaction, processing, and consensus model.

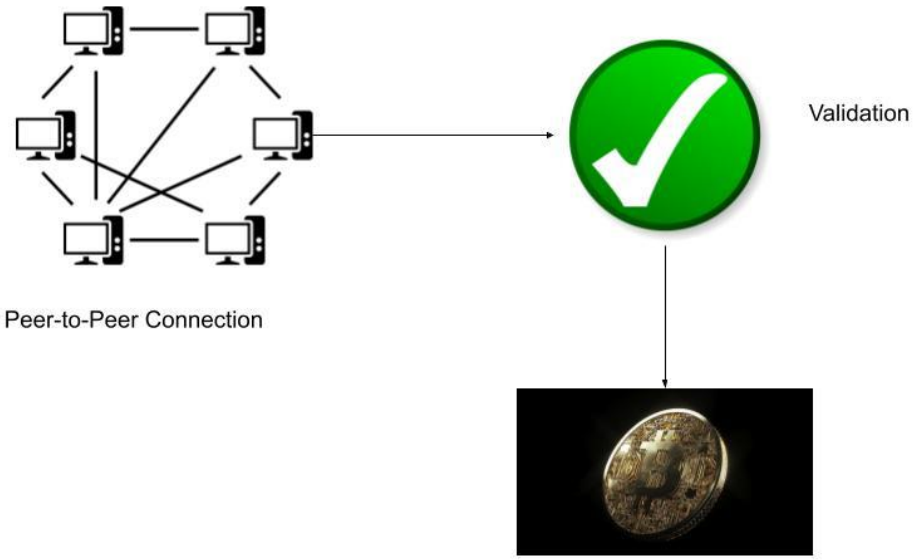


Figure 2. Working of Block chain

3.1 Elliptical Curve Cryptography

Elliptical Curve Cryptography (ECC) is the public key model for the equivalent security examination for the RSA cryptosystem for the small keys. The proposed independent uses the elliptical curve in the finite field GF(p) through the discrete log cryptosystem. The primary factor in the elliptical curve system is management of smaller key, bandwidth, and faster implementation for the security system for the limited integrated circuit with personal computer, wireless devices and smart cards. With the elliptical curve GF(p) the points are set equation $y^2 mod\ P = x^3 + ax + b(mod\ P)$ with the domain paramters such as $D = (p, a, b, G, n)$Where, prime number is represented as >3, the coefficient curve variables are stated as a,b denoted as $4a^3 + 27b^2 \neq 0$, generator base point is stated as G and the point order is represented as n.

Assume the prime number as the p >3 over the elliptical curve value of $y^2 = x^3 + ax + b$ over the solution set of Z_p for the solution $(x, y) \in Z_p$ with the converengence of $y^2 = x^3 + ax + b$ with the define oint P1 and P2 represented as $P3 = P1 + P2$. Addition between point P (xp,yp) and Q(xq,yq) will result to R (xr,yr) if P ≠ - Q, otherwise P + Q = θ where θ is point at infinity R (xr,yr) is defined as:

xr = λ 2 - xp - ; yr = λ ((xp - xr) - yp) where: λ = (3xp2 + a) / 2yp

if P = Q or λ = (yq- yp) / xq - xp) if P ≠ Q

Multiplication between point P and scalar M results to point Q where Q = MP is considered as addition point P, M times. The strength of ECC, relies on the difficulty to find M, for the given Q and P. The private key dB is a random number [1, n-1], while the public key pB = (dB *G). The shared secret key between user Alice and Bob can be computed by multiplying Alice's private key to Bob's public key or Alice's public key multiplies Bob's private key.

3.2 ECC Algorithm for secure data

The ECC model comprises of the coordinates value to estimate the message original value comprises of the number and alphabets. The plaintext point is generated with P_m for the original message M with the mapping function. The plaintext original message is computed with the simple task to withstand the condition as follows:

1. The point in the mapping needs to be estimated in elliptical curve point.
2. However, the mapping function is reversible for the plaintext map in the original messages

Sender Side Mapping

1. The information are arranged with the digits and alphabets through the assigned range of m = 0 to 35
2. The integer value 'a' is evaluated in the sender and receiver set of 'a'
3. Based on each number compute the equation x = m*a + i.
4. With the mapped coordinate (x,y) the value is increased by the value of 1
5. The expected value is estimated as the x = m*a+a-1.

Receiver side (Reverse Mapping) where the value of 'm' is obtained back by calculating (x - 1)/a.

Algorithm 1: VBECC model for data for Intelligent Edge Computing
Choose an elliptic curve which satisfies the equation of the form y 2 mod p = x 3 + ax + b mod p Choose the fixed curve point and form the field of Points called G Key Generation for User A . Select private key dA. Calculate public key PA = dA * G where G is the field containing the EC point Generation of Secret Key KA = dA * PB Key Generation for User B Select private key dB Calculate public key PB = dB * G where G is the field containing the EC Point Generation of Secret Key KB = dB * PA Mapping the message (m) to a plaintext message (Pm) Encryption: Evaluate the plain text such as Pm with the user B with the multiple point of pair with secret key as B's subtracted from the second point C_m= {s_G, P_m + s P_B } Decryption: Decrypt the ciphertext based on first point pait secret key of B subtracted from the second point. P_m + PB – dB (sG) = Pm + s (dBG) – dB(sG) = Pm. Reverse map Pm to get back the message m.

Customizable Blockchain based online voting is developed using the framework shown in Figure 3. To achieve security goals (Confidentiality, Integrity, Availability) the proposed online voting uses ECC Encryption for confidentiality, SHA-256 Hash for integrity and Fingerprint using FCS for authentication. The process architecture model uses the authentication, arbitration agent and blockchain.

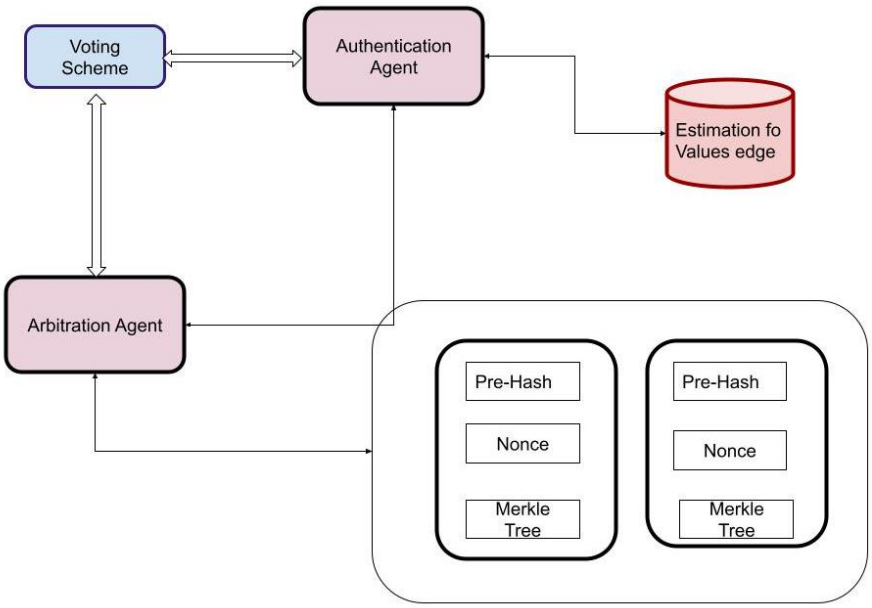


Figure 3. Security Framework for the Block chain Model

Upon the completion of the cryptographic process, to overcome the limitations associated with the conventional DL model a modified approach is presented. The proposed DL model incorporates a Transductive deep model with a hidden Markov process is applied for attack prevention and classification. The constructed VBECC model constructs the Transductive learning for the computation of encrypted and decrypted data. Also, the proposed VBECC uses the CICIDS dataset for the evaluation of attacks in the IoT environment. Those processed data were evaluated with a hidden Markov model for attack detection. The detected attack is computed and processed with the reinforcement learning model. Simulation analysis is performed for the proposed VBECC with conventional ANN and CNN models. The estimation of the observation is defined as t and VBECC is represented as si. It is represented as follows in (1):

$$\delta t(i) = \max_{i=1,\dots N}\left[\delta_t(i)a_{ij}\right]b_j(O_{t+1}) \quad (1)$$

The state sequence of the image argument us maximized with every t and j, the array is denoted asψt(j). The initialization process is presented as follows in equation (2) & (3):

$$\overline{\delta_1(\iota)} = \pi_i b_i(o_1), i = 1,2,\dots\dots, N \quad (2)$$

$$\psi_1(i) = 0 \quad (3)$$

The VBECC in the image is represented as in equ (4) & (5)

$$\delta_t(j) = \max_{j=1\dots N}\left[\hat{\delta}_{t-1}(i)a_{ij}\right]b_j(o_t), t = 2,\dots T, j = 1,\dots N \quad (4)$$

$$\psi_t(f) = \text{argmax}_{j=1-N}\left[\delta_{t-1}(i)a_{ij}\right], t = 2,\dots T, j = 1,\dots N \quad (5)$$

Termination of the MLIC applied over the VBECC as in equation (6) & (7)

$$P^* = \max_{i=1.N}[\delta_T(i)](6)$$

$$q_i^* = \underset{i=1,N}{\operatorname{argmax}}[\delta_T(i)](7)$$

. With the estimated features in the VBECC model the analysis is performed for the data classification between nodes in the Edge Computing network model. The edge computing model based the features are evaluated for the attack prevention and classification with the ECC model features.

4. Results and Discussion

The performance of proposed VBECC is observed that the throughput of the network is significantly improved compared to existing methods. The performance is estimated for 20 - 200 nodes effectively increase the throughput. Overall, the performance of proposed MOA - MAC is effective compared with existing S - MAC protocol. The classification performances of the different classification model are presented in table 1.

Table 1. Comparative Analysis of Classifier

Parameters	**CNN**	**ANN**	**RNN**	**Proposed VBECC**
Accuracy %	97	96	97	98
Precision %	96	95	99	97
Recall %	95	94	93	97
F1 – Score	95	94	96	96

The attack classification performance expressed that the proposed VBECC scheme achieves an accuracy of 98% while CNN, ANN, and RNN exhibit the accuracy of 97%, 96 %, and 97% respectively. This implies that the proposed VBECC scheme exhibits significant performance in attacks classification. Similarly, in the case of recall proposed VBECC achieves a higher % rather than CNN, ANN, and RNN classifiers. The recall of the proposed VBECC is 97% which is approximately 3% higher than the conventional technique CNN, ANN, and RNN classifier.

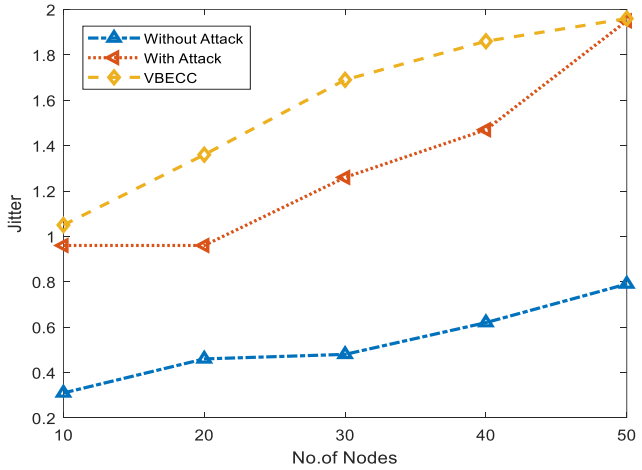
The performance of the proposed VBECC exhibits higher performance in terms of accuracy and recall. In terms of precision proposed VBECC exhibits reduced performance than the RNN classifier. The reduced precision can be due to an increase in the number of hidden layers. Through the estimation of the classifier proposed VBECC for the attack, detection is estimated. With proposed VBECC parameters are computed for varying the environment as normal, with attack and without attack. The estimation is computed for the mobility of 10m/sec. In table 2 performance of the proposed VBECC for with and without attack, scenario is presented.

Table 2. Comparison of Performance

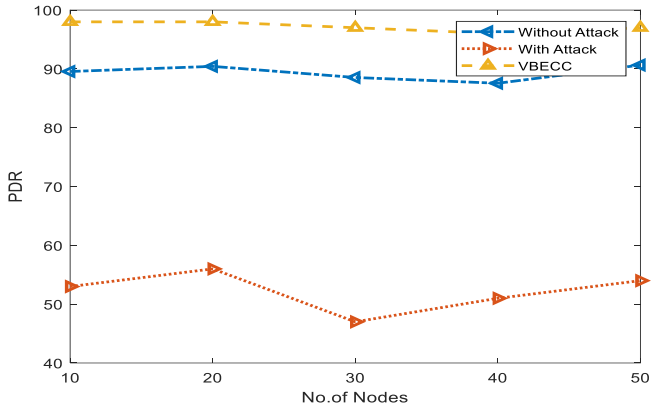
Jitter			
No.of Nodes	Without attack	With attack	VBECC
10	0.31	0.96	1.05
20	0.46	0.96	1.36
30	0.48	1.26	1.69
40	0.62	1.47	1.86
50	0.79	1.95	1.96
PDR			
No.of Nodes	Without attack	With attack	VBECC
10	89.56	53	98
20	90.43	56	98
30	88.54	47	97
40	87.56	51	96
50	90.65	54	97

E2E			
No.of Nodes	Without attack	With attack	VBECC
10	0.63	1.34	0.63
20	0.58	1.53	0.58
30	0.77	1.96	0.77
40	0.73	2.35	0.73
50	0.72	2.06	0.72
Throughput			
No.of Nodes	Without attack	With attack	VBECC
10	93	52	99
20	91	56	98
30	92	44	98
40	93	47	97
50	92	49	98

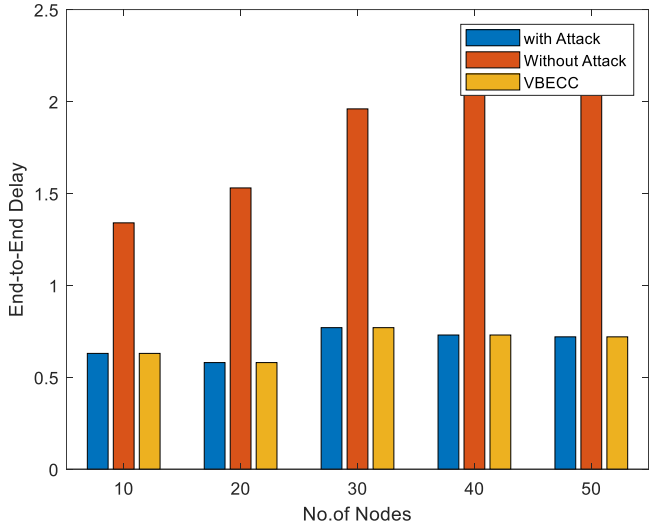
The computation of variables for proposed VBECC evaluated with consideration of with and without attack scenario. The performance analysis expressed that the proposed VBECC scheme increases the performance of network rather than with incorporated attack. In figure 4 performance of proposed VBECC for with and without attack scenario is presented for different parameters.



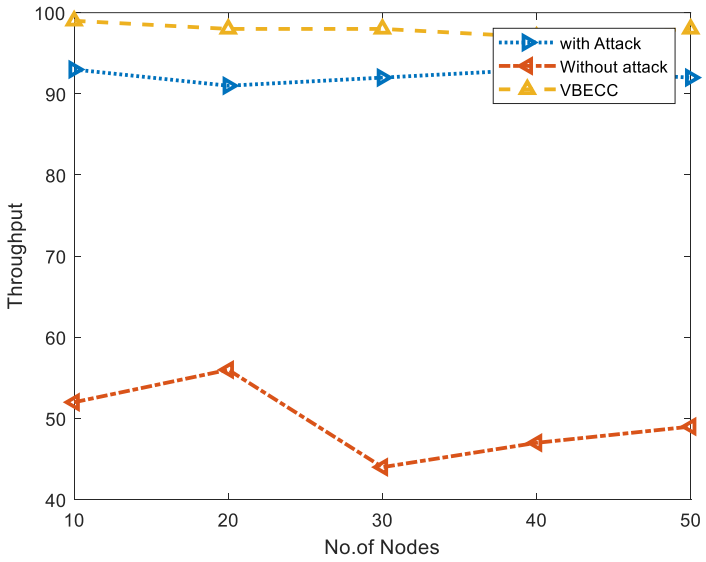
(a)



(b)



(c)



(d)

Figure 4. (A) Comparison of Jitter (B) Comparison of PDR (C) Comparison of E2E (D) Comparison of Throughput

Similarly, for the proposed VBECC the attack detection rate of the network is computed as stated in table 3. The comparative analysis for the different nodes in the network is presented in figure 5.

Table 3. Attack Detection Rate for Varying Node

Attack Nodes	**Node = 10**	**Node = 20**	**Node = 30**	**Node = 40**	**Node = 50**
2	91	89	90	87	84
4	88	86	84	83	82
6	85	92	86	79	89
8	87	85	82	77	84
10	83	83	88	82	78

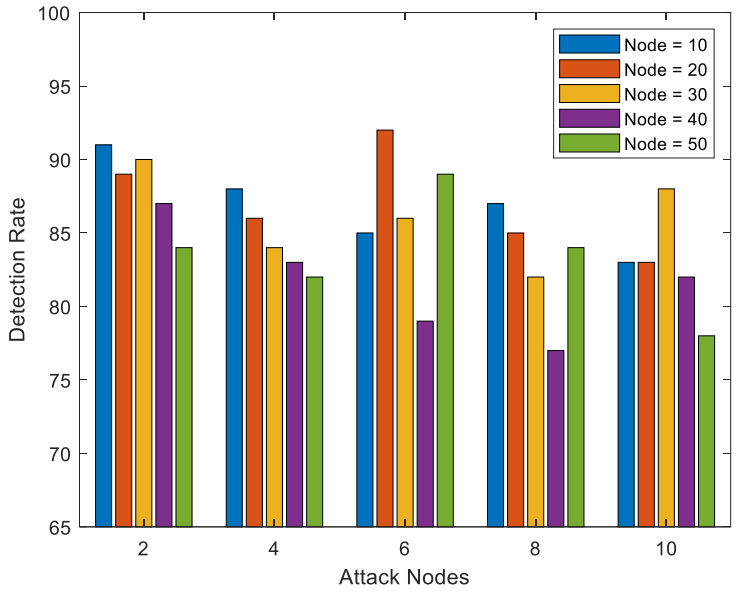


Figure 5. Comparison of Detection Rate

Based on the consideration of the different attacks node in the varying number of nodes as 10,20, 30, 40 and 50 detection rate are estimated. The attack node of node 10 detection rate is measured as 91%. Similarly, for varying node size and attack node detection rate is estimated. The attack detection rate of the proposed VBECC for varying nodes and mobility is computed. The performance of the proposed VBECC for attack classification is presented in table 4 and figure 6.

Table 4. VBECC Attack Classification Performance

	Accuracy	Precision	Recall
Normal activity	97	97	98
Anomaly	98	97	98
DoS	95	96	96
Probe Attack	91	91	92
U2R (User to Root) Attack	91	92	91
R2L (Root to Local)	94	95	95

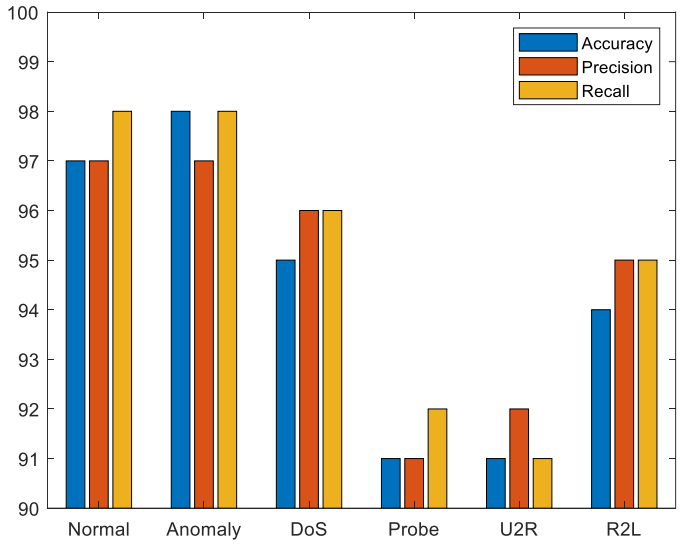


Figure 6. Comparison of Performance with Different Classifier

The proposed VBECC scheme classifier performance for different attacks is computed for analysis. The analysis expressed that the proposed VBECC scheme exhibits a higher accuracy value of anomaly with 98%. In the case of a black hole attack, the classification accuracy is estimated as 96%. Similarly, in the estimation of precision DoS and Blackhole attack, it is achieved as 96%. The recall value is estimated higher value of 98% for anomaly detection.

5. Conclusion

Cloud computing model is extension edge computing technology for the real-time application to achieve security and reliability. Edge computing technology is transfer of sensitive information for the increased information processing. The edge computing model uses the sensitive privacy information processing maintenance for the stored edge server in service location. This paper uses the VBECC model millimetre communication edge computing application for the voting scheme with millimetre application. The simulation analysis expressed that VBECC scheme ~8% increases the conventional technique for the improved data security in the edge computing model.

References

[1] Bhat, S. A., Sofi, I. B., & Chi, C. Y. (2020). edge computing and its convergence with blockchain in 5G and beyond: security, challenges, and opportunities. *IEEE Access*, *8*, 205340-205373.

[2] Bonnah, E., & Shiguang, J. (2020). DecChain: A decentralized security approach in Edge Computing based on Blockchain. *Future Generation Computer Systems*, *113*, 363-379.

[3] Liao, Z., Pang, X., Zhang, J., Xiong, B., & Wang, J. (2021). Blockchain on security and forensics management in edge computing for iot: A comprehensive survey. *IEEE Transactions on Network and Service Management*.

[4] Nguyen, D. C., Ding, M., Pham, Q. V., Pathirana, P. N., Le, L. B., Seneviratne, A., ... & Poor, H. V. (2021). Federated learning meets blockchain in edge computing: Opportunities and challenges. *IEEE Internet of Things Journal*, *8*(16), 12806-12825.

[5] Luo, C., Xu, L., Li, D., & Wu, W. (2020). Edge computing integrated with blockchain technologies. In *Complexity and Approximation* (pp. 268-288). Springer, Cham.

[6] Xuan, S., Chen, Z., Chung, I., Tan, H., Man, D., Du, X., ... & Guizani, M. (2021). ECBCM: a prestige-based edge computing blockchain security consensus model. *Transactions on Emerging Telecommunications Technologies*, *32*(6), e4015.

[7] Zhang, L., Zou, Y., Wang, W., Jin, Z., Su, Y., & Chen, H. (2021). Resource allocation and trust computing for blockchain-enabled edge computing system. *Computers & Security*, *105*, 102249.

[8] Xu, H., Huang, W., Zhou, Y., Yang, D., Li, M., & Han, Z. (2021). Edge computing resource allocation for unmanned aerial vehicle assisted mobile network with blockchain applications. *IEEE Transactions on Wireless Communications*, *20*(5), 3107-3121.

[9] Wu, Y., Dai, H. N., & Wang, H. (2020). Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0. *IEEE Internet of Things Journal*, *8*(4), 2300-2317.

[10] Lu, Y., Zhang, J., Qi, Y., Qi, S., Zheng, Y., Liu, Y., ... & Wei, W. (2021). Accelerating at the edge: a storage-elastic blockchain for latency-sensitive vehicular edge computing. *IEEE transactions on intelligent transportation systems*.

[11] Aswathy, S. U., Tyagi, A. K., & Kumari, S. (2021). The Future of Edge Computing with Blockchain Technology: Possibility of Threats, Opportunities, and Challenges. *Recent Trends in Blockchain for Information Systems Security and Privacy*, 261-292.

[12] Abdellatif, A. A., Samara, L., Mohamed, A., Erbad, A., Chiasserini, C. F., Guizani, M., ... & Laughton, J. (2021). Medge-chain: Leveraging edge computing and blockchain for efficient medical data exchange. *IEEE Internet of Things Journal*, *8*(21), 15762-15775.

[13] Zhang, P., Sun, H., Situ, J., Jiang, C., & Xie, D. (2021). Federated transfer learning for iiot devices with low computing power based on blockchain and edge computing. *Ieee Access*, *9*, 98630-98638.

[14] Wang, X., Garg, S., Lin, H., Kaddoum, G., Hu, J., & Hossain, M. S. (2020). A secure data aggregation strategy in edge computing and blockchain empowered Internet of things. *IEEE Internet of Things Journal*.

[15] Dai, Y., Xu, D., Zhang, K., Maharjan, S., & Zhang, Y. (2020). Deep reinforcement learning and permissioned blockchain for content caching in vehicular edge computing and networks. *IEEE Transactions on Vehicular Technology*, *69*(4), 4312-4324.

[16] Bhattacharya, P., Tanwar, S., Shah, R., & Ladha, A. (2020). Mobile edge computing-enabled blockchain framework—a survey. In *Proceedings of ICRIC 2019* (pp. 797-809). Springer, Cham.

[17] Cui, L., Su, X., Ming, Z., Chen, Z., Yang, S., Zhou, Y., & Xiao, W. (2020). Creat: Blockchain-assisted compression algorithm of federated learning for content caching in edge computing. *IEEE Internet of Things Journal*.

[18] Ajayi, O. J., Rafferty, J., Santos, J., Garcia-Constantino, M., & Cui, Z. (2021). BECA: A Blockchain-Based Edge Computing Architecture for Internet of Things Systems. *IoT*, *2*(4), 610-632.

[19] Dirgantoro, K. P., Lee, J. M., & Kim, D. S. (2020, February). Generative adversarial networks based on edge computing with blockchain architecture for security system. In *2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)* (pp. 039-042). IEEE.

[20] Gupta, R. Singh, V. K. Nassa, R. Bansal, P. Sharma and K. Koti, "Investigating Application and Challenges of Big Data Analytics with Clustering," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), 2021, pp. 1-6, doi: 10.1109/ICAECA52838.2021.9675483.

[21] V. Veeraiah, H. Khan, A. Kumar, S. Ahamad, A. Mahajan and A. Gupta, "Integration of PSO and Deep Learning for Trend Analysis of Meta-Verse," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2022, pp. 713-718, doi: 10.1109/ICACITE53722.2022.9823883.

[22] Anand, R., Shrivastava, G., Gupta, S., Peng, S. L., & Sindhwani, N. (2018). Audio watermarking with reduced number of random samples. In Handbook of Research on Network Forensics and Analysis Techniques (pp. 372-394). IGI Global.

[23] Meelu, R., & Anand, R. (2010, November). Energy Efficiency of Cluster-based Routing Protocols used in Wireless Sensor Networks. In AIP Conference Proceedings (Vol. 1324, No. 1, pp. 109-113). American Institute of Physics.

[24] Pandey, B.K. et al. (2023). Effective and Secure Transmission of Health Information Using Advanced Morphological Component Analysis and Image Hiding. In: Gupta, M., Ghatak, S., Gupta, A., Mukherjee, A.L. (eds) Artificial Intelligence on Medical Data. Lecture Notes in Computational Vision and Biomechanics, vol 37. Springer, Singapore. https://doi.org/10.1007/978-981-19-0151-5_19

[25] V. Veeraiah, K. R. Kumar, P. LalithaKumari, S. Ahamad, R. Bansal and A. Gupta, "Application of Biometric System to Enhance the Security in Virtual World," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2022, pp. 719-723, doi: 10.1109/ICACITE53722.2022.9823850.

[26] R. Bansal, A. Gupta, R. Singh and V. K. Nassa, "Role and Impact of Digital Technologies in E-Learning amidst COVID-19 Pandemic," 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2021, pp. 194-202, doi: 10.1109/CCICT53244.2021.00046.

[27] A. Shukla, S. Ahamad, G. N. Rao, A. J. Al-Asadi, A. Gupta and M. Kumbhkar, "Artificial Intelligence Assisted IoT Data Intrusion Detection," 2021 4th International Conference on Computing and Communications Technologies (ICCCT), 2021, pp. 330-335, doi: 10.1109/ICCCT53315.2021.9711795.

[28] Pathania, V. et al. (2023). A Database Application of Monitoring COVID-19 in India. In: Gupta, M., Ghatak, S., Gupta, A., Mukherjee, A.L. (eds) Artificial Intelligence on Medical Data. Lecture Notes in Computational Vision and Biomechanics, vol37. Springer, Singapore. https://doi.org/10.1007/978-981-19-0151-5_23

[29] Kaushik Dushyant; Garg Muskan; Annu; Ankur Gupta; SabyasachiPramanik, "Utilizing Machine Learning and Deep Learning in Cybesecurity: An Innovative Approach," in Cyber Security and Digital Forensics: Challenges and Future Trends, Wiley, 2022, pp.271-293, doi: 10.1002/9781119795667.ch12.

[30] Babu, S.Z.D. et al. (2023). Analysation of Big Data in Smart Healthcare. In: Gupta, M., Ghatak, S., Gupta, A., Mukherjee, A.L. (eds) Artificial Intelligence on Medical Data. Lecture Notes in Computational Vision and Biomechanics, vol 37. Springer, Singapore. https://doi.org/10.1007/978-981-19-0151-5_21

[31] Anand, R., Sindhwani, N., & Saini, A. (2021). Emerging Technologies for COVID-19. Enabling Healthcare 4.0 for Pandemics: A Roadmap Using AI, Machine Learning, IoT and Cognitive Technologies, 163-188.

[32] BijenderBansal; V. NishaJenipher; Rituraj Jain; R. Dilip; MakhanKumbhkar; SabyasachiPramanik; Sandip Roy; Ankur Gupta, "Big Data Architecture for Network Security," in Cyber Security and Network Security , Wiley, 2022, pp.233-267, doi: 10.1002/9781119812555.ch11.

[33] A. Gupta, D. Kaushik, M. Garg and A. Verma, "Machine Learning model for Breast Cancer Prediction," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2020, pp. 472-477, doi: 10.1109/I-SMAC49090.2020.9243323.

[34] Sreekanth, N., Rama Devi, J., Shukla, A. et al. Evaluation of estimation in software development using deep learning-modified neural network. ApplNanosci (2022). https://doi.org/10.1007/s13204-021-02204-9

[35] V. Veeraiah, N. B. Rajaboina, G. N. Rao, S. Ahamad, A. Gupta and C. S. Suri, "Securing Online Web Application for IoT Management," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2022, pp. 1499-1504, doi: 10.1109/ICACITE53722.2022.9823733.

[36] Anand, R., Singh, J., Pandey, D., Pandey, B. K., Nassa, V. K., & Pramanik, S. (2022). Modern Technique for Interactive Communication in LEACH-Based Ad Hoc Wireless Sensor Network. In Software Defined Networking for Ad Hoc Networks (pp. 55-73). Springer, Cham.

[37] V. Veeraiah, G. P, S. Ahamad, S. B. Talukdar, A. Gupta and V. Talukdar, "Enhancement of Meta Verse Capabilities by IoT Integration," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2022, pp. 1493-1498, doi: 10.1109/ICACITE53722.2022.9823766.

[38] Gupta, N. ., Janani, S. ., R, D. ., Hosur, R. ., Chaturvedi, A. ., & Gupta, A. . (2022). Wearable Sensors for Evaluation Over Smart Home Using Sequential Minimization Optimization-based Random Forest. International Journal of Communication Networks and Information Security (IJCNIS), 14(2), 179–188. https://doi.org/10.17762/ijcnis.v14i2.5499

[39] Keserwani, H. ., Rastogi, H. ., Kurniullah, A. Z. ., Janardan, S. K. ., Raman, R. ., Rathod, V. M. ., & Gupta, A. . (2022). Security Enhancement by Identifying Attacks Using Machine Learning for 5G Network. International Journal of Communication Networks and Information Security (IJCNIS), 14(2), 124–141. https://doi.org/10.17762/ijcnis.v14i2.5494