Securing the Internet of Things-enabled Smart City Infrastructure Using a Hybrid Framework

Achyut Shankar[1]*, Carsten Maple[2]

[1]Amity University, Noida, Uttarpradesh, India, [2]WMG, University of Warwick, United Kingdom

[1]ashankar2711@gmail.com, [2]cm@warwick.ac.uk

Abstract:

Since the Internet of Things (IoT) employs a diverse range of new technologies, it is impossible to build a single recommended design adopted as a master plan for all possible requests. Some possible IoT application areas haven't been looked into yet or don't have enough information on how to approach them. This shows that more research needs to be done in this difficult area to find new and potentially big benefits for society. Although smart cities offer residents and providers of capital several advantages, there are numerous ways that breaches could compromise the safety and security of individuals. As a result, several different recommendation designs can coexist in the IoT. This research examines the effects of ethics and technology on the security of IoT-enabled systems in smart city infrastructure. Hence provides a secure IoT network architecture for smart cities combining blockchain and deep learning to safeguard privacy and credibility. This research presents a Secure Smart City Infrastructure using Blockchain and Deep Learning (SSCI-BDL) framework to ensure privacy protection and trustworthiness among IoT communication in smart cities. This framework involves the blockchain network for security management in the smart city infrastructure. This framework integrates the deep learning model with an optimization algorithm that maintains efficient resource utilization in the smart city infrastructure. The simulation results show that the system has high security of 99.5% and the lowest latency rate of 4.1% compared to existing models. Overall, the proposed framework's efficiency gives the highest rate of 99.8%.

Keywords: Deep Learning, Security, Privacy Protection, Blockchain, Smart City Infrastructure

Introduction

Strong Private Public Partnerships are needed to integrate people, policies, procedures, and technology from both government and industry into the overall strategy process to design and develop a "Secure Smart City." A smart city's urban safety ecosystem of residents might entail

several scenarios and risks, such as terrorism, crime, weather-related incidents, and natural catastrophes, making it difficult to maintain security. Therefore, from a security perspective, a smart city design must have procedures and tools that safeguard residents. A smart city is an IoT-connected community that provides users with safety, healthcare, convenience, a higher standard of life, etc. [1, 2]. Smart city technologies can potentially make human lives and residential care easier and more enjoyable [3]. They provide helpful capabilities such as tracking habits and security evaluations, which have sparked the interest of consumers and IoT device manufacturers [4]. Even though smart cities provide several benefits to householders and potential investors, there are many possibilities of cyber-attacks that might threaten consumers' security and privacy [5]. As a result, the adaptability and scalability necessary for efficient implementation in the novel field of autonomous smart city technologies and amenities are absent [6,7].

Furthermore, blockchain has demonstrated exceptional performance as a backbone of cybersecurity architecture across many smart city technologies, such as IoT communication and data transfer [8]. Blockchain technology and integrated storage platforms may be utilized to overcome security issues in smart city infrastructures [9]. Blockchain is a hyperlinked collection of malice-proof documents managed by a group of autonomous systems. Blockchain technology is built on the principles of rigidity [10], autonomy [11], and accessibility [12]. The three functionalities of blockchain technology have opened their horizons to various application fields, including the essence of digital currency and the viability assessment of intelligent operating systems. In contrast, blockchain technology ensures safety [13, 14].

The hybrid architecture could be used for attack activity because earlier techniques identify configurations using a signature-based mechanism and data stream analysis [15, 16]. As a result, it is critical to managing intelligent blockchain-based systems by building strong and adaptable algorithms to analyze massive quantities of generated data [17]. Deep learning includes using devices for learning, reasoning, and operation without human involvement [18]. It is an Artificial Intelligence (AI) platform [19]. The fundamental objective of deep learning is to develop an efficient algorithm that can take information from the inputs and forecast and modify the outcomes using mathematical techniques [20, 21] due to the number of additional layers applied to the data to learn from it. If you are unaware, a deep learning model updates the weights using an

optimization function when it learns. The outcomes help us comprehend how the input factors affect the time series predictions. Future predictive models could be improved using these findings.

According to the preceding discussion, the advancement of DL and blockchain-based mechanisms may be integrated to address computational intelligence and security issues on the internet of things-enabled smart city infrastructure [22]. Additionally, fog and edge computation may process information closer to the data stream than the cloud platform, which can assist in circumventing bandwidth and compute restrictions and high latency issues [23, 24]. The operational insights enabled by fog and edge cloud applications improve the capacity to translate huge data at static and data in movement into immediate processes [25]. This research presents a secure smart city infrastructure using blockchain and deep learning (SSCI-BDL) framework to ensure privacy protection and trustworthiness among IoT communication in smart cities. This framework involves the blockchain network for security management in the smart city infrastructure. Based on the objective of the proposed study and problem definition identified in the special issue scope, various literature reviews are done in the background from which the solution for challenges are given in this manuscript using the proposed SSCI-BDL framework. The major research contributions of the study are listed as follows.

1. The architecture and function features of the proposed framework in ensuring the security aspects of the smart city are detailed.
2. An introduction to how blockchain and deep learning techniques are integrated into the security aspects of smart cities with the developed framework.
3. The developed numerical equation for security aspects of the smart city using the SSCI-BDL framework

The rest of this work is organized as follows. Background studies, another name for the literature review, are detailed in Section 2. The architecture and function features of the proposed framework are discussed in Section 3. The integration of blockchain and deep learning techniques is discussed in Section 4. Section 5 details the numerical computations. Section 6 discusses the experimentation outcomes, and Section 7 concludes the research with major findings.

Background Study

Deep learning is a branch of computer science that focuses on developing systems that train through learning [26, 27]. It is the capacity to educate a machine without directly coding it. Deep learning incorporates work from various fields, including metaphysics [28], evolutionary computation [29], pattern recognition [30], signal processing [31], psychology and neuroscience [32], computational diversity [33], and machine intelligence [34]. Blockchains are irreversible collections of records that are algorithmically linked together for auditing purposes [35]. It is analogous to an accounting book. Blockchain is a hyperlinked collection of malice-proof documents managed by a group of autonomous systems [36]. Blockchain technology is built on the principles of rigidity, autonomy, and accessibility. This research examines the effects of ethics and technology on the security of IoT-enabled systems in smart city infrastructure. This section significantly discusses the previous study's contributions to securing the IoT-enabled smart city infrastructure using a hybrid framework.

Cha J et al. [37] suggested a consumer-centric blockchain architecture (CCBA) to secure the sharing of edge data in IoT. They reported that security and privacy are key problems due to substantial data development. Data leaks and thefts are possible, including personal and confidential data, medical data, and business data. Due to safety and privacy issues, several important complications in community trust, personal security, monetary penalties, and customer confidence can occur.

Aujla GS et al. [38] presented a software-based blockchain framework (SBBF) for understanding complicated blockchain topologies. They built a consensus mechanism solution for virtual servers using the conscious application framework, generating and managing particular consensus utilities. Even though the developed system has several benefits to consumers and potential investors, there are many possibilities of cyber-attacks that might threaten consumers' security and privacy.

Rathore S and Park JH [39] suggested a cryptographic crowd-intelligence network (CCIN) decrease congestion problems. However, these studies only examine blockchain as an interface system on top of the IoT environment, resulting in unsatisfactory throughput. Moreover, these methodologies rely on static optimization methods, which cannot define the long-term effectiveness of cognitive offloading. As a result, their approaches cannot be used in real-world dynamic situations.

Singh M et al. [40] utilized an advanced deep learning algorithm (ADLA) to analyze data streams to detect breaches and attack activities. As a result, it is critical to manage intelligent blockchain-based systems by building strong and adaptable algorithms to analyze massive quantities of generated data. Deep learning includes using devices for learning, reasoning, and operation without human involvement.

As a result of the literature study, this study will use a hybrid framework approach to secure smart cities by incorporating IoT sensors and continuous improvement. The primary contributions of this research are to give a complete overview of state-of-art innovations relevant to blockchain-based smart cities enabled by Deep Learning and offer a new perspective on numerous applications, which is supported by the most recent phases of technological progress [41]. This research presents a secure smart city infrastructure using blockchain and deep learning (SSCI-BDL) framework to ensure privacy protection and trustworthiness among IoT communication in smart cities. This framework integrates the deep learning model with an optimization algorithm that maintains efficient resource utilization in the smart city infrastructure.

Vinayakumar et al. (2020) developed a botnet detection system that was built on a two-level deep learning architecture [42]. The goal of this system was to differentiate botnets from authorised behaviours at the application layer of the Domain Name System (DNS). Siamese networks are employed at the first level of the system to determine how similar DNS requests are based on a threshold that has previously been set. This determination is made using the threshold. This assists in selecting the DNS information that shows up across Ethernet connections the most frequently. It is suggested that for the second level of the framework, a domain generation approach that is based on deep learning architectures be used to sort typical domain names from unusual ones. This would be done in order to complete the framework. The findings of the trial demonstrated that all aspects of the test, including the F1 score, the speed of detection, and the amount of false alarms, had improved.

A DL-based botnet detection method that makes use of network traffic flows was proposed by Sriram et al. (2020). [43] The botnet detection system first gathers network traffic flows, then converts those flows into connection data, and finally utilises a DL model to identify assaults that originate from hijacked Internet of Things devices. Many different tests are performed on benchmark data sets that are either well-known or brand new in order to find the optimal DL

model. The characteristics of the dataset are presented in a manner that makes it simpler for the reader to comprehend them. The conventional ML models were not as successful as the newly developed DL model.

A binary file byte sequence for the Executable and Linkable Format was proposed by Chaganti et al. in 2022. (ELF, formerly called Extensible Linking Format). Using input features, the Bidirectional-Gated Recurrent Unit-Convolutional Neural Network (Bi-GRU-CNN) model for IoT malware detection and classification was developed [44]. In addition, we investigate the detection and classification performance of IoT malware using RNN-based DL model combinations. There is also a comparison between their performance and that of the suggested approach. According to our evaluation of the effectiveness of our suggested strategy, it has a 100% accuracy rate for identifying IoT malware and a 98% accuracy rate for categorising IoT malware by family.

Secured smart city infrastructure using blockchain and deep learning (SSCI-BDL) framework

The main problem definition chosen for this work is because several potential IoT application areas are undiscovered or lack enough direction to approach them. More thorough research in this challenging area is necessary to develop new and major potential benefits for society. Although there are many benefits for citizens and capital providers in smart cities, there are several ways that security flaws could jeopardize people's safety and security. A formal system model is given to guarantee privacy protection and reliability among IoT connectivity in smart cities. A Secure Smart City Infrastructure using Blockchain and Deep Learning (SSCI-BDL) framework has been developed.

As a result, several different recommendation designs can coexist in the internet of things (IoT). This research examines the effects of ethics and technology on the security of IoT-enabled systems in smart city infrastructure. Figure 1 illustrates the secured smart city infrastructure using blockchain and deep learning (SSCI-BDL) framework to ensure privacy protection and trustworthiness among IoT communication in smart cities.

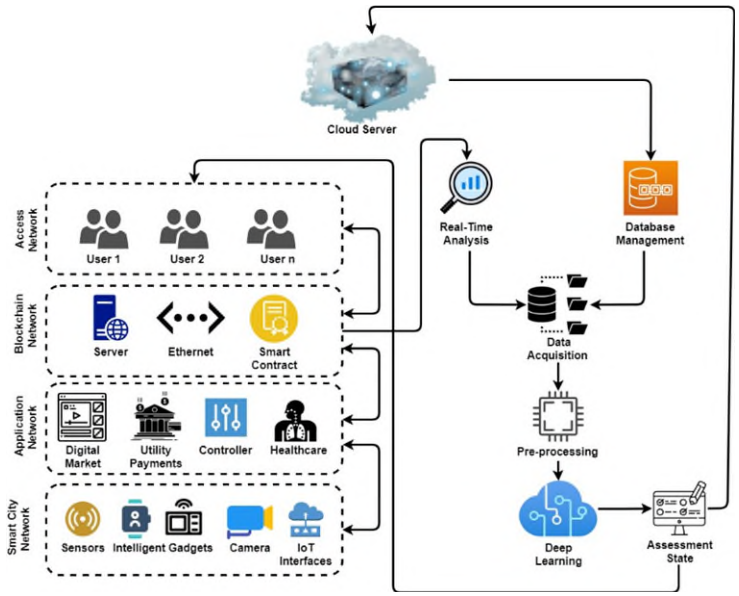

Figure 1. Proposed SSCI-BDL framework

The smart city network collects data from multiple sources, including sensors, intelligent gadgets, cameras, and IoT interfaces. The data collected by such intelligent systems are evaluated and interpreted in the application network. Application network includes utility payments, digital market, controller, and healthcare. The blockchain network plays a significant role in data communication through servers, ethernet, and smart contracts. The hybrid framework will subsequently be utilized in such systems to analyze and forecast data (database management and real-time analysis). The hybrid framework's databases could be handled in a blockchain network, minimizing data mistakes such as duplication, data loss, inaccuracies, and interruption. Blockchains' operation depends on the collected information. Thus, information issues in the hybrid framework will be avoided. Instead of the complete gathering of databases, the hybrid framework can be concentrated on particular blockchain parts. The algorithm will give an exclusive framework for various applications, including identifying fraud and forecasting data theft recognition. The performance of the SSCI-BDL framework was at its highest, and the latency rate for various fog nodes and simulation results was minimized. In this article, the term "latency rate" refers to the time it takes a data packet to move between two network nodes.

The SSCI-BDL framework can anticipate health issues, energy usage, transportation, traffic management, etc. Because the SSCI-BDL framework learns rapidly and is effective in

operational convolution, it can be widely employed in many areas for categorization and prediction purposes. The deep learning device is a feedforward learning algorithm, which implies that information moves only one way through a sequence of network layers; however, in this developed framework, the backpropagation strategy is applied in the learning phase. In which data travels backward through the network, and the learning algorithm modifies the weight values to accomplish high precision with the lowest error range. The network's parameters remain stable throughout the evaluation stages, in which the training model is extracted to predict the real-time data. The suggested SSCI-BDL method comprises three nodes: input nodes, hidden nodes, and outcome nodes. The machine learning technique uses a single hidden node and numerous neurons to prepare the dataset. Still, in a deep learning technique, several hidden nodes have a fixed set of neurons to enhance the network's performance.

Integration of Blockchain and Deep Learning Techniques – A Hybrid Framework

The IoT communication layer collects data from sensors critical for assessing the smart city environment, surroundings, and people. Sensors, digital media, and healthcare monitoring devices are the three main categories of such equipment. Sensors are utilized to compute environmental conditions. For example, the thermostat is used to measure and maintain the temperature of a room. The IoT monitoring network includes monitoring sensors, wearables, and CCTV cameras in a blockchain layer. Data from these networks is gathered and maintained on a centralized database named a blockchain, which serves as the stack's initial interface.

The SSCI-BDL method can be used to improve the intelligence of blockchain-enabled application systems. The use of SSCI-BDL for blockchain technology security can be enhanced. SSCI-BDL can also shorten the time necessary to gain comprehension by improving information exchange pathways. It also offers the opportunity to design better frameworks by leveraging the controlled architecture of the blockchain platform. The intelligent system collects data from multiple sources, including sensors, intelligent gadgets, and IoT interfaces. The data collected by such intelligent systems are evaluated and interpreted. The blockchain network performs a significant role in data communication.

The intelligent system gathers information from various devices, including sensors, smart devices, and IoT interfaces. These intelligent systems analyze and interpret the data they acquire.

Information errors such as duplication, missing input data, imperfections, and noise are reduced. Data issues can be reduced in the SSCI-BDL method because data is dispersed on a blockchain. Regardless of the actual data, the SSCI-BDL architecture can be tailored to concentrate on particular parts of the blockchain. It is possible for it to incorporate a specific framework for a variety of applications, such as the identification of data theft protection or the detection of fraud. The blockchain infrastructure is built on the cutting edge of IoT technology, and it consists of three essential components: a blockchain interface design, a consensus mechanism, and deep learning.

The suggested SSCI-BDL architecture employs huge volumes of hidden nodes, neurons, and several triggering mechanisms to increase the privacy and security of a smart city. The proposed approach is divided into three layers: data gathering, preparation, and assessment. The assessment layer has two sub-layers: forecasting and execution analysis. The gathered data is sent into the gathering layer as an entry. Specific information cleansing and preparation methods have been implemented to eliminate discrepancies in the preparation layer. The SSCI-BDL was used to improve smart city communication in any harmful or invasive behavior in the application interface.

A database server system may be viewed as a digger, verifying new transactions and adding new blocks. Still, smart contracts adhere to preset regulations to make autonomous transactions easier and faster. Other methods include public, corporate, and collaborative blockchains, but in a modern city network, the generally separately owned blockchain is utilized to save overhead expenses. Figure 2 illustrates the proposed hybrid framework.

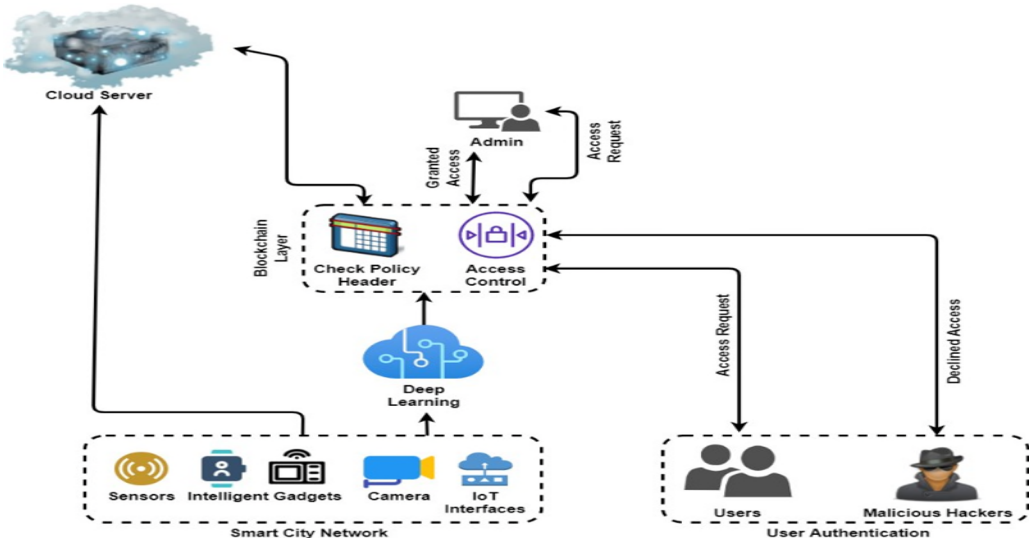

Figure 2. Proposed hybrid framework

The application node is designed to facilitate the integration of existing blockchain platforms with specialized smart city applications. This framework addresses smart home capabilities such as e-commerce, authentication protocols, house and healthcare connectivity, and the automated payments of smart support functions. Finally, the network infrastructure is at the top of the Structure. It allows service providers, such as smart grids, retail stores, utility suppliers, enterprises, and so on, to benefit from blockchain-based smart city technology.

The introduction of smart gadgets cleared the door for innovative Internet of Things (IoT) techniques to dynamically and economically operate smart household systems. Sensors, CCTV, intelligent television, fitness gadgets, mobile phones, and controllers are the primary components of an improved smart city ecosystem. A smart city with IoT devices provides various services such as remote monitoring, signal activation, safety monitoring, etc. To improve the smooth functioning of the smart city and identify harmful actions by attackers, a tailored network management device provides a warning signal to the smart city community. Cloud servers provide globally distributed, scalable, and cost-effective computing resources to support the unprecedented amounts of data that are being collected, while blockchain technology acts as the trusted, decentralised source of truth to enable analytics and decision-making from the data gathered.

As illustrated in Figure 2. the user must determine their degree of accessibility and deploy it to the home care device. Concerning figure 2, the user's level of accessibility is given as follows: the admin receives each user's request and has the option of accepting or rejecting it. It is essential to have access to home care services of a high quality in order to promote and maintain health, prevent and treat disease, and reduce unnecessary disability and premature mortality. These goals can be accomplished by providing structure and organisation, as well as headers containing information about the situation.

For instance, the house owner (Admin) is given approval at the highest level, whilst teens, kids, visiting relatives, and teenagers must request clearance at the intermediate level. The control permissions for outsiders and neighbouring people are practically nonexistent. After receiving a response from the user, the home server conducts an investigation into the directory of network security. After that, the house server will transmit this command to the blockchain network in order to obtain legal authorization for the particular user. The permissions for a large number of users and devices are stored in the blockchain strategy header. A block data segment that is used for

carrying out policy actions and procedures is referred to as the strategy header. The request made by the individual user is sent to the admin, who has the ability to accept or reject any request made by a user. After the administrator has either granted or denied authorization, blockchain diggers will enter the header's policies and begin conducting activities. This method is helpful for warding from criminal hackers. With user authentication, humans and computers can exchange credentials during network transactions to verify each other's identities. This process ensures the legitimacy of a user before granting them access to a system or network.

SSCI-BDL Framework

The categorized features with N data integration sequences $F = \{p_{u,v}, q_u\}_{u=1}^{N}$, whereas $p_{u,v} = (e_{u,v}, f_{u,v})$ is a multimodel series of extracted data $(e_{u,v} \in E^{ne*T})$ and integrated data $(f_{u,v} \in E^{bf*T})$ of span T with $v = 1,2, \dots, T$. The way of extracting to predict the real-time data in the evaluation stage can be explained as multimodel series of extracted data $(e_{u,v} \in E^{ne*T})$ and integrated data $(f_{u,v} \in E^{bf*T})$ of span T .Whereas, $p_{u,v}$ indicates the v state of the u integrated data series. Whereas q_u refers to the state label indicator in a signified state set β. It is important to recall that the proposed SSCI-BDL model relates to the probability matrix and that the possibility of the state label is expressed by Equation (1)

$$x(q|p; b) = \sum_h exp(E(q, h|p; b) - C(b)) \quad (1)$$

Whereas, $b = [\varphi, \mu]$ is a state vector, $h = \{h_1, h_2, \dots, h_T\}$, with $h_u \in I$ refers to latent parameters. The number of latent parameters, in common, differs from the state value, since h_v can relate to a structural variable in a state. But the same notation is utilized for convenience explains as since h_v can correspond to a structural variable in a state. The same notation is utilized for convenience in hidden layers h_l as denoted in equation 5

The formula $h = \{h_1, h_2, \dots, h_T\}$, where $h_u \in I$ denotes latent parameters. Since h_v can correspond to a structural variable in a state, the number of latent parameters common to all of them differs from the state value. Equation 2, the relation to a structural variable is given as h. $E(q, h|p; b)$ identified as stability vector and $C(b)$ refers to a log partition to express the normalization function as expressed in equation (2)

$$C(b) \log \sum_{q'} \sum_{h} exp\ (E(q', h|p; b)) \quad (2)$$

In common, the probability is acceptable for each potential formation of individual and pair states as expressed in equation (3)

$$E(q, h|p; b) = \sum_{l \in s} \sum_{o} \mathrm{P}_o(q, h_l, p; \varphi_o) + \sum_{l,p \in \rho} \sum_{o} \delta_o\ (q, h_l, h_p; \omega_o) \quad (3)$$

Where the variables φ and ω represents scaler and vector nodes required to be expressed in potential formation, and $\mathrm{P}_o(q,\ h_l,\ p;\ \varphi_o)$, $\delta_o(q,\ h_l,\ h_p;\ \omega_o)$ represents scaler and vector factors. The scaler factor expressed in equation (4)

$$\mathrm{P}_o(q, h_l, p; \varphi_o) = \sum_{l} \theta_{1,o}\ (q, h_l; \varphi_{1,o}) + \sum_{k} \theta_{2,o}\ (q, h_l; \varphi_{2,o}) \quad (4)$$

It can also be identified as a stability function integrated with two functions. The role of the state is to model the interconnection of the label q with the hidden layer h_l is denoted in equation (5)

$$\theta_{1,o}(q, h_l; \varphi_{1,o}) = \sum_{\alpha \in \beta} \sum_{\gamma = I} \varphi_{1,o}\ \partial(q = \alpha)\partial(h_l = \gamma) \quad (5)$$

Where an identification variable for the connection used in modeling the function is given as ∂.

If its dispute is valid, it equals 1; otherwise, 0. The indication feature modeling is the interconnection between the hidden layers h_l and interaction p, expressed in equation (6)

$$\theta_{2,O}(q, h_l; \varphi_{2,o}) = \sum_{\gamma = I} \varphi_{2,o} \partial\ (h_l = \gamma)p \quad (6)$$

The vector factors is an intermediate feature and indicate the interaction between a pair of covert related hidden layers h_l and h_p as expressed in equation (7)

$$\delta_o(q, h_l, h_p; \omega_o) = \sum_{\substack{\alpha \in \beta \\ \mu, \gamma = I}} \omega_o \partial(q = \alpha)\partial(h_l = \mu)\partial(\ h_p = \gamma) \quad (7)$$

Based on the outcome observed from the above mathematical formulations, the hybrid framework (integrated blockchain and deep learning) could be utilized to analyze data streams to detect breaches and attack activities. As a result, it is critical to manage intelligent blockchain-based systems by building strong and adaptable algorithms to analyze massive quantities of generated data. Deep learning includes using devices for learning, reasoning, and operation without human involvement. The fundamental objective of deep learning is to develop an efficient

algorithm that can take information from the inputs and forecast and modify the outcomes using mathematical techniques.

The advancement of deep learning and blockchain-based mechanisms are integrated to address computational intelligence and security issues on the internet of things-enabled smart city infrastructure. Additionally, fog and edge computation may process information closer to the data stream than the cloud platform, which can assist in circumventing bandwidth and compute restrictions and high latency issues. The operational insights enabled by fog and edge cloud applications improve the capacity to translate huge data at static and data in movement into immediate processes. This study developed a secure smart city infrastructure using blockchain and deep learning (SSCI-BDL) framework to ensure privacy protection and trustworthiness among IoT communication in smart cities. This framework involves the blockchain network for security management in the smart city infrastructure.

Experimental Outcomes and Discussions

This section discusses the significant functionality of the developed secure smart city infrastructure using blockchain and deep learning (SSCI-BDL) framework over conventional smart city security. Strategies like consumer-centric blockchain architecture (CCBA), software-based blockchain framework (SBBF), cryptographic crowd-intelligence Network (CCIN), and advanced deep learning algorithm (ADLA). This study obtains smart city security data from 24 fog nodes. As shown in Figure 2, the developed framework (SSCI-BDL) ensures privacy protection and trustworthiness among IoT communication in smart cities. This framework involves the blockchain network for security management in the smart city infrastructure. This framework integrates the deep learning model with an optimization algorithm that maintains efficient resource utilization in the smart city infrastructure.

In addition to this, the framework that was designed makes use of the computational technique in order to achieve the 16 results of the simulation. The data server has the capacity to store 2 terabytes of data and has a synthesis speed of 2.4 gigahertz. It is utilised for the functions of data mining, synthesis, and storage. The distributed ledger technology (Blockchain) and integrated storage systems are two potential solutions to the security challenges faced by smart city infrastructures. A blockchain is a distributed, hyperlinked ledger that stores records that are

immune to tampering and are controlled by a network of self-governing computers. The underlying architecture of blockchain technology is based on the tenets of rigidity, autonomy, and accessibility. The accuracy, efficiency, security rate, and latency rate are some of the quality indicators that are utilised in the process of evaluating the simulation results produced by the established framework. Using the developed framework (SSCI-BDL), a comparative analysis is performed on conventional smart city security strategies such as CCBA, SBBF, CCIN, and ADLA in order to evaluate the privacy protection and trustworthiness among IoT communication in smart cities. This is done in order to evaluate the privacy protection and trustworthiness among IoT communication in smart cities.

Accuracy Analysis

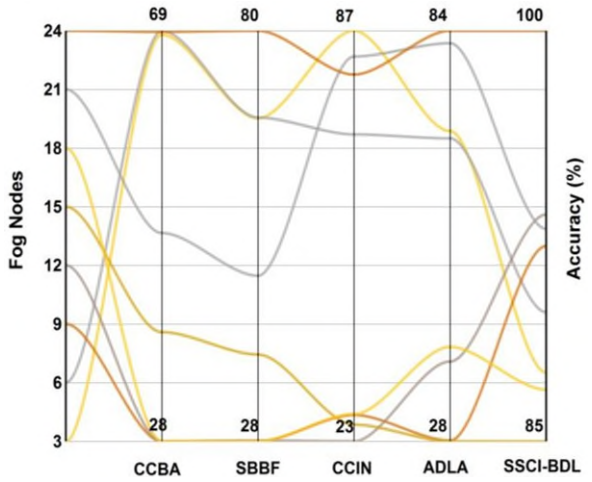

Figure 3. Accuracy

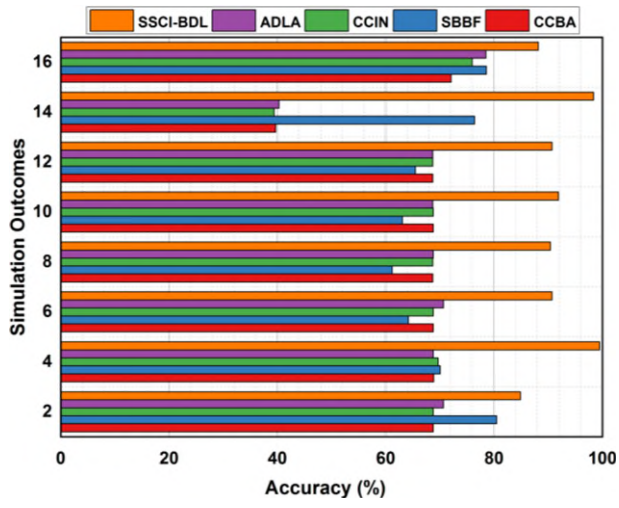

Figure 4. Accuracy

(Fog Nodes) (Simulation Outcomes)

The developed framework accuracy significantly improved for varying fog nodes and simulation outcomes, as illustrated in Figures 3 and 4. Here, the starting state obtains the information from the IoT sensor and studies whether the state is either steady or unsteady. Based on this investigation state, the accuracy range is enhanced, and this information is linked with the IoT sensor data. If there is any unethical activity is identified, the warning signal is sent to the smart city community people, and it is expressed as $F = \{p_{u,v}\ , q_i\}_{u=1}^{N}$. The information will be transferred from the fog nodes to the IoT cloud platform. The outcome is represented as a warning signal. This warning signal is sent on the plan, and the information relates to the state of synchronizing the historical data. This match state is directed at the integrated blockchain and deep learning framework, distinguishing individuals' behavioral movements in smart cities. The number of data gathered from IoT sensor devices is interconnected with classifying steady or unsteady activity. Improved accuracy over a wider range and the ability to accurately identify human activities are highlighted in this assessment. If the people's behavior is studied, the warning signal is not transferred; otherwise, it is transferred. The tracking states are utilized to identify the condition's state to detect the outcomes realistically.

Efficiency Aspects

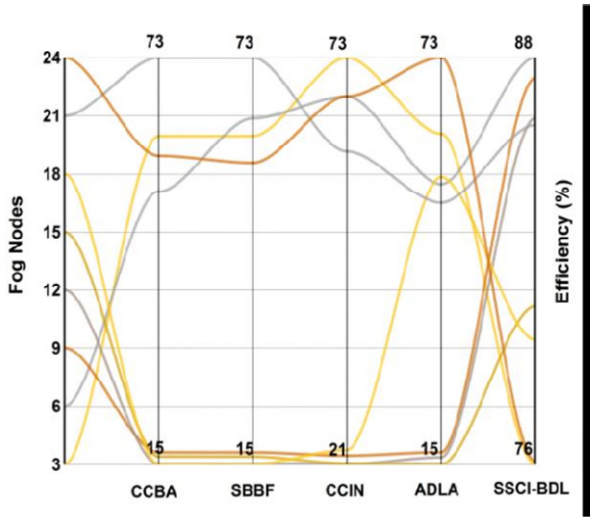

Figure 5 Efficiency (Fog Nodes)

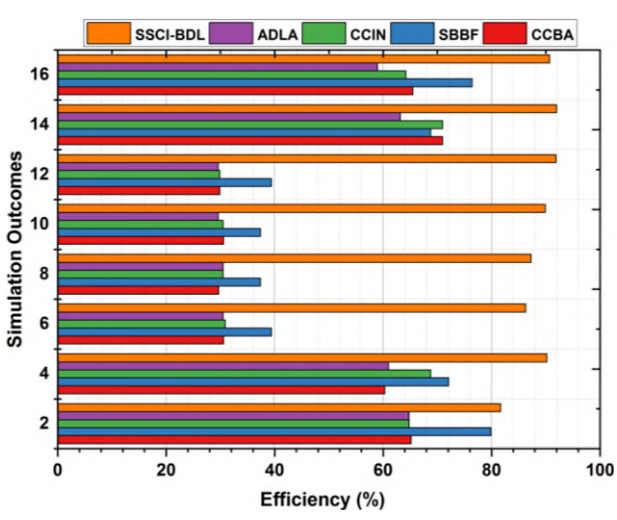

Figure 6. Efficiency (Simulation Outcomes)

The optimization algorithm aims to provide the "optimal" design about a list of constraints or priorities using efficiency ratio calculation. These include maximizing elements like output and system efficiency. This results in an improved efficiency ratio, which is written as $P_o(q,\ h_l,\ p;\ \varphi_o)$, and is carried out through an identification state using an optimization algorithm. The efficiency ratio improved for varying fog nodes and the simulation outcomes, as illustrated in Figures 5 and 6. If the smart city community people's activity is unsteady, the information developed from IoT sensors matches the fault values in the data center. Whereas the data is studied, the indication is carried out as the warning signal. In this way, the efficiency ratio is enhanced, and it is expressed as $P_o(q,\ h_l,\ p;\ \varphi_o)$, it is performed through an identification state. The divergence between the study and unsteady data is observed at a short processing range, and the results are calculated in real-time. The outcome is therefore decided to human activity emergency state and ambiguity. Data are traced intermittently, and consistency and instability are measured during data processing. The facility is done in real-time in this evaluation phase and is interconnected to the constant processing of outcomes. The historical state mapping and information synthesis were performed using the health monitoring system. The efficiency ratio is interconnected to the mapping technique for the strategic effort. The fog nodes are utilized to transfer data and develop realistic outcomes on the IoT network. Thus, fog nodes grasp the user request and their behavior and develop a stronger warning signal.

Security Rate

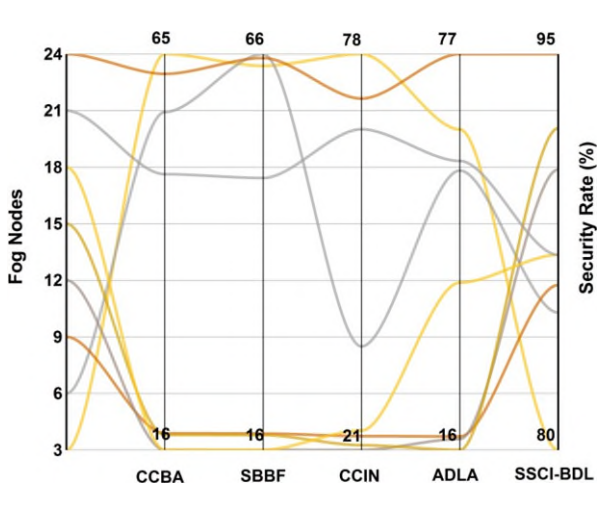

Figure 7. Security Rate

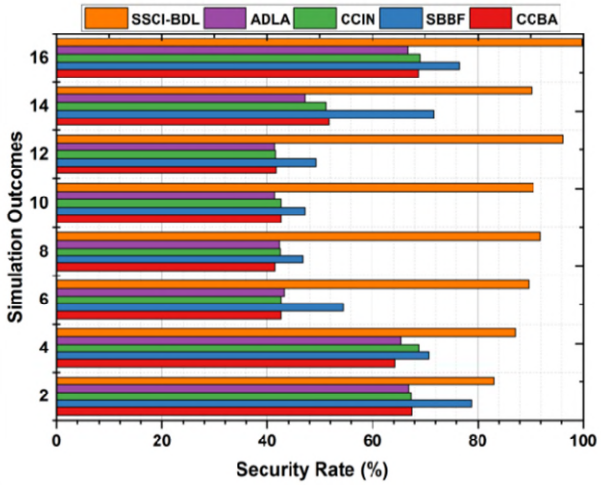

Figure 8. Security Rate

(Fog Nodes) (Simulation Outcomes)

The security rate for varying fog nodes and simulation outcomes for the developed framework and variation in smart city security infrastructures are illustrated in Figures 7 and 8. The information is transferred to the fog nodes and regulates the mapping variable with the predicted model as computed as $\sum_{\gamma=l}\ \varphi_{2,o}\partial\ (h_l\ =\ \gamma)p$. The information is categorized as study and unstudy, and the prediction is concentrated by mapping. The predicted model is compared to the historical processing state and indicates the truncated cost to trace activity. The service outcome is sent on a schedule, and it causes a higher level of accuracy. The developed framework enhances the security rate for several IoT sensing devices with an improvement in accuracy. The developed framework forms the IoT network; the information is obtained, linked, and utilized for data identification and simulation outcomes. The user request is in this processing state as an emergency, and the response from the admin is given immediately.

Latency Rate Analysis

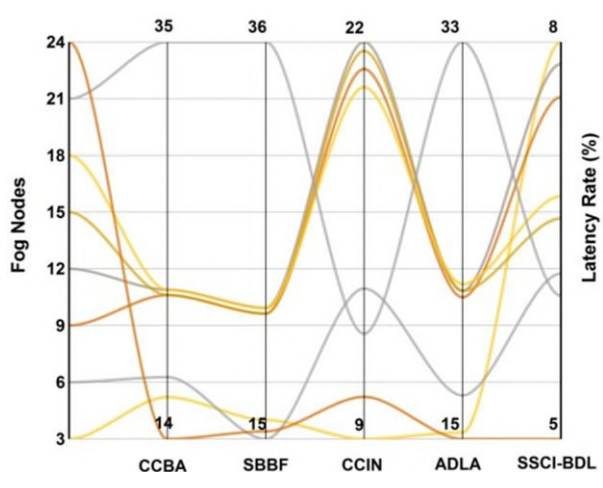

Figure 9. Latency Rate (Fog Nodes)

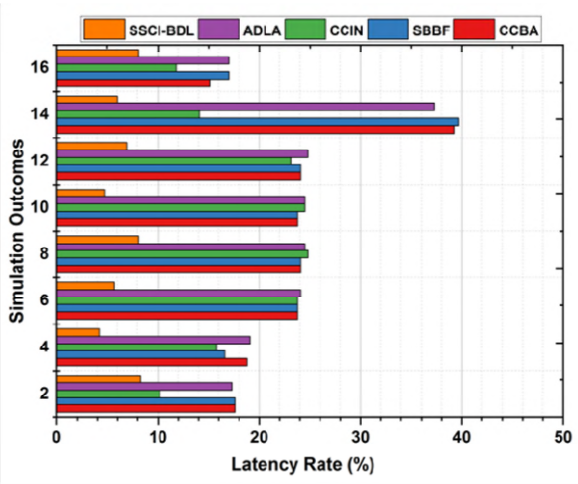

Figure 10. Latency Rate (Simulation Outcomes)

The latency rate for varying fog nodes and simulation outcomes were decreased and showed optimal performances than the conventional smart city security strategies like CCBA, SBBF, CCIN, and ADLA, as illustrated in Figures 9 and 10. The usage of the information is identified from the historical state and developed the improved performance denoted

as $\sum_{\mu,\gamma=I}^{\alpha\in\beta} \omega_o \partial(q=\alpha)\partial(h_l=\mu)\partial(h_p=\gamma)$. Collected information is utilized through the opinion from biometric signals and user requests. The decay rate for various fog nodes and simulation results was reduced, and performance was at its best in the SSCI-BDL framework. This manuscript's latency rate describes the time it takes a data packet to travel from one network node to another. Here, several IoT sensors are utilized, exploring a neighboring state is uninterruptedly performed, and the outcomes are stored. The fog nodes' data are utilized to forecast data for interconnection with the historical state. The user behavior is identified realistically for this utilization of collected data. This work utilized the input system reference state. According to the preceding discussion, the advancement of DL and blockchain-based mechanisms may be integrated to address computational intelligence and security issues on the internet of things-enabled smart city infrastructure. This research presents a secure smart city infrastructure using blockchain and deep learning (SSCI-BDL) framework to ensure privacy protection and trustworthiness among IoT communication in smart cities. This framework involves the blockchain network for security management in the smart city infrastructure. The comparison outcomes are given in Tables 1 and 2.

Table 1 Comparison outcomes for fog nodes

Quality Indicators	CCBA	SBBF	CCIN	ADLA	SSCI-BDL
Accuracy (%)	68.9	78.9	87.1	83.9	99.7
Efficiency (%)	72.9	74.1	73.2	71.9	88.3
Security Rate (%)	64.8	64.9	76.9	76.3	95.2
Latency Rate (%)	12.6	15.1	8.9	14.8	4.3

Table (1) expresses the developed framework's quality indicators outcomes (SSCI-BDL) relative to the conventional smart city security strategies for fog nodes. The developed framework

(SSCI-BDL) provides improved outcomes in all quality indicators with conventional smart city security strategies like CCBA, SBBF, CCIN, and ADLA. Comparative investigation developed framework with conventional approaches, the developed framework provides efficiency, optimal accuracy, security rate, and latency by 17.44%, 30.89%, 31.93% & 70.94%, respectively.

Table 2 Comparison outcomes for simulation outcomes

Quality Indicators	CCBA	SBBF	CCIN	ADLA	SSCI-BDL
Accuracy (%)	71.0	81.1	75.3	77.9	99.6
Efficiency (%)	64.8	80.1	72.0	63.7	99.8
Security Rate (%)	67.9	79.1	68.8	66.4	99.5
Latency Rate (%)	14.9	15.8	9.9	16.8	4.1

Table (2) express the quality indicators outcomes for the developed framework (SSCI-BDL) relative to the conventional smart city security strategies for simulation outcomes. The developed framework (SSCI-BDL) provides optimal accuracy, efficiency, security rate, and latency outcomes by 99.6%, 99.8%, 99.5%, and 4.1%. Simultaneously, the CCBA framework for simulation outcomes provides poor results. Comparative investigation developed framework with conventional approaches, the developed framework provides efficiency, optimal accuracy, security rate, and latency rate by 35.07%, 28.71%, 31.75% & 75.59%, respectively.

Conclusion

In this research, a secured smart city infrastructure using a blockchain and deep learning (SSCI-BDL) framework is developed to ensure privacy protection and trustworthiness among IoT communication in smart cities. According to the preceding discussion, advanced deep learning and blockchain-based mechanisms may be integrated to address computational intelligence and security issues on the internet of things-enabled smart city infrastructure. The operational insights

enabled by fog and edge cloud applications improve the capacity to translate huge data at static and data in movement into immediate processes. This framework integrates the deep learning model with an optimization algorithm that maintains efficient resource utilization in the smart city infrastructure. The simulation results show that the system has high security of 99.54% and the lowest latency of 0.13ms compared to existing models. Overall, the proposed framework's efficiency gives the highest rate of 99.89%. Future success of a smart city will require innovative solutions in six domains: environment and living and health, energy, safety and security, economy, governance and education, , and mobility.

References

[1] Singh SK, Jeong YS, Park JH. A deep learning-based IoT-oriented infrastructure for a secure smart city. Sustainable Cities and Society. 2020 Sep 1;60:102252.

[2] Peneti S, Kumar MS, Kallam S, Patan R, Bhaskar V, Ramachandran M. BDN-GWMNN: Internet of Things (IoT) Enabled Secure Smart City Applications. Wireless Personal Communications. 2021 Mar 12:1-7.

[3] Rathore S, Kwon BW, Park JH. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. Journal of Network and Computer Applications. 2019 Oct 1;143:167-77.

[4] Rahman MA, Rashid MM, Hossain MS, Hassanain E, Alhamid MF, Guizani M. Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city. IEEE Access. 2019 Jan 30;7:18611-21.

[5] Singh S, Sharma PK, Yoon B, Shojafar M, Cho GH, Ra IH. Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. Sustainable Cities and Society. 2020 Dec 1;63:102364.

[6] Nguyen TN, Zeadally S, Vuduthala A. Cyber-Physical Cloud Manufacturing Systems with Digital-Twins. IEEE Internet Computing. 2021 Feb 11.

[7] Karrupusamy P, Chen J, Shi Y. Sustainable communication networks and application. Lecture Notes on Data Engineering and Communications Technologies. 2020:65-72.

[8] Hu L, Nguyen NT, Tao W, Leu MC, Liu XF, Shahriar MR, Al Sunny SN. Modeling of cloud-based digital twins for smart manufacturing with MT connect. Procedia manufacturing. 2018 Jan 1;26:1193-203.

[9] Dash RK, Nguyen TN, Cengiz K, Sharma A. Fine-tuned support vector regression model for stock predictions. Neural Computing and Applications. 2021 Mar 15:1-5.

[10] Khan F, Jan MA, Rehman AU, Mastorakis S, Alazab M, Watters P. A Secured and Intelligent Communication Scheme for IIoT-enabled Pervasive Edge Computing. IEEE Transactions on Industrial Informatics. 2020 Nov 13.

[11] Yang S, Yin D, Song X, Dong X, Manogaran G, Mastorakis G, Mavromoustakis CX, Batalla JM. Security situation assessment for massive MIMO systems for 5G communications. Future Generation Computer Systems. 2019 Sep 1;98:25-34.

[12] Manogaran G, Alazab M, Shakeel PM, Hsu CH. Blockchain-assisted secure data sharing model for the Internet of Things-based smart industries. IEEE Transactions on Reliability. 2021 Feb 8.

[13] Khan F, Kumar RL, Kadry S, Nam Y, Meqdad MN. Cyber-physical systems: A smart city perspective. International Journal of Electrical & Computer Engineering (2088-8708). 2021 Aug 1;11(4).

[14] Jegadeesan S, Azees M, Kumar PM, Manogaran G, Chilamkurti N, Varatharajan R, Hsu CH. An efficient anonymous mutual authentication technique for providing secure communication in mobile cloud computing for smart city applications. Sustainable Cities and Society. 2019 Aug 1;49:101522.

[15] Ahmed SH, Bashir AK, Guibene W. Introduction to the special section on emerging technologies for connected vehicles and ITS networks. Computers & Electrical Engineering. 2019 Apr 11;75:309-11.

[16] Fang L, Yin C, Zhu J, Ge C, Tanveer M, Jolfaei A, Cao Z. Privacy protection for medical data sharing in smart healthcare. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM). 2020 Dec 16;16(3s):1-8.

[17] Zhang P, Pang X, Kibalya G, Kumar N, He S, Zhao B. GCMD: Genetic Correlation Multi-Domain Virtual Network Embedding Algorithm. IEEE Access. 2021 Apr 30;9:67167-75.

[18] Younan M, Houssein EH, Elhoseny M, Ali AE. Performance analysis for similarity data fusion model enables time-series indexing in the internet of things applications. PeerJ Computer Science. 2021 May 20;7:e500.

[19] Raza M, Kumar PM, Hung DV, Davis W, Nguyen H, Trestian R. A digital twin framework for Industry 4.0 enabling next-gen manufacturing. In2020 9th International Conference on Industrial Technology and Management (ICITM) 2020 Feb 11 (pp. 73-77). IEEE.

[20] Xu X, Chen Y, Zhang J, Chen Y, Anandhan P, Manickam A. A novel approach for scene classification from remote sensing images using deep learning methods. European Journal of Remote Sensing. 2020 Oct 8:1-3.

[21] Zhang R, Jackson Samuel RD. Fuzzy efficient energy smart home management system for renewable energy resources. Sustainability. 2020 Jan;12(8):3115.

[22] Xue K, Deng Y, Zhang H, Pandiyan S, Manickam A. Cycling environment investigation and optimization of the central urban road in Qingdao. Computational Intelligence. 2020 Jul 3.

[23] Muñoz-Araque DM, Garcia MH, Garcia PG, Montenegro C. Navigation of Resources from Tangible Object Recognition to Improve Virtual Tours in Botanical Gardens. International Conference on Information Technology & Systems 2020 Feb 5 (pp. 525-534). Springer, Cham.

[24] Thapliyal M, Ahuja NJ, Shankar A, Cheng X, Kumar M. A differentiated learning environment in domain model for learning disabled learners. Journal of Computing in Higher Education. 2021 May 10:1-23.

[25] Ramesh S, Yaashuwanth C, Muthukrishnan BA. Machine learning approach for secure communication in wireless video sensor networks against denial- of- service attacks. International Journal of Communication Systems. 2020 Aug;33(12):e4073.

[26] Gupta D, Rani S, Ahmed SH, Garg S, Piran MJ, Alrashoud M. ICN-Based Enhanced Cooperative Caching for Multimedia Streaming in Resource-Constrained Vehicular Environment. IEEE Transactions on Intelligent Transportation Systems. 2021 Jan 8.

[27] Srivastava AK, Grotjahn R, Ullrich PA. A Multimodel Technique for Estimating Future Changes in Extreme Precipitation. InAGU Fall Meeting Abstracts 2019 Dec (Vol. 2019, pp. A51Q-2832).

[28] Hammachukiattikul P, Sekar E, Tamilselvan A, Vadivel R, Gunasekaran N, Agarwal P. Comparative Study on Numerical Methods for Singularly Perturbed Advanced-Delay Differential Equations. Journal of Mathematics. 2021 Jun 4;2021.

[29] Abbas K, Tawalbeh LA, Rafiq A, Muthanna A, Elgendy IA, El-Latif A, Ahmed A. Convergence of Blockchain and IoT for Secure Transportation Systems in Smart Cities. Security and Communication Networks. 2021 Apr 27;2021.

[30] Abd El-Latif AA, Abd-El-Atty B, Mazurczyk W, Fung C, Venegas-Andraca SE. Secure data encryption based on quantum walks for 5G Internet of Things scenario. IEEE Transactions on Network and Service Management. 2020 Jan 28;17(1):118-31.

[31] Smys S, Wang H, Basar A. 5G Network Simulation in Smart Cities using Neural Network Algorithm. Journal of Artificial Intelligence. 2021;3(01):43-52.

[32] Lin X, Wu J, Mumtaz S, Garg S, Li J, Guizani M. Blockchain-based on-demand computing resource trading in IoV-assisted smart city. IEEE Transactions on Emerging Topics in Computing. 2020 Feb 6.

[33] Xiao W, Liu C, Wang H, Zhou M, Hossain MS, Alrashoud M, Muhammad G. Blockchain for Secure-GaS: Blockchain-powered Secure Natural Gas IoT System with AI-enabled Gas Prediction and Transaction in Smart City. IEEE Internet of Things Journal. 2020 Oct 6.

[34] Gumaei A, Al-Rakhami M, Hassan MM, Pace P, Alai G, Lin K, Fortino G. Deep learning and blockchain with edge computing for 5G-enabled drone identification and flight mode detection. IEEE Network. 2021 Feb 16;35(1):94-100.

[35] Qian Y, Jiang Y, Chen J, Zhang Y, Song J, Zhou M, Pustišek M. Towards decentralized IoT security enhancement: A blockchain approach. Computers & Electrical Engineering. 2018 Nov 1;72:266-73.

[36] Tanwar S, Bhatia Q, Patel P, Kumari A, Singh PK, Hong WC. Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward. IEEE Access. 2019 Dec 23;8:474-88.

[37] Cha J, Singh SK, Kim TW, Park JH. Blockchain-empowered cloud architecture based on secret sharing for a smart city. Journal of Information Security and Applications. 2021 Mar 1;57:102686.

[38] Aujla GS, Singh M, Bose A, Kumar N, Han G, Buyya R. Blocksdn: Blockchain-as-a-service for software-defined networking in smart city applications. IEEE Network. 2020 Apr 2;34(2):83-91.

[39] Rathore S, Park JH. A Blockchain-based Deep Learning Approach for Cyber Security in Next Generation Industrial Cyber-Physical Systems. IEEE Transactions on Industrial Informatics. 2020 Nov 26.

[40] Singh M, Aujla GS, Bali RS. A Deep Learning-Based Blockchain Mechanism for Secure Internet of Drones Environment. IEEE Transactions on Intelligent Transportation Systems. 2020 Jul 7.

[41] Wu H, Zhang Z, Guan C, Wolter K, Xu M. Collaborate edge and cloud computing with distributed deep learning for smart city internet of things. IEEE Internet of Things Journal. 2020 May 25;7(9):8099-110.

[42] Vinayakumar, R., Mamoun Alazab, Sriram Srinivasan, Quoc-Viet Pham, Soman Kotti Padannayil, and Ketha Simran. "A visualized botnet detection system based deep learning for the internet of things networks of smart cities." *IEEE Transactions on Industry Applications* 56, no. 4 (2020): 4436-4456.

[43] Sriram, S., R. Vinayakumar, Mamoun Alazab, and K. P. Soman. "Network flow-based IoT botnet attack detection using deep learning." In *IEEE INFOCOM 2020-IEEE conference on computer communications workshops (INFOCOM WKSHPS)*, pp. 189-194. IEEE, 2020.

[44] Chaganti, Rajasekhar, Vinayakumar Ravi, and Tuan D. Pham. "Deep learning based cross architecture internet of things malware detection and classification." *Computers & Security* 120 (2022): 102779.