

# Archimedes assisted LSTM model for blockchain based privacy preserving IoT with smart cities

Sanjaikanth E Vadakkethil Somanathan Pillai<sup>1</sup>, Rohith Vallabhaneni<sup>2</sup>, Srinivas A Vaddadi<sup>2</sup>,  
Santosh Reddy Addula<sup>2</sup>, Bhuvanesh Ananthan<sup>3</sup>

<sup>1</sup>School of Electrical Engineering and Computer Science, University of North Dakota, Grand Forks, USA

<sup>2</sup>Department of Information Technology, University of the Cumberland, Williamsburg, USA

<sup>3</sup>Department of Electrical and Electronics Engineering, PSN College of Engineering and Technology, Tirunelveli, India

## Article Info

### Article history:

Received Mar 19, 2024

Revised Sep 10, 2024

Accepted Sep 29, 2024

### Keywords:

Archimedes optimizer

Blockchain

Data security

Internet of things

Long short-term memory

## ABSTRACT

Presently, the emergence of internet of things (IoT) has significantly improved the processing, analysis, and management of the substantial volume of big data generated by smart cities. Among the various applications of smart cities, notable ones include location-based services, urban design and transportation management. These applications, however, come with several challenges, including privacy concerns, mining complexities, visualization issues and data security. The integration of blockchain (BC) technology into IoT (BIoT) introduces a novel approach to secure smart cities. This work presents an Archimedes assisted long short-term memory (LSTM) model intrusion detection for BC based privacy preserving (PP) IoT with smart cities. After the stage of pre-processing, the LSTM is utilized for automated feature extraction and classification. At last, the Archimedes optimizer (AO) is utilized to optimize the LSTM's hyper-parameters. In addition, the BC technology is utilized for securing the data transmission.

*This is an open access article under the [CC BY-SA](#) license.*



## Corresponding Author:

Sanjaikanth E Vadakkethil Somanathan Pillai

School of Electrical Engineering and Computer Science, University of North Dakota  
Grand Forks, USA

Email: s.evadakkethil@und.edu

## 1. INTRODUCTION

The concept of a smart city is seen as a technological framework employed by various stakeholders within a city to achieve specific goals. These objectives encompass aspects such as promoting good governance, improving daily living conditions, optimizing resource utilization, and creating new opportunities for commerce [1]. Technological progress has made in enhancements in day-to-day life and this next generation advancement not only facilitates industries but also enables economies for exploring different opportunities. Simultaneously, people are interconnected through mobiles and laptops. Moreover, smart devices have become ubiquitous in cities worldwide [2].

Cities are currently in an expansion phase, focusing on the growth of control systems, services, screening and infrastructure to assimilate recent changes. Aspects like location services, weather, smart traffic, and transportation are interconnected [3]. However, the uncontrollable emergence of cities introduces new challenges that need consideration by stakeholder's and government officials. The concepts of smart city revolve around embedded models, smart, and sensing methodologies [4]. Basically, smart cities leverage constant structures to elevate living standards. Two major issues, security, and concerns related to electrical crimes, are prominent. Ensuring security in a smart city involves addressing three crucial components: governance, technological, and societal aspects.

Intrusion detection system (IDS) proves to be more effective in monitoring activities, detecting unauthorized utilization, identifying potential destruction of information systems, and safeguarding against both internal and external intrusions [5]. Particularly in the context of newly created online applications based on the web within smart cities and the internet of things (IoT) system, IDS is regarded as a crucial security solution. However, IDS based models often generate a higher volume of inappropriate and false alarms when abnormal behaviors are detected. An excessive false alarm rate can significantly hamper the IDS performance in comparison to actual cyber attacks, posing a considerable challenge for security analysts. Moreover, it entails substantial costs for the detection, management, and IDS computation [6]. Conventional IDS based methodologies also present elevated failures when applied to IoT, given the dynamic nature of smart city applications. Hence, there is a pressing need for a robust security network specifically designed to facilitate the rapid emergence of the smart city field in an IoT network.

Security is not merely a requirement for the continued utilization of blockchain (BC); it can actively contribute to data dispersion by operating at an accelerated pace. One notable advantage of incorporating BC networks is their ability to store data in an immutable manner without the need for a centralized database. Moreover, BC tracks and executes transactions among multiple participants within a trusted environment [7]. Through the utilization of robust encryption using private and public keys, the BC further enhances the security levels for its participants. The contributions are:

- To present an automated model for BC based privacy preserving (PP) IoT with smart cities.
- To introduce the long short-term memory (LSTM) with Archimedes optimizer (AO) to optimize the LSTM's hyper-parameters and attain better performance.

The remaining sections are: Section 2 furnishes a literature review, examining research endeavors that have utilized diverse BC based PP model. Section 3 furnishes a detailed elucidation of the proposed BC based PP model, accompanied by a succinct analysis. Section 4 delineates the experimental components, and section 5 encapsulates the work with a conclusion.

## 2. RELATED WORKS

Ji *et al.* [8] presented BC based PP for telecare clinical information models. This existing work provided location based clinical information among clinical analyzers, clinical workers and patients. Then, the security measures like decentralization, multi stage privacy recovery, retrievability, confidentiality, unforgeability, and verifiability were analyzed. However, this model was complex to analyze the shared location's validity.

Yang *et al.* [9] developed BC based location PP crowd sensing model to protect location of the worker. The model safeguards the information of location and ensures equitable trading without relying on trusting unauthorized users. In addition, this existing model overcomes re-identified attacks using the private BC. This network disperses transactions of worker's data across numerous systems. This prevents attackers from deducing the identity of workers through analysis of their transactions.

Zhu *et al.* [10] developed federated learning (FL) with BC methodology based PP. This existing model leveraged decentralized models evaluated through BC for establishing a safe learning coordinate model and for detecting and eliminating Byzantine members. Experimentation was carried out by varying 5 cross validation for training the personal and local approaches.

Kumar *et al.* [11] suggested attention-bidirectional long short term memory (A-Bi-LSTM) with chameleon swarm algorithm (CSA) for BC based PP. Then, the BC was employed to ensure the secure data transmission to cloud servers and the accuracy attained by this existing work was 97.4%. Moreover, the BC provided an open digital ledger, decentralized, and distributed, serving as a platform for storing transactions using various approaches.

Weng *et al.* [12] presented DeepChain cooperative training framework featuring an incentive model. This existing work preserved the local gradient privacy and ensured transparency in the train set. Through the utilization of incentive models and transactions, members were incentivized to act honestly, specifically in tasks such as parameter updation and gradient collection. This approach ensures fairness throughout the collaborative training process.

Numerous data-securing systems have been developed by researchers to provide security and privacy for apps intended for smart city applications. Data integrity and privacy concerns with smart apps have not been satisfactorily addressed by previous centralized cloud-based data-sharing frameworks. On the other hand, blockchain-based solutions offer more advancements in resolving privacy concerns. First, client data is divided into different communities based on similarity labels utilizing data gathered from sensors via a detection algorithm. With a specified detection algorithm, it possesses a certain kind of control over community data. Nevertheless, data security during data transfer via sensors has not been covered by this architecture [13]. One of the most promising solutions for ensuring data integrity for IoT applications is blockchain. Its traceability and tamper-proofing capabilities enable decentralized data storage for intelligent

applications as well as transparent sharing services. A block header, timestamp, transaction data, and a prior block hash are all included in each individual block that makes up the blockchain. To provide transparency, all nodes have a full copy of the transaction data; this places a significant burden on the system. Lastly, blocks are added in accordance with a schedule. Multiple parties are transacting in smart city apps at various times and locations, therefore uploading data directly could put a heavy load on the blockchain [14], [15]. Blockchain-based solutions give smart city security alternatives an upgrade. Most smart applications are suitable for the distributed environment that blockchain ensures [16]–[18]. Despite this, blockchain technology holds great promise for addressing the security and privacy issues in smart cities. Many IoT devices have minimal power, little data storage, and insufficient battery life, which prevents them from handling complex tasks.

Furthermore, in blockchain-based networks, consensus mechanisms like proof-of-work (PoW) require additional resources. Nodes engaged in the distributed network decision-making process during mining require a significant amount of processing power. Another interesting use of blockchain technology that applies various access controls to IoT smart apps is smart contracts. Furthermore, the security and privacy of smart applications depend heavily on the provenance of data [19]–[22]. Access-based access control (ABAC) offers the fine-grained policies utilized to permit or prohibit different actions of smart ecosystems, as well as the flexibility and granularity required to properly protect the data collected and shared by smart entities. However, prior to using the framework, ABAC must overcome issues with complexity, overhead, and privacy [23].

The following research gaps were identified from the detailed literature review. Integration of blockchain and LSTM models:

- Optimization of computational efficiency: the integration of blockchain with LSTM models is computationally intensive. Research is needed to optimize these models for real-time processing in resource-constrained IoT environments within smart cities.
- Scalability of combined systems: while blockchain provides a secure and decentralized framework, its scalability when integrated with LSTM models for large-scale IoT deployments in smart cities is still an open question.
- Privacy and data security: fine-tuning privacy mechanisms: there is a need to explore more sophisticated privacy-preserving mechanisms that balance data utility and privacy, particularly when sensitive IoT data is used for training LSTM models.
- Data anonymization techniques: research is needed to develop and evaluate new data anonymization techniques that can be integrated with blockchain to further enhance privacy while maintaining the accuracy of LSTM predictions.

### 3. PROPOSED METHOD

In this work, an efficient deep learning (DL) model LSTM with AO algorithm for BC based PP model in the smart city environment. Figure 1 defines the framework of the proposed BC based PP model. Here, the min-max normalization is applied for converting the raw data into an essential format. Subsequently, the LSTM model is utilized for the IDS classification process. At last, the AO method is exploited for the optimal tuning of hyper-parameters in the LSTM network [24].

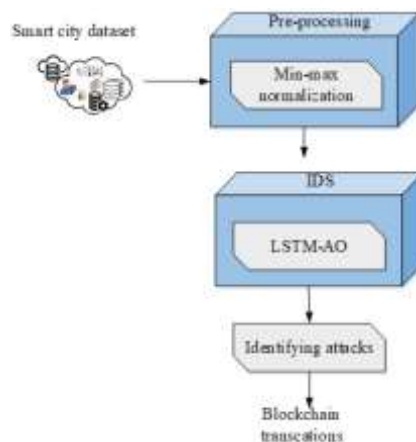


Figure 1. Framework of the proposed BC based PP model

**3.1. Pre-processing**

In this instance, min-max normalization has been employed to scale the dataset to the variance of the unit. This method is widely utilized for assessing the degree of similarity between data points. Let us consider data  $G$  is derived from a dataset and it varies from  $G_{min}$  to  $G_{max}$  and it is expressed as:

$$G_{norm} = \frac{G - G_{min}}{G_{max} - G_{min}} \tag{1}$$

**3.2. Optimal feature extraction and classification**

Let the input data  $Z_l$  has the input  $i_l$ , forget  $f_l$  and output  $o_l$  gates and these gates are utilized for learning useful features and eliminating unnecessary features as shown in Figure 2. LSTM is designed to handle time series data in a sequential manner. Within a given time period, the data may contain both valuable and irrelevant information. The role of the  $f_l$  is to make decisive choices regarding the retention or discarding of specific information and it is given as:

$$f_l = \sigma(W_f[h_{l-1}, x_l] + b_f) \tag{2}$$

Following the decision made by the  $f_l$ , information proceeds to the  $i_l$ . The  $i_l$  plays a crucial role in the determination of which parameters should be updated and specifies the manner in which these updates are to be executed:

$$i_l = \sigma(W_i[h_{l-1}, x_l] + b_i) \tag{3}$$

$$C_l = \tanh(W_c[h_{l-1}, x_l] + b_c) \tag{4}$$

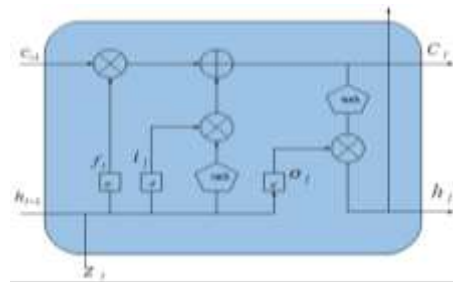


Figure 2. LSTM model

After undergoing screening by both the  $f_l$  and the  $i_l$ , the information finally arrives at the  $o_l$ . The primary aim of the  $o_l$  is to make decisions regarding which information should be selected for output:

$$o_l = \sigma(W_o[h_{l-1}, x_l] + b_o) \tag{5}$$

$$h_l = o_l \times \tanh C_l \tag{6}$$

where,  $C_l$  is the present state of the cell,  $W_i, W_f, W_c$  and  $W_o$  are the weighting matrices;  $b_i, b_f$  and  $b_o$  are the bias values.

Optimizing the Hyper-parameters of LSTM model: The hyper-parameters of LSTM are optimized by the AO optimizer. The AO functions as a population based model where the submerged entities serve as the individuals of a population. In line with other metaheuristic approaches with respect to population, AO begins the search model by initializing objects representing candidate solution's, each endowed with randomized accelerations densities, and volumes. During this phase, every candidate solution's undergoes initialization with a randomized direction in the fluid. Following the fitness assessment in the initial population, AO iteratively operates till the ending process is met. AO systematically adjusts the densities and volumes of every object in all iterations. The candidate's acceleration is then updated, considering its collision condition with the nearby candidate's. The newly calculated accelerations, densities, and volumes jointly determine the updated position of the candidate's. The subsequent section presents a thorough mathematical expression delineating the steps involved in AO.

Initialization: the following expression is utilized for initializing the candidate's position  $O_k$ :

$$O_k = ll_k + r \times (ul_k - ll_k) \quad (7)$$

Where  $ll_k, ul_k$  and  $r$  are the lower and upper limits in the  $k^{th}$  candidate's and random number. The acceleration( $ac$ ) density ( $de$ ) and volume ( $vo$ ) for every  $k^{th}$  candidate's is expressed as:

$$de_k = r \quad (8)$$

$$vo_k = r \quad (9)$$

$$ac_k = ll_k + r \times (ul_k - ll_k) \quad (10)$$

updating densities, and volumes: The densities, and volumes of  $k^{th}$  candidate's for the iteration  $t + 1$  is given as:

$$\begin{aligned} de_k^{t+1} &= de_k^t + r \times (de_b - de_k^t) \\ vo_k^{t+1} &= vo_k^t + r \times (vo_b - vo_k^t) \end{aligned} \quad (11)$$

where,  $de_b$  and  $vo_b$  are the best values of density and volume.

Initially, the interaction between candidate's results in collisions, and over time, these entities endeavor to achieve an equilibrium phase. AO employs a transfer operation  $T_f$  and this operation serves as a mechanism for guiding the system dynamics, steering it from an exploration phase, characterized by diverse searches, towards an exploitation phase, where the focus is on refining and optimizing identified options.

$$T_f = \exp\left(\frac{t-t_m}{t_m}\right) \quad (12)$$

where  $t$  and  $t_m$  are the present and maximum iterations. The density term  $de$  aid on the global to local search is given as:

$$de^{t+1} = \exp\left(\frac{t_m-t}{t_m}\right) - \left(\frac{t}{t_m}\right) \quad (13)$$

exploration stage: when  $T_f \leq 0.5$ , interaction among candidates happens and the random object ( $ro$ ) is selected and the acceleration( $ac$ ) is updated as:

$$ac_k^{t+1} = \frac{de_{ro} + vo_{ro} \times ac_{ro}}{de_k^{t+1} \times vo_k^{t+1}} \quad (14)$$

where  $ac_k^{t+1}, de_k^{t+1}$  and  $vo_k^{t+1}$  are the acceleration, density and volume at the  $k^{th}$  candidate's.  $ac_{ro}, de_{ro}$ , and  $vo_{ro}$  are the acceleration, density and volume of the random object ( $ro$ ).

Exploitation stage: when  $T_f > 0.5$ , there is no interaction among candidates and the acceleration( $ac$ ) is updated as:

$$ac_k^{t+1} = \frac{de_b + vo_b \times ac_b}{de_k^{t+1} \times vo_k^{t+1}} \quad (15)$$

acceleration normalization: for computing the Acceleration normalization  $ac_{k-norm}^{t+1}$ , the following expression is given as:

$$ac_{k-norm}^{t+1} = u \frac{ac_k^{t+1} - \min(ac)}{\max(ac) - \min(ac)} + g \quad (16)$$

where  $u$  and  $g$  are the normalized term.  $\max(ac)$  and  $\min(ac)$  are the maximum and minimum accelerations.

Updating stage: when  $T_f \leq 0.5$ , the  $k^{th}$  candidate's for the iteration  $t + 1$  is given as:

$$x_k^{t+1} = x_k^t + K_1 \times r \times ac_{k-norm}^{t+1} \times de \times (x_r - x_k^t) \quad (17)$$

when  $T_f > 0.5$ , the  $k^{th}$  candidate's for the iteration  $t + 1$  is given as:

$$x_k^{t+1} = x_b^t + F \times K_2 \times r \times ac_{k-norm}^{t+1} \times de \times (x_b - x_k^t) \tag{18}$$

where  $F$  is the Flag,  $K_1$  and  $K_2$  are the constant parameters. The pseudocode of AO is given in the Algorithm 1.

**Algorithm 1. Pseudocode of the AO**

```

Initializing  $k^{th}$  candidate's solution with randomized acceleration( $ac$ ) density ( $de$ ) and volume ( $vo$ ) using the Equations (7) to (9)
Execute initial population and choose the best value of fitness
while  $t \leq max\_iter$  do
  for candidate's solution  $k$  do
    Updating densities, and volumes using Equations (11)
    Updating  $T\_fandde$  using the Equations (12) and (13)
    When  $T_f \leq 0.5$ 
      Update the acceleration( $ac$ ) using the Equation (14)
      Update the solution using the Equation (17)
    else
      When  $T_f > 0.5$ 
        Update the acceleration normalization  $ac_{k-norm}^{t+1}$  using the Equation (15)
        Update the solution using the Equation (18)
    end if
  end for
  Execute every candidate's solution and choose the best value of fitness
   $t = t + 1$ 
end while
return best value of fitness
    
```

**3.3. BC technology**

This study employs BC for ensuring the secure transmission of data within the smart city environment. BC operates as a decentralized peer-to-peer (P2P) network, wherein each transaction is verified by registered nodes and securely recorded in an established and distributed ledger. In this context, the consensus mechanism plays a pivotal role in the BC, guaranteeing the reliability of the network. Notably, the absence of a centralized authorization for authenticating events necessitates that all transactions be validated by BC nodes through consensus mechanism.

**4. RESULTS ANALYSIS**

This section presents an examination of the outcomes derived from the BC based PP-IDS model in the smart city environment. Measures utilized to evaluate the performance are given in Table 1. Terms like  $S_{po}$  and  $S_{ne}$  are the true and false positives,  $R_{po}$  and  $R_{ne}$  true and false negatives are utilized for performance evaluation.

Table 1. Performance measures

Metrics	Expressions
Accuracy	$\frac{S_{po} + S_{ne}}{S_{po} + S_{ne} + R_{po} + R_{ne}}$
Precision	$\frac{S_{po}}{S_{po} + R_{po}}$
Sensitivity	$\frac{S_{po}}{S_{po} + R_{ne}}$
Specificity	$\frac{S_{ne}}{S_{ne} + R_{po}}$

**4.1. Dataset description**

The benchmark test for a BC based PP-IDS model in the smart city environment, developed across multiple prior studies, and utilized the NSL-KDD dataset [25]. This dataset encompasses the KDDTrain+ for training and KDDTest+ for testing purposes. The dataset has the classes like normal, DoS, R2L, probe and U2R.

**4.2. Comparative analysis**

Initially, the performance of the proposed approach like accuracy-loss curves and confusion matrix is given. Then, the comparative analysis is made for different models. Table 2 indicates the robustness of the suggested BC based PP-IDS. The analyses obtained through the proposed technique have proficiently categorized samples across all classes like normal, DoS, R2L, probe and U2R with better performance.

**Table 2. Performance of the proposed BC based PP-IDS model**

Classes	Accuracy (%)	Precision (%)	Sensitivity (%)	Specificity (%)
Normal	98.4	97.9	97.1	96.4
DoS	98.2	98.2	98.4	98.7
R2L	97.9	98.6	97.2	97.4
probe	95.1	97.1	98.4	98.2
U2R	95.8	96.4	98.9	98.7

Figure 3 delineates the accuracy-loss curves of the proposed BC based PP-IDS model. The analysis is made by varying the epoch values of 160. In Figure 3(a), the fitting curves for training-testing accuracy and loss demonstrate satisfactory convergence, suggesting that the parameter settings of the model are well-founded. Similarly in Figure 3(b), the loss curve is plotted.

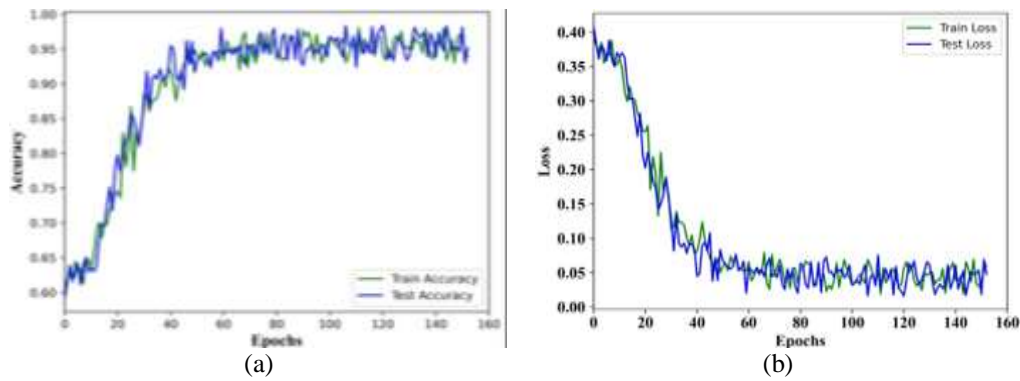


Figure 3. Accuracy-loss curves of the proposed model; (a) accuracy curve and (b) loss curve

Assessing the performance of the algorithms involves further evaluation through the utilization of the confusion matrix. Figure 4 illustrates the confusion matrix of the proposed BC based PP-IDS model. Here, 8,490 instances are classified as normal, 1,181 instances are classified as DoS, 170 instances are classified as R2L, 9 instances are classified as probe and 12,488 instances are classified as U2R.

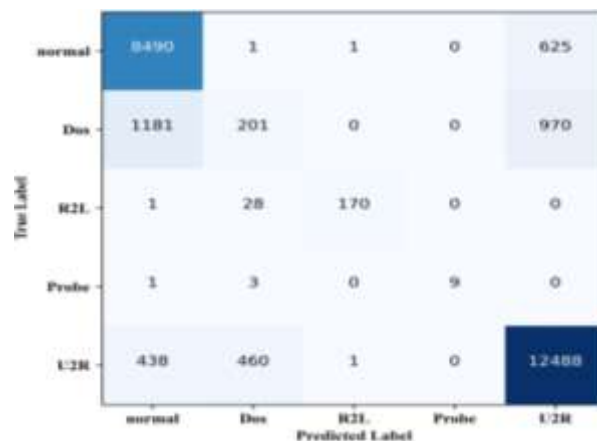


Figure 4. Confusion matrix of the proposed BC based PP-IDS model

Table 3 delineates the comparative analysis of the various ML and DL models. The models like support vector machine (SVM), Naïve Bayes (NB), CNN, LSTM, Bi-GRU and the proposed BC based PP-IDS model. Demonstration has confirmed the superiority of the proposed BC based PP-IDS over other models by achieving better accuracy (97.08%), precision (97.64%), sensitivity (98%) and specificity (97.88%) on the NSL-KDD dataset.

Table 3. Comparative analysis

Methods	Accuracy (%)	Precision (%)	Sensitivity (%)	Specificity (%)
SVM	90.7	89.1	90.3	89.4
NB	92.3	88.4	94.2	89.9
CNN	93.1	94.2	95.1	90.2
LSTM	94.5	95.3	96.3	90.4
BiGRU	96.1	95.8	97.2	95.2
Proposed	97.08	97.64	98	97.88

The proposed model applied within the context of blockchain-based privacy-preserving IoT for smart cities can have several practical impacts such as; Enhanced data security and privacy:

- Privacy-preserving mechanisms: by integrating Blockchain with LSTM models, smart cities can ensure that sensitive data collected from IoT devices is processed and stored securely. The LSTM model helps in predicting and analyzing trends while ensuring that data remains anonymized, protecting citizens' privacy.
- Immutable and transparent ledger: blockchain provides an immutable record of transactions, ensuring that data integrity is maintained and that all actions taken on the data are transparent and traceable. Improved decision-making in real-time.
- Accurate forecasting: the LSTM model's capability to handle sequential data allows for accurate forecasting and pattern recognition, which is crucial for real-time decision-making in smart cities. For example, it can be used for traffic management, energy distribution, and public safety measures.
- Predictive maintenance: IoT devices in smart cities can benefit from predictive maintenance algorithms powered by LSTM, reducing downtime and ensuring the efficient operation of city infrastructure.

## 5. CONCLUSION

This study introduced a robust BC based PP-IDS model, integrating BC and optimized DL model to enhance security within the smart city environment. The proposed BC based PP-IDS model technique comprises various stages including preprocessing, and automated feature extraction and classification. Additionally, BC technology was harnessed for the secure transmission of data in the IoT. The robustness of the suggested BC based PP-IDS model was validated using the benchmark dataset, and the outcomes are thoroughly examined from multiple perspectives. Experimental findings underscore the superiority of the proposed BC based PP-IDS compared to recent approaches. Consequently, the proposed BC based PP-IDS emerges as an effective methodology for enhancing security in diverse sectors of the smart city environment. Future work may focus on further improving the proposed BC based PP-IDS model's performance by incorporating hybrid DL and optimization models.

## ACKNOWLEDGEMENTS

The author with a deep sense of gratitude would thank the supervisor for his guidance and constant support rendered during this research.

## REFERENCES





- [1] H. Jiang, J. Li, P. Zhao, F. Zeng, Z. Xiao, and A. Iyengar, "Location privacy-preserving mechanisms in location-based services," *ACM Computing Surveys*, vol. 54, no. 1, pp. 1–36, Jan. 2021, doi: 10.1145/3423165.
- [2] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "MediBchain: A blockchain based privacy preserving platform for healthcare data," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10658 LNCS, 2017, pp. 534–543. doi: 10.1007/978-3-319-72395-2\_49.
- [3] R. Varsha, M. M. Nair, S. M. Nair, and A. K. Tyagi, "Deep learning based Blockchain solution for preserving privacy in future vehicles," *International Journal of Hybrid Intelligent Systems*, vol. 16, no. 4, pp. 223–236, Feb. 2020, doi: 10.3233/HIS-200289.
- [4] S. Mishra and V. K. Chaurasiya, "Hybrid deep learning algorithm for smart cities security enhancement through blockchain and internet of things," *Multimedia Tools and Applications*, vol. 83, no. 8, pp. 22609–22637, Aug. 2024, doi: 10.1007/s11042-023-16406-6.







- [5] P. Jisna, T. Jarin, and P. N. Praveen, "Advanced intrusion detection using deep learning-LSTM network on cloud environment," in *Proceedings of the 4th International Conference on Microelectronics, Signals and Systems, ICMSS 2021*, IEEE, Nov. 2021, pp. 1–6. doi: 10.1109/ICMSS53060.2021.9673607.
- [6] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: A review," *IEEE Access*, vol. 6, pp. 10179–10188, 2018, doi: 10.1109/ACCESS.2018.2799854.
- [7] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, N. Kumar, and M. M. Hassan, "A privacy-preserving-based secure framework using blockchain-enabled deep-learning in cooperative intelligent transport system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 16492–16503, Sep. 2022, doi: 10.1109/TITS.2021.3098636.
- [8] Y. Ji, J. Zhang, J. Ma, C. Yang, and X. Yao, "BMPLS: Blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems," *Journal of Medical Systems*, vol. 42, no. 8, p. 147, Aug. 2018, doi: 10.1007/s10916-018-0998-2.
- [9] M. Yang, T. Zhu, K. Liang, W. Zhou, and R. H. Deng, "A blockchain-based location privacy-preserving crowdsensing system," *Future Generation Computer Systems*, vol. 94, pp. 408–418, May 2019, doi: 10.1016/j.future.2018.11.046.
- [10] X. Zhu, H. Li, and Y. Yu, "Blockchain-based privacy preserving deep learning," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11449 LNCS, 2019, pp. 370–383. doi: 10.1007/978-3-030-14234-6\_20.
- [11] K. P. M. Kumar *et al.*, "Privacy preserving blockchain with optimal deep learning model for smart cities," *Computers, Materials and Continua*, vol. 73, no. 3, pp. 5299–5314, 2022, doi: 10.32604/cmc.2022.030825.
- [12] J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, "DeepChain: auditable and privacy-preserving deep learning with blockchain-based incentive," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2019, doi: 10.1109/tdsc.2019.2952332.
- [13] M. Gupta, F. M. Awaysheh, J. Benson, M. Alazab, F. Patwa, and R. Sandhu, "An attribute-based access control for cloud enabled industrial smart vehicles," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4288–4297, Jun. 2021, doi: 10.1109/II.2020.3022759.
- [14] M. Ramaiah, V. Chithanuru, A. Padma, and V. Ravi, "A review of security vulnerabilities in Industry 4.0 application and the possible solutions using blockchain," in *Cyber Security Applications for Industry 4.0*, Boca Raton: Chapman and Hall/CRC, 2022, pp. 63–95. doi: 10.1201/9781003203087-3.
- [15] C. Chen, J. Yang, W. J. Tsaur, W. Weng, C. Wu, and X. Wei, "Enterprise data sharing with privacy-preserved based on hyperledger fabric blockchain in IIOT's application," *Sensors*, vol. 22, no. 3, p. 1146, Feb. 2022, doi: 10.3390/s22031146.
- [16] U. Khalil, Mueen-Uddin, O. A. Malik, and S. Hussain, "A blockchain footprint for authentication of IoT-enabled smart devices in smart cities: state-of-the-art advancements, Challenges and Future Research Directions," *IEEE Access*, vol. 10, pp. 76805–76823, 2022, doi: 10.1109/ACCESS.2022.3189998.
- [17] N. Deepa *et al.*, "A survey on blockchain for big data: Approaches, opportunities, and future directions," *Future Generation Computer Systems*, vol. 131, pp. 209–226, Jun. 2022, doi: 10.1016/j.future.2022.01.017.
- [18] C. Li, M. Dong, X. Xin, J. Li, X. B. Chen, and K. Ota, "Efficient privacy preserving in IoMT with blockchain and lightweight secret sharing," *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 22051–22064, Dec. 2023, doi: 10.1109/IIOT.2023.3296595.
- [19] H. H. Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Hyperledger fabric blockchain for securing the edge internet of things," *Sensors*, vol. 21, no. 2, p. 359, Jan. 2021, doi: 10.3390/s21020359.
- [20] N. K. Tyagi and M. Goyal, "Blockchain-based smart contract for issuance of country of origin certificate for indian customs exports clearance," *Concurrency and Computation: Practice and Experience*, vol. 35, no. 16, Jul. 2023, doi: 10.1002/cpe.6249.
- [21] A. Padma and R. Mangayarkarasi, "Detecting security breaches on smart contracts through techniques and tools a brief review: applications and challenges," in *Cognitive Science and Technology*, vol. Part F1466, 2023, pp. 361–369. doi: 10.1007/978-981-99-2742-5\_38.
- [22] P. Sharma, S. Namasudra, N. Chilamkurti, B. G. Kim, and R. G. Crespo, "Blockchain-based privacy preservation for IoT-enabled healthcare system," *ACM Transactions on Sensor Networks*, vol. 19, no. 3, pp. 1–17, Aug. 2023, doi: 10.1145/3577926.
- [23] M. Tahir, M. Sardaraz, S. Muhammad, and M. S. Khan, "A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics," *Sustainability (Switzerland)*, vol. 12, no. 17, p. 6960, Aug. 2020, doi: 10.3390/SU12176960.
- [24] F. A. Hashim, K. Hussain, E. H. Houssein, M. S. Mabrouk, and W. Al-Atabany, "Archimedes optimization algorithm: a new metaheuristic algorithm for solving optimization problems," *Applied Intelligence*, vol. 51, no. 3, pp. 1531–1551, Mar. 2021, doi: 10.1007/s10489-020-01893-z.
- [25] M. H. Zaib, "NSL-KDD network security, information security, cyber security," 2019, [Online]. Available: <https://www.kaggle.com/hassan06/nslkdd>.

## BIOGRAPHIES OF AUTHORS







**Sanjaikanth E Vadakkethil Somanathan Pillai**     (Senior Member, IEEE) holds an MS in Software Engineering from The University of Texas at Austin, Texas, USA, and a BE from the University of Calicut, Kerala, India. Currently pursuing a PhD in Computer Science at the University of North Dakota, Grand Forks, North Dakota, USA, his research spans diverse areas such as mobile networks, network security, privacy, location-based services, and misinformation detection. He can be contacted at email: [s.evadakkethil@und.edu](mailto:s.evadakkethil@und.edu).



**Rohith Vallabhaneni**     is a dedicated worker with a strong work ethic in leading teams to solve organizational issues. He is capable of learning all aspects of information within a company and using the technical knowledge and business background to effectively analyze security measures to determine their effectiveness in order to strengthen the overall security posture. He has great work ethic and outstanding team leadership skills and seek to accomplish organizational goals, while growing in knowledge and experience. He can be contacted at email: rohit.vallabhaneni.2222@gmail.com.







**Srinivas A Vaddadi**     is a dynamic and forward-thinking professional in the field of Cloud and DevSecOps. With a solid educational foundation in computer science, Srinivas embarked on a journey of continuous learning and professional growth. Their relentless pursuit of knowledge and commitment to staying at the forefront of industry advancements has earned them recognition as a thought leader in the Cloud and DevSecOps space. He can be contacted at email: vsad93@gmail.com.



**Santosh Reddy Addula**     a Senior Member of the IEEE, holds a Master of Science in Information Technology from the University of the Cumberland in Kentucky, USA. With extensive experience in the IT industry, he has demonstrated expertise across multiple domains. Santosh is an innovator with a strong portfolio of patents and has significantly contributed to academic research through his articles as an author and co-author. He can be contacted at email: santoshaddulait@gmail.com.



**Bhuvanesh Ananthan**     received the B.E. degree in Electrical and Electronics Engineering from Anna University in 2012, M.Tech. in Power System Engineering from Kalasalingam University in 2014 and Ph.D. degree from Faculty of Electrical Engineering of Anna University in 2019. He has published more than 100 papers in reputed international journals, 55 papers in international conferences and 20 books. He can be contacted at email: bhuvanesh.ananthan@gmail.com.