Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2023 SCPE. Volume 24, Issues 3, pp. 561–584, DOI 10.12694/scpe.v24i3.2272

PRIVACY AND SECURITY ENHANCEMENT OF SMART CITIES USING HYBRID DEEP LEARNING-ENABLED BLOCKCHAIN

JOSEPH BAMIDELE AWOTUNDE*, TAREK GABER†, L V NARASIMHA PRASAD‡, SAKINAT OLUWABUKONLA FOLORUNSO§ AND VUYYURU LAKSHMI LALITHA¶

Abstract. The emergence of the Internet of Things (IoT) accelerated the implementation of various smart city applications and initiatives. The rapid adoption of IoT-powered smart cities is faced by a number of security and privacy challenges that hindered their application in areas such as critical infrastructure. One of the most crucial elements of any smart city is safety. Without the right safeguards, bad actors can quickly exploit weak systems to access networks or sensitive data. Security issues are a big worry for smart cities in addition to safety issues. Smart cities become easy targets for attackers attempting to steal data or disrupt services if they are not adequately protected against cyberthreats like malware or distributed denial-of-service (DDoS) attacks. Therefore, in order to safeguard their systems from potential threats, businesses must employ strong security protocols including encryption, authentication, and access control measures. In order to ensure that their network traffic remains secure, organizations should implement powerful network firewalls and intrusion detection systems (IDS). This article proposes a blockchain-supported hybrid Convolutional Neural Network (CNN) with Kernel Principal Component Analysis (KPCA) to provide privacy and security for smart city users and systems. Blockchain is used to provide trust, and CNN enabled with KPCA is used for classifying threats. The proposed solution comprises three steps, preprocessing, feature selection, and classification. The standard features of the datasets used are converted to a numeric format during the preprocessing stage, and the result is sent to KPCA for feature extraction. Feature extraction reduces the dimensionality of relevant features before it passes the resulting dataset to the CNN to classify and detect malicious activities. Two prominent datasets namely ToN-IoT and BoT-IoT were used to measure the performance of this anticipated method compared to its best rivals in the literature. Experimental evaluation results show an improved performance in terms of threat prediction accuracy, and hence, increased security, privacy, and maintainability of IoT-enabled smart cities.

Key words: Blockchain, Deep Learning, Convolutional neural network, Principal Component Analysis, Privacy and security, Intrusion detection, Internet of Things, Sensor technology

AMS subject classifications. 68M12, 68T05

1. Introduction.

The increase in urbanization in recent years has demanded the economic, ecological, and social expansion of metropolises to improve one's quality of life meaningfully. This has brought about the introduction of the smart city concept to bring about development in urban cities. According to the United Nations assessment, by 2050, more than 70% of the world's population would be living in cities [1]. In various fields, like medicine, transport, teaching, budget, working conditions, and living environments, the development procedure has significantly enhanced people's living principles [2]. Nonetheless, the high density of the population poses significant hurdles in terms of distributing available resources using brand-new technologies. The swift growth of the urban population thus has an impact on eco-friendly reserve limitations like air smog, transportation jamming, garbage dumping, and greenhouse gas emissions. For cities' long-term development, all of these concerns and challenges necessitate innovative answers, bringing the notion of "Smart City", SC,

*Department of Computer Science, Faculty of Information and Communication Sciences, University of Ilorin, Ilorin 240003, Nigeria. Artificial Intelligent Systems Research Group (ArISRG), Department of Mathematical Sciences, Olabisi Onabanjo University, ago-iwoye, Nigeria (Corresponding author, awotunde.jb@unilorin.edu.ng)

†Faculty of Computers and Informatics, Suez Canal University, Ismailia 41522, Egypt. School of Science, Engineering, and Environment, University of Salford, Manchester M5 4WT, UK. (t.m.a.gaber@salford.ac.uk).

‡Department of CSE, Institute of Aeronautical Engineering, Hyderabad, India (lvnprasad@yahoo.com).

§Department of Mathematical Science, Olabisi Onabanjo University, Ago- Iwoye, 120107, Nigeria. Artificial Intelligent Systems Research Group (ArISRG), Department of Mathematical Sciences, Olabisi Onabanjo University, Ago-Iwoye, Nigeria (sakinat.folorunso@ oouagoiwoye.edu.ng).

¶Koneru Lakshmaiah Education Foundation, India. (Vlakshmilalitha@kluniversity.in).

into play [3, 4, 5].

Thus, the integration of the Internet of Things (IoT) and other tools have been used to resolve urban issues and problems [6, 7]. IoT-enabled applications are critical for making the best use of existing resources and technologies in the development of SCs. However, it has a single-point-of-failure problem that causes safety, confidentiality, latency, and reliability difficulties. Using IoT intelligent services provides chances to address the aforementioned difficulties and create a high-quality living. Due to qualities like transparency, trust-free, decentralization, and immutability. While providing high-quality services, blockchain tools can be utilized to address the aforementioned danger and privacy complications. Within today's (4G/5G) and next-generation (6G) wireless systems, IoT is likely to become the dominant trend in Internet and service-centric computing, which will play a large role in the next generation of sustainable smart cities.

Appropriate with larger collections of ecological, commercial, and community data conveyed via IoT, connectivity among resources in IoT-enabled SCs may be built and refined [8, 9, 10]. As a result, ecologically sustainable living and governance become a reality using the smart cities paradigm. One of the primary aiding tools for SC applications is the IoT which makes use of Internet technologies to connect smart devices and items [11, 13, 12]. In such an IoT model, data is acquired through a variety of physical devices, dispersed through wireless systems, and then handled in real time. Actuators are controlled using the data collected and processed [14]. As a result, in the comprehensive growth of IoT connectivity in smart cities, safety, secrecy, reliance, scalability, and centralization are all critical challenges that must be addressed [15, 16]. IoT systems, on the other hand, are highly dispersed and diverse, making them different from traditional systems.

The sole characteristics of IoT, computing power, memory volume, network bandwidth, and battery lifespan have made IoT security, privacy, and trust in SC design harder to maintain [17]. However, the interconnectedness of numerous IoT devices in smart systems creates a wide range of possible attacks aimed at IoT devices in SCs. The two main types of attacks in a smart city are cyber and physical. Physical attacks are launched using devices in the network where attackers can modify or temper the sensors and devices since the invaders are nearer to the devices [17, 18]. There are various attacks like Sleep Denial Attacks, malicious code injection, Permanent Denial of Service, radio frequency congestion, and false node injection in the smart city [19, 20]. In cyber-attacks, the attackers can inject malware or malicious software to gain illegal entrance to the structures of the network schemes [21].

Attacks like Ransomware, Denial-of-Service (DoS), Man-In-The-Middle, and Distributed Denial-of-Service (DDoS) are some examples of cyber-attacks targeting a smart city [22, 23]. Such attacks are becoming more common at an alarming rate, posing a threat to data security, reliability, and accessibility. Furthermore, the expanding privacy concerns include the vulnerability of sensitive data through inference and data-harming attacks, which can affect smart cities. For instance, attackers attempt to adjust IoT devices in data and inference poisoning attacks by adding made-up data measurements [24]. As a result, regular communications between smart things are hampered, and the power of smart devices is wasted [25]. Additionally, it is possible that such attacks could take a detrimental effect on the performance of data analysis systems that use machine learning (ML), e.g., intrusion detection systems (IDS).

As a result, privacy is critical in the operation of SCs and associated networks. The architecture encompassing security, privacy, and trust can be deemed a sufficient method to address the existing challenges. Hence, IoT-based SCs and their networks require a reliable and effective security system. To improve the eminence of the data in IoT-based systems, the use of redundant sensors has been generally adopted. On the other hand, the use of various sensors, reliable, unreliable, or corrupted, can provide many readings or observations of the same thing [26, 27]. Hence, it is expected that it is needed to deal with and find a permanent solution to those vulnerable and unreliable IoT nodes, thus providing reality and trust from unreliable results [28]. In the case of addressing such security issues, solutions could result in high computation costs of ML-based IDS models [29], privacy violations of Cloud-IoT applications [30], and/or a high false alarm rate of IDS models [31]. Therefore, it has become important to develop holistic smart cities that will maintain trustworthiness among IoT nodes.

Therefore, to overcome the aforementioned issues, this paper proposes a blockchain-enabled hybrid convolutional neural network CNN with Kernel Principal Component Analysis (KPCA) for the confidentiality security and privacy of SCs. Blockchain technology is a viable method to support cloud computing by making a distributed cloud for IoT-enabled smart cities. This will completely identify and measure the cloud infrastruc-

ture by managing the cloud and holding it responsible for its actions, and allow consumers of the IoT-enabled stage to confirm that the environment is working perfectly and in real-time.

This was achieved using a two-level security-preserving method. Blockchain technology is used at the first level for data authentication and for the prevention of captured data from poisoning attacks. The Kernel Principal Component Analysis (KPCA) method was used in the second phase for the choice of important characteristics and attributes from the datasets are transformed into an encoded format for preventing assumption attacks based on the deep learning technique used and improving the overall effectiveness of the proposed system. The obtained reduced features are used as an input to the CNN for the classification of normal and attack, and the blockchain is used for the authentication and privacy of the IIoT-based systems. Two prominent datasets namely ToN-IoT [32] and BoT-IoT [33, 34] were used to evaluate the security mechanism since both datasets have various IoT-based attacks like DoS, Ransomware, normal vectors, MITM, and Theft as mentioned earlier, and are publicly available [35].

The following are the study contributions:

(i) The paper proposed a privacy and trustworthy framework using blockchain technology to provide dependability within the device layer of IoT architecture, and KPCA was used for feature reduction with blockchain-based enabled Proof of Work (ePoW) for the protection of IoT-based systems from inference and poisoning attacks.

(ii) CNN was used for the classification of data for the detection of suspicious activities within the smart city networks.

(iii) The paper used blockchain-enabled to prevent the cloud database from the problems of redundancy in IIoT-based data using an on-chain technique called CloudBlock-EdgeBlock architecture to deploy the proposed system since it supports verifiability services, and traceability within IoT nodes in a smart city, timestamp records are generated for each transaction. The CloudBlock-EdgeBlock architecture was used to enhance blockchain-enabled on-chain devices in order to support indisputability, verifiability, and traceability by generating timestamp records for each transaction performed in the smart city within IIoT-based nodes. This was done to address the problems of Cloud-fog redundancy in IIoT data.

(iv) The proposed system efficiency is measured using F1-score, precision detection rate, and accuracy. Two publicly datasets BoT-IoT and BoT-IoT are used for the experimental performance and the results were compared with most recently related systems using non-blockchain and blockchain systems.

The remaining part of the paper is organized as follows: section 2 discussed the Blockchain-enabled AI in IoT-based Smart Cities. Section 3 presented the Artificial Intelligence enabled Intrusion Detection for IoT in Smart Cities. Section 4 reviewed related work in the areas of Blockchain, and applications of deep learning in smart cities. Section 5 presents the methodology employed in this study. Section 6 presented the experimental results and also discusses the performance analysis of the study. Finally, section 7 concluded the study with future and open research in the area.

2. The Blockchain-enabled with Artificial Intelligence in the Internet of Things for Smart Cities. In order to provide improved services to its citizens while ensuring effective and optimal use of available resources, for the combination and administration of physical, social, and corporate infrastructures, a smart city requires information technology [36]. The IoT is a concept that enables humans and devices to communicate via the internet. Smart houses, intelligent automobiles, smart industries, and smart transportation are among the equipment capable of intercommunication [37]. The IoT offers a variety of solutions for many fields, as depicted in fig.2.1, to help them maximize their output more effectively and efficiently. Despite its many benefits, IoT is plagued by challenges including data protection, centralized, data analytics, connectivity, and more technology limitations. In 2015, over 800,000 user devices were found to have been infected as a result of spam emails and distributed phishing [39].

The author in [36] claimed that as the quantity of smart devices grows, so does the amount of data created. As a result, big data analytics is an important consideration for any IoT application. Various studies contribute different solutions for IoT applications using technologies including Artificial Intelligence (AI) and Deep Learning (DL) to address this issue of data analytics [40]. The DL approach is utilized to evaluate massive volumes of data in order to provide information for outcome, forecasting, and categorization procedures. The

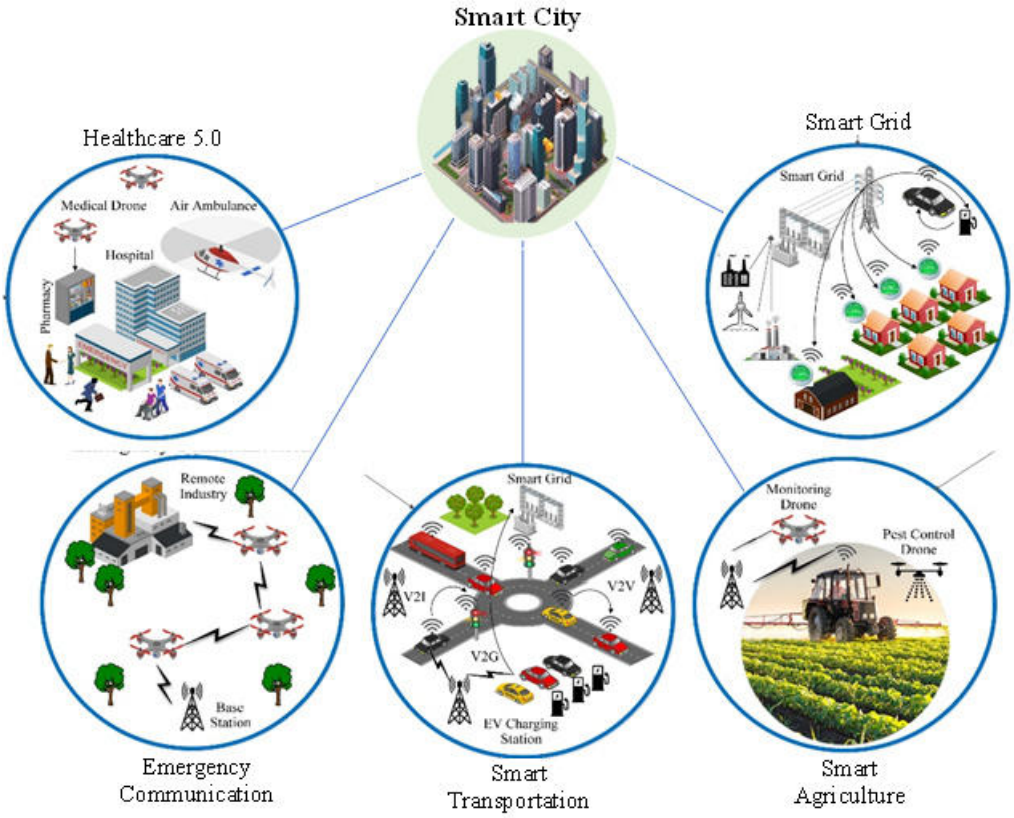

Fig. 2.1: Application-specific view of Smart Cities

DL analytics tool can extract and scale features from a large volume of data from IoT applications [41].

Blockchain technology creates a network that is decentralized, distributed, and secure. In blockchain tools, each node is linked in a decentralized peer-to-peer network, where each transaction is immediately transactions are shared without the use of timestamps and documented with timestamps influence. Agriculture, healthcare, security, and finance are all areas where the blockchain method might be beneficial. Through cryptographic hashing, the data provided in blocks is additionally involved and safeguarded in chains with digital signs. Because each block is connected to the one before it, hackers will be unable to hack transactions by injecting harmful data into the system. Digital signatures, validation, smart contracts, decentralization, and immutable explainable AI have all been handled by combining the blockchain approach with artificial intelligence for IoT frameworks. With the development of smart IoT devices and their interconnections, massive amounts of data are now being generated in a consolidated format.

As a result, technological advancements frequently generate difficulties such as space, security, and privacy. A decentralized database system is being constructed with the combination of blockchain and AI for IoT to address these challenges [42]. While sharing the transaction with anyone else on the network, it should be safe, digitally signed, verified, and transparent. A secure transaction model like this can be used in a variety of applications, including healthcare, smart homes, agriculture, military, industrial, smart transportation, and many more. [43]. For strengthening network security, blockchain equipment implements the concept of smart contracts, which are then kept in a digital ledger [44]. AI is used in a variety of advanced technology domains; decentralized AI, blockchain (BC), IoT intelligence, machine automation, and so on are only a few examples. The combination of AI and the IoT offers advantages in terms of data collection and processing [45]. AI,

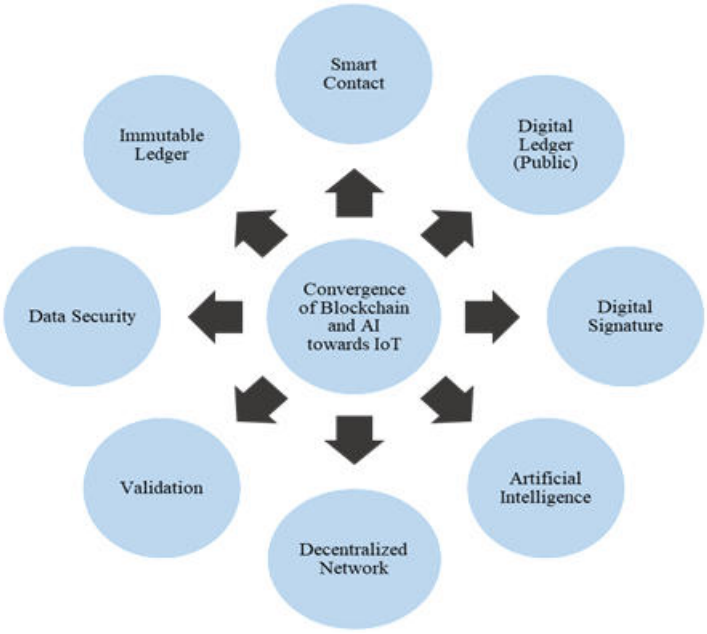

Fig. 2.2: The basic convergence of blockchain and AI for IoT applications.

blockchain, and the IoT have attracted interest from numerous academics in recent years as smart and digital technologies have evolved, and they have risen to prominence as the most widely used technology, generating innovative ideas in a variety of research domains [39]. Fig.2.2 illustrates the basic confluence of blockchain and AI for IoT applications.

The concept of SCs is slowly but steadily becoming a reality as various countries throughout the world adopt and create their own smart city models. At the heart of the smart city are the devices and actuators built into smart gadgets that detect the location and help people make better decisions. The microchips in these devices have been designed to make decisions on their own based on the data collected from the sensors. This entails combining various technologies, like AI, protocols, IoT, wireless sensor networks (WSN), and so on. The AI, IoT, ML, DL, and the terms "cognitive computing" and "big data analytics" have been used interchangeably all played a role in making this goal a reality [46, 47].

One such promising initiative that has been implemented globally with the goal of making residents' life more convenient and inclusive is a smart city [48, 49]. The concept is to employ current technology to transform each object of a traditional city into an independent entity that can run on its own without any external assistance. All daily activities, such as authority, strategies, services, and responses, are computerized, and operators can access them via smart devices from anywhere on the globe. By employing environmentally safe and cost-effective strategies, automation has aided in the reduction of environmental dangers.

3. Artificial Intelligence enabled Intrusion Detection for IoT in Smart City. The increased use of the internet in recent years globally has made it a favorable environment for nefarious activity. Malicious IoT-based systems for SCs are an example of these activities, and they are one of the greatest severe pressures to internet users and smart cities. This rapid development has dramatically increased the number of urbanities that moved to the internet to create a smart city. The fast-growing in these areas expanded online crimes that run using malicious network nodes. Detection and analysis of these networks became one of the major problems of online space [40]. Many professional users that are conscious of malicious activities have also been victims of such attacks.

Typically, malicious pages are online attacks trying to steal users' sensitive information by making a malicious network node and leading users to that, so users may think they interact with a legitimate IoT platform

while using a malicious one. Presently, there are many types of malicious activities in IoT-based systems, and they can appear to be any normal network, such as phishing websites and malware-hosting or malware propagation [50]. The SC is one of the core areas of the IoT field, burgeoning and integrated into daily human events. A smart city is defined as an internet-enabled city for the remote control, monitoring, and management of city appliances via a designated device like a smartphone, tablet, or laptop. A smart city environment, otherwise called an intelligent city, city automation, or domotics, offers users comfortability, convenience, city safety, security, and energy efficiency [51].

According to authors in [52], the smart city incorporates communication networks for connecting major city appliances and services for remote control, monitoring, and access of the residence from within or outside the premises. The major benefits associated with smart city automation systems are healthy living with its deployment in healthcare systems, reduction in energy consumption, and home safety and security. Some countries support the full deployment of smart city automation systems for their residents by putting laws, rules, and subsidies to facilitate its use and encourage residents to adopt a decrement in the rate of energy demand [53]. The increasing interest in research about the city automation system has proven that it is an area that needs exploration to enhance its functionality and accessibility. However, some challenges are still mitigating against the extensive use of smart city automation systems: cost, data storage security, and secured communication channels. This has led to various research works to give an in-depth discussion of smart city automation and find solutions to the challenges of safety and confidentiality in the smart city. The IoT-enabled smart city has been subjected to a variety of cyber-attacks, putting its ability to provide flawless operations to metropolitan areas in jeopardy. Users and city automation suffer financial and reputational harm as a result of such threats, as well as the stealing of confidential documents.

As a result, several Intrusion Detection Systems (IDSs) have been established to combat and defend IoT-enabled smart city systems. However, gathering data that can be used in the advancement of a sophisticated IDS is a tough mission, and there are significant problems in identifying prevailing and novel assaults [20, 40]. As the quantity of IoT-based smart city devices and applications grows, protecting important public infrastructure is becoming a more pressing issue in every city [54]. Malware that takes advantage of zero-day vulnerabilities is one of the most common threats in IoT networks using several ways, the offenders infect vulnerable machines to track and change their behavior [20]. These malicious behaviors demonstrated that traditional cyber-threat methods are no longer adequate for protecting crucial infrastructure such methods are weak and not able to recognize the threats in real time. The NIDS is critical in identifying and responding to any online threats as a cybersecurity mechanism.

The IoT-enabled smart city has evolved into a critical component of today's data and information transfer machinery, prompting the need for global network security [56]. NIDS are frequently used to detect system traffic to protect workstation schemes against numerous grid invasions. Intrusion, according to [40], is a framework for attempting to compromise an information system's security services. In reaction to the difficulties raised by these intrusive systems, researchers have been encouraged to develop novel IDSs. Several IDSs have been developed and enhanced in the past, but they remain susceptible to a diversity of occurrences. The potential of IDS to track and foresee malicious conduct and unknown assaults has sparked a surge of interest in anomaly detection research. Current machine learning-based irregularity detection algorithms, on the other hand, have a significant false alarm rate [57]. According to recent studies, feature selection is now at the heart of an added precise IDS [40, 59].

The feature selection strategy is utilized in most detection methods to choose the fitness values input characteristics for classification models, to improve overall finding performance and lower error rate in NIDS [60]. A classifier feature directions, in particular, are large, and not all of them relate to the groups to be classified, necessitating the adoption of a feature selection approach. The feature selection techniques, on the other hand, can be split into three categories [61]. The most prevalent feature selection technique relies on dataset characteristics without observing the classifier's effectiveness to select the most effective feature. The wrapper technique, on the other hand, is superior since it assesses the quality of the feature subclass using the classifier feedback, resulting in improved prediction performance. Similar to wrapper techniques, to improve the search efficiency of the learning algorithm, a classifier with an inherent process modeling function could be used in the integrated process. Several other Till now, IDS sections have been developed. The IDSs can be

classed as rule-based or non-rule-based, misappropriation discovery, or various techniques, depending on the categorization algorithm used. IDSs can be characterized as real-time if they use permanent system tracking, or intermittent or passive if the traceability takes place only intermittently at set times or even offline utilizing data collected and analyzed over time.

The information received from the detection systems concerning the identified attacks is used to take countermeasures. The more precisely sorted and effective remedies selected, the less they hamper the device's or channel's regular functioning, and the more potent the assault is classed. Additionally, if the same type of attack is not identified, a counterattack may have more severe consequences than the attack itself. As a result, an IDS was created and demonstrated the work in each sort of attack. Furthermore, the system's false alarm rate is minimal, and its detection accuracy is good for both routine and irregular assaults, allowing for little processing to appropriately classify.

Because IDSs are utilized in the dependable and alert system of cyberattacks is crucial in industrial control systems that govern critical infrastructures [62], the latter attribute is essential. The feature extraction technique works well for designing and implementing authentic safety resolutions, as well as increasing IDS performance [63]. The necessity for improved correctness and a lower incorrect alarm rate in particular phenomenon discovery approaches developed the idea of data preprocessing and recognition as two reciprocal stages for IDS models [64, 65]. After eradicating superfluous features from the dataset and preserving a reduced feature set that may be utilized to produce a high-performance version, the preprocessing step employs the reduction attributes to remove the identification process. to use the base classifier to forecast attack kinds.

4. Related Work. The aim of this study is to integrate blockchain with AI for security, privacy, and intrusion detection in IoT-based enabled smart cities. Various works have been proposed to improve security, privacy, and trustworthiness within IoT-based nodes. Several studies have been published in the literature to promote trustworthiness among IoT nodes. In IoT-based systems, [66] suggested a trust architecture that integrated cross-layer permission protocol with Software Defined Network. A Trust Chain was presented by [67]. For allocating reliance and status scores between supply chain actors, this concept offers a three-layered trust management structure based on a consortium blockchain. To lower the number of computational resources used on the Internet of Vehicles [68] introduced consortia blockchain-based reserve distribution and a lightweight Proof-of-Reputation framework (IoV). Proof of reputation consensus procedure was proposed by [69].

The node's asset, consensus involvement, and transaction activity are used to generate the reputation score. A new block with the highest reputation is constructed based on the above score, and reputation-based voting is used to validate the new block. As a result, this method eliminates the need for miners. [70] developed a blockchain-based trust and status scheming system for safety and information critical domains in a distributed multi-agent framework. When agents engage with one another, a reputation score is calculated, and the score is kept on the blockchain to ensure that interactions between agents are trustworthy. Data pre-processing and Gaussian combination are employed for privacy, and ID uses the Kalman filter. A deep blockchain architecture for IoT was created by [71].

Bidirectional Long Short-Term Memory (BiLSTM) was utilized to create a privacy-preserving BC with smart contracts and irregularity discovery. The authors in [20] proposed an IIoT-DL-based ID framework with hybrid rule-based feature selection to train and verify information gathered from TCP/IP packets. A deep feedforward neural network model and a hybrid rule-based feature selection model were used in the training procedure. The results of the performance comparison show that the scheme outperforms other techniques with an accuracy and detection rate of 99.0%, and FPR of 1.0%, for the NSL-KDD dataset. In the case of the UNSW-NB15 dataset the accuracy, detection rate, and FPR of 98.9, 99.9, and 1.1% respectively. The researchers of suggested IDs in wireless connections in [72] and the Aegean AWID datasets were used to demonstrate the system's correctness. A PC, two workstations, one tablet, two cell phones, and an intelligent TV were used to collect the AWID dataset from a SOHO 802.11 wireless network protocol. However, the gathering only includes traces from the Media Access Control surface session and does not include data from IoT devices.

The researchers of [32] created a BoT-IoT dataset using a detailed simulation founded on an IoT network. DDoS, DoS, network check, and keylogging were among the acceptable and aggressive traffic retrieved, and data leakage is an instance of an attack that included both legal and unfriendly traffic. The internet traffic reported by the modeled IoT-based model utilizing the BoT-IoT dataset was more than 72 million. The study has

presented a scaled-down version of the dataset with approximately 3.6 million entries for assessment purposes. A comparable dataset was used in [73] for ADS identification based on DoS assaults in an IoT network of sensors. The data acquired utilizing traditional and DoS assaults are SNMP/TCMP flooding, Ping of Death, and TCP SYN flooding, which simulated a smart home environment. However, because the dataset was not gathered using an IoT-based device, vulnerabilities such as XSS-Cross-site-site were not present in Spyware and scripting. The researchers of [74] suggested an ML-based approach for extracting malware pictures with a blend of local and global features.

The Mailing dataset was utilized to evaluate the performance of the proposed method, which includes 9339 samples from 25 ransomware families. After extracting features, the model showed a 99.21% accuracy rate and 98.40% precision classification utilizing 5288 samples from 8 ransomware families from the dataset. The researchers of [75] suggested a CNN model remove threats from a corpus of binary executables, and their approach achieved 98.52 percent classification accuracy using the Mailing dataset of 9339 pieces from 25 ransomware. Aside from that, this pattern is utilized to select 10% of data arbitrarily for analysis of the dataset. In [76], the study proposes a ransomware detection technique based on CNN. On the same dataset, this model obtained a 98 percent accuracy rate. Within every cycle, a randomized mechanism is used to pick 10% of the samples to study the ransomware group in concern. The researchers advocated employing a Gaussian distribution for demographic initiation [77].

Moreover, to accomplish better discovery throughout each iteration, the Gaussian density function and the local-global best function were utilized in cooperation with the local technique. LGBA-performance NN's was assessed to that of various current advanced approaches, including weight optimization utilizing Particle Swarm Optimization (PSO-NN) and BA-NN. The trial findings demonstrated that LGBA-NN outperformed other variations in multi-class botnet security attacks, with an accuracy of 85.5 and 85.2 percent, accordingly. The researchers of [78] present a spyware detection technique based on ensemble learning. The foundation phase classification is performed by a stacking ensemble of fully integrated and one-dimensional CNNs, whereas the final classification is performed by an ML algorithm. The researchers compared and examined 15 ML classifications for a meta-learner in the research. In the assessment, five ML approaches were used: naive Bayes, decision tree, random forest, gradient boosting, and AdaBoosting.

Tests on the Windows Portable Executable malware dataset resulted in the following findings. The best results were obtained using an ensemble of seven neural network models plus the ExtraTrees classifier as a concluding classification model. [79] proposes a unique multilevel DL image classification method for intrusion detection systems. The network properties are transformed into four-channel images. The pictures are then used to train and assess the pre-trained DL model ResNet50. The suggested approach is tested against two publicly available benchmark datasets, UNSW-NB15 and BOUN Ddos. The suggested approach detects the general assault with 99.8 percent accuracy on the UNSW-NB15 dataset. On the BOUN DDos dataset, the suggested model detects DDoS assaults with 99.7 percent accuracy and ordinary traffic with 99.7 percent accuracy.

The evaluation of existing related works has shown that there is a necessity for a better AI-based model to increase the accuracy and performance of IDS for IoT-based enabled smart cities. This motivates the use of a blockchain for security and privacy-preserving systems for the protection of IoT-based nodes in smart cities, KPCA for feature selection reduction, and CNN for the datasets classification, thus sensing attack trends within data as suspect vectors using depth coverage for data transmission. The proposed model will protect the captured data in SCs, and protect the process of IoT-based data sources within network traffic.

5. Methods and Materials. This section presents the proposed model by explaining in detail the system deployed to eliminate the problems of standalone architecture using cloud databases in IoT-based enabled smart cities. The system takes benefit of the mixture of blockchain and AI-based models for the security and privacy of the IoT-based smart city platform. The blockchain was used on the cloud side to protect the captured data that are stored on the cloud database using CloudBlock and EdgeBlock. The framework contains a two-level security-privacy-preservation method and intrusion detection using CNN techniques after employing KPCA for feature reduction for better accuracy. The sub-section discusses in detail the methodology.

The CloudBlock and EdgeBlock framework: the framework creates various data centers provided by several merchants. The CloudBlock is made up of numerous companies that offer various types of data facilities. The concept made use of three data facilities, A, B, and C, which are entities in the CloudBlock system; the design

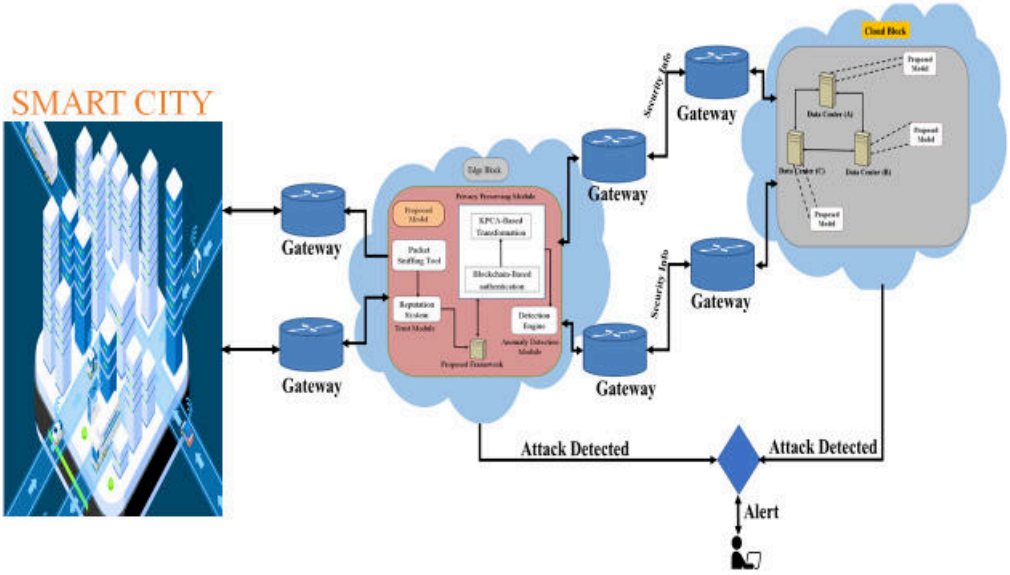

Fig. 5.1: The proposed framework for Privacy and Security Enhancement in Smart Cities.

is deployed at each center to construct a blockchain network. End-users gain trust in this method because the network becomes unchangeable, open to scrutiny, and traceable [80]. When the CloudBlock and EdgeBlock receive the request for information, the preceding protocol is followed, and the service is supplied to the client application, with the administrator being warned in the case of attack cases. The proposed system is based on the combination of blockchain-based on-chain, and AI-based models to create a sustainable smart city.

The proposed framework employed the edge and cloud to take advantage of the combination networks to address the challenges of the IoT-based enabled smart city systems. The effectiveness of the blockchain paradigm was used to protect the IoT-based aided smart cities system, by integrating blockchain and IoT-enabled at edge and cloud sides. Fig. 5.1 displayed the proposed model deployed blockchain and IoT-based enabled edge and cloud called EdgeBlock and CloudBlock. The proposed architecture is to enhanced the smart city applications privacy and security. The suggested framework has three main layers namely: the blockchain security management, a two-level privacy-protection technique, and intrusion detection using CNN algorithm as discussed in detail below: Edge placement framework: The nearest gateway/router is used to forward the network traffic to the EdgeBlock once the data is captured and generated from the IoT-based devices within the level of the smart city. To sniff the incoming traffic at the EdgeBlock, the previous involves a packet sniffing device (sensor) to extract the related features. The EdgeBlock is used to bring the processing closer to the client without necessarily needing to work with cloud network nodes.

Address-based blockchain reputation system was used to verify the reliability of the source of captured data and to compute the status score. The transaction is divided into three based on the outcome of the status score: Authentic, Universal, and Deceitful, then stored in the proposed framework. The privacy-protection module stored the three trust data classes alongside the raw data. To generate a message digest with proof of hash in this segment, blockchain-based ePoW was used, and the message summary is distributed into the blockchain system. The next second-level privacy uses the KPCA technique for converting captured data into a newly converted format that prevents intruders and harmful assaults like DoS, FDIA, and DDoS and removes irrelevant parameters through the feature selection. The CNN model is used to classify the data into standard and various types of attack, and the administrator will be alerted based on which the class of the intruders. The security information along with the demand is sent to the CloudBlock module if information available at the edge side is provided for regular contracts where obligatory information is not accessible. CloudBlock Distribution Framework: This consists of various data centers from several vendors. Three centers were used

for the proposed model called A, B, and C as displayed in fig.5.1.

The proposed system is installed in each data center, resulting in the formation of a blockchain network. When CloudBlock gets an inquiry, the resource is supplied to the requester, and the administrator is notified of any attack occurrences. Therefore, the proposed system utilized the collaborative combination within edge-cloud infrastructure and integrates Blockchain enabled on-chain, and off-chain with the DL model for the development of a sustainable smart city.

5.1. Pre-processing. The preparation stage receives the data set, which consists mostly of two approaches. Data conversion and data normalization are two of them. For processing, the data conversion converts nominal features to numeric features. The data normalization process reduces the huge disparity in attribute values to a reasonable range of values. We employed the minimum-maximum scaling method, which is formally stated as equation (5.1):

$$Y = \frac{Y - min(Y)}{(max(Y) - min(Y)} \tag{5.1}$$

where Y denotes the feature value in the data set, and it is in the range of [0, 1].

5.2. Feature Extraction. Following preprocessing, the dataset is subjected to feature extraction, with KPCA being the most popular method for reducing the data to a lower dimension. As a result, KPCA for complex structures does not take into account non-linear data features. Using KPCA, this issue can be resolved. The feature space R is represented in the mapping function P equation (5.2)

$$P : \phi \varepsilon R_m \rightarrow P\phi \varepsilon R \tag{5.2}$$

where

$$\sum_{i=1}^{t} P(\phi_i) = 0, \tag{5.3}$$

is the covariance matrix can be calculated using the formula equation (5.4)

$$Co_{mtx} = \frac{1}{t} \sum_{i=1}^{t} (P(\phi_i) - mean)(P(\phi_i) - mean)^T \tag{5.4}$$

$$M_{ean} = \frac{1}{t} \sum_{i=1}^{t} (P(\phi_i) \tag{5.5}$$

$$Co_{mtx} = \frac{1}{t} \sum_{i=1}^{t} (P(\phi_i)(P(\phi_i)^T \tag{5.6}$$

Eigenvalue and Eigenvector are two terms that are used interchangeably. An equation can be used to evaluate equation (5.7)

$$Co_{mtx} I = \lambda_i I \tag{5.7}$$

Combining equations (5.6) and (5.7), we get

$$Co_{mtx} = \frac{1}{t} \sum_{i=1}^{t} (P(\phi_i) I P(P(\phi_i)^T = \lambda_i I \tag{5.8}$$

The eigenvector can be rewritten using the formula given in equation (5.9)

$$I = \frac{1}{t}\sum_{i=1}^{t}(\delta_i P(\phi_i)) \tag{5.9}$$

For determining the quotient i, a kernel matrix W of size txt is defined. The elements are calculated using equations in this case (5.10).

$$W_{ij} = (P(\phi_i)(P(\phi_i)^T = (P(\phi_i) \cdot (P(\phi_j) = W(\phi_i, \phi_j) \tag{5.10}$$

when there is no mean in projected dataset $(P(\phi_i)$.

5.3. The Convolutional Neural Network. The convolution kernel was used to train in the convolution layer for the higher layer's feature map. The outcome is a new feature graph including numerous feature graphs that is fed into a convolution core's input signal. Several feature graphs can be convoluted together to generate another output layer in each output feature graph [46]. The following is how the convolution layer is calculated:

$$X_j^l = f\left(\sum_{i\varepsilon M_j} X_i^{l-1} \times K_{ij}^l + b_j^l\right) \tag{5.11}$$

where X_j^l stands for the j feature of the layer map l, K_{ij}^l for the convolutional kernel function, f for the activation function, and b_j^l and M_j for the bias parameter and input feature graph respectively. Each output feature graph is formed using a bias coefficient from a combination as an input feature graph. The error signal of the layer with the weights of the feature graphs is determined using the result of the preceding step, and constant l is set in the bottom sample layer δ. The operation is repeated in the convolution layers to obtain the error signal b_j^l of each feature graph j.

$$\delta_j^l = \beta_j^{l+1}\left(f'(u_j^l \cdot up(\delta_j^l + 1)\right) \tag{5.12}$$

The layer may be used, to sum up the elevation in (5.11), the calculation for a sampling operation is given in equation 5.13:

$$\frac{\delta E}{\delta b_j} = \sum_{u,v}(\delta_j^l)_{uv} \tag{5.13}$$

Finally, the weight gradient of the convolution kernel can be determined using the classic BP approach in CNNs that include weighted values with varied connections. It must first generate a gradient for each link associated with a given weight and then combine the gradients.

$$\frac{\delta E}{\delta K_{ij}^l} = \sum_{u,v}(\delta_j^l)_{uv}(p_i^{l+1})_{uv} \tag{5.14}$$

where $p_i^(l+1)$ can be multiplied by K_{ij}^l been a small block element in the convolutional where the value of the output conversion feature graph's is (u, v) placement. This can be multiplied by a deconvolution element been the result of a small block of the upper (u, v) position. The lowest sampling layer works based on the notion that each outcome featured chart is a small representation of the convolution layer.

$$X_j^i = f(\beta_j^i down(X_j^{l-1}) + b_j^i) \tag{5.15}$$

The n times smaller for feature graph to achieve scaling invariance, where $down(X_j^{l-1})$ is the specimen frame and the low bit value is $n * n$. Each output feature graph has its own multiplying offset variable and admixture bias variable β.

$$\delta_j^l = f'(u_j^i) \cdot conv2(\delta_j^{l+1}, rot180(k_j^l - 1), "full") \tag{5.16}$$

Table 5.1: Characteristics of the ToN-IoT Dataset

Class	Total	Characteristics
Benign	300,000	Standard unmalicious movements
Backdoor	20,000	A way of exploiting remote devices by reacting to client applications that have been carefully designed.
DoS	20,000	An effort to overwhelm a workstation system's resources in order to obstruct access to its data.
DDoS	20,000	A similar approach to DoS, but with several scattered sources.
Injection	20,000	SQL injection and code injection are some of the most prevalent assaults that use unverified inputs to modify the course of operation.
MITM	1043	Person in the Middle is a technique of eavesdropping on traffic and conversations that involves putting an assailant between a target and the host with which the target is seeking to contact.
Password	20,000	includes a variety of brute-force and sniffer methods aimed at collecting credentials.
Ransomware	20,000	An assault in which data on a server are encrypted and money is demanded in return for the decoding technique.
Scanning	20,000	An exploit that encrypts data on a website and requests money in exchange for the decoding process.
XSS	20,000	Cross-site Scripting (XSS) is a type of infiltration in which the intruder transmits malicious files to end users via internet apps.

To connect the convolution function to the entire convolution function, and before calculating, the volume kernel must be rotated 180 degrees. In complement 0, it can handle the convolution border as well as the missing pixel. After that, a t_0 will be obtained as equation 5.17:

$$\frac{\delta E}{\delta b_j} = \sum_{u,v} (\delta_j^l)_{uv} \tag{5.17}$$

$$\frac{\delta E}{\delta \beta_j} = \sum_{u,v} (\delta_j^l \cdot down(X_j^{l-1})_{uv} \tag{5.18}$$

In the convolution neural net, the frequency increase from time t to time $t+1$ is analogous to the BP approach.

$$w(t+1) = w(t) + \mu\delta(t)x(t) \tag{5.19}$$

Here $\delta(t)$ is the error term, the learning rate is μ, and the input of the neuron is denoted as $x(t)$.

5.4. Datasets. Two prominent datasets that were publicly available were used in the study namely: ToN-IoT and BoT-IoT datasets.

5.4.1. The ToN-IoT Dataset. The dataset is freely available established by UNSW Canberra Cyber IoT-Lab at The Australian Defense Force Academy, and is gotten from a practical and large-scale system [26-27]. A variety of normal and cybersecurity Incidents from IoT networks are compiled in parallelization for the dataset.

To replicate the capability as well as the adaptability of automotive IoT and industry Networks 4.0, the IoT lab has constructed a new testbed that connects Simulated machines, physical equipment, hacking platforms, and cloud and fog systems are all examples of technology, and IoT sensors are among the devices available. The dataset covers many modern DoS, DDoS, and other device-connected assaults spyware, that have been installed via the IoT network in comparison to web apps, Internet of Things interfaces, and electronic systems. There are 43 features in the dataset. The dataset was split into two parts: a train set and a test set, each comprising 70% and 30% of the total. The statistics of the collection containing both standard and unique network attacks are shown in table 5.1.

5.4.2. The BoT-IoT Dataset. This data was developed by creating a realistic network platform in the UNWS of Canberra Cyber Range Center [32]. The Message Queuing Telemetry Transport protocol is used to generate this data gathering, which connects machine-to-machine connections, making it a viable alternative

Table 5.2: Features of the used BoT-IoT Dataset

Class	Total	Characteristics
Benign	477	Normal unmalicious flows
Reconnaissance	91,082	A way of exploiting remote devices by reacting to client applications that have been carefully designed.
DoS	1,650,260	An effort to overwhelm a computer device's resources in order to obstruct accessibility to its information.
DDoS	1,926,624	The DDoS is a type of DoS attack that uses many distributed sources.
Theft	79	Data theft and keylogging are examples of attacks aimed at obtaining sensitive data.

Table 5.3: The selected features for ToN-IoT and BoT-IoT Datasets using the KPCA feature selection method.

Class	Total Features Selected	Selected Features
Benign	17	F1, F2, F3, F4, F5, F6, F7, F8, F9, F10, F11, F12, F13, F14, F15 F16, F17
Recon	7	F1, F2, F3, F4, F5, F6, F7

for IoT solutions. Table 1 shows the statistics of various assaults in the BoT-IoT dataset. Various assaults, like DDoS, DoS, and Theft, are included in the dataset. Table 5.2 shows the characteristics of the BoT-IoT dataset.

Table 5.3 shows the reduced features after applying the KPCA algorithms to the datasets used to assess the effectiveness of the proposed approach. The features of the ToN-IoT were reduced to 17 features while BoT-IoT features were reduced to 7 features.

5.5. Performance analysis. The accompanying performance indicators were used to test the hypothesized algorithm's results and evaluate it to other latest systems based on DL and hybrid rule-based techniques. The amount of right/wrong outputs in a classifying job was totaled and evaluated to the benchmark findings. Accuracy, Precision, Sensitivity, Specificity, and F1-score are the most commonly used matrices. The numerical metrics true positive (TP), true negative (TN), false positive (FP), and false-negative (FN) were obtained to rectify the confusion matrix, as shown in equations 5.20 - 5.26 [81].

$$Accuracy = \frac{(TP + TN)}{(TP + FP + FN + TN)} \tag{5.20}$$

$$Precision = \frac{TP}{(TP + FP)} \tag{5.21}$$

$$SensitivityorRecall = \frac{TP}{(TP + FN)} \tag{5.22}$$

$$Specificity = \frac{TN}{(TN + FP)} \tag{5.23}$$

$$F1 - score = \frac{2 * (Precision * Recall)}{(Precision + Recall)} \tag{5.24}$$

$$TPR = \frac{TP}{(TP + FN)} \tag{5.25}$$

$$FPR = \frac{FP}{(FP + TN)} \tag{5.26}$$

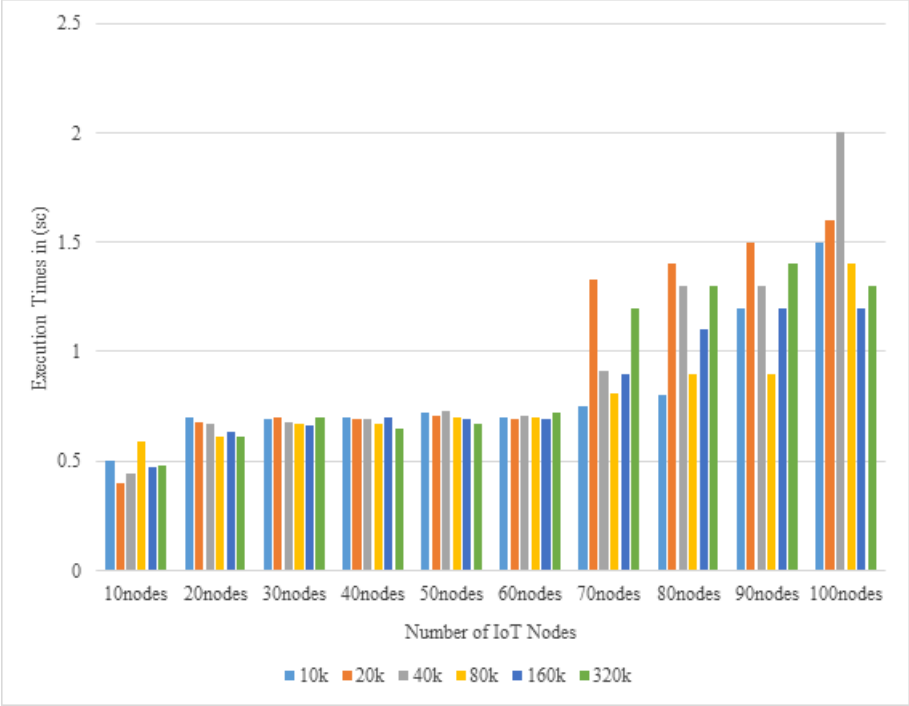

Fig. 6.1: The effect of adjusting the amount of IoT nodes in the CloudBlock off-chain memory in a Blockchain network on posting duration.

6. Results and Discussion. The platforms used for the experiment and implementation of the proposed models are the R programming language and the Scikit-learn library used for the implementation of the AI model [82]. The KPCA was used for feature selection in order to eliminate the unnecessary elements from both datasets, and the suggested model was evaluated using performance indicators. The Solidity programming language with Ethereum was used for the implementation of the Blockchain Machinery. An HP with Window 11 Intel(R) Core(TM) i7-2520M CPU @ 2.50GHz with 128 GB RAM and 2 TB hard disk. The results were compared with the recent state-of-the-art model using the same datasets, non-blockchain and blockchain framework.

6.1. The proposed model for security and privacy process. The IoT-based devices' dependability and reliability were evaluated, and the CloudBlock was used to the data for general transactions and honesty. The proposed model was studied in uploading files on the CloudBlock storage. The peers are represented from 10-100 in the X-axis, and the time taken to upload various file sizes is represented in the Y-axis with sizes of 10KB-30Kb. In the off-chain storage network. Fig.6.1 shows the results obtained using the method and Investigates the time impact when the system is expanded statically. There is a direct link between the quantity of active participants and the memory usage that grows as more IoT units are joined to the network must be published in terms of scalability.

6.2. Trust Management Process. The reputation score was computed for the proposed model using 100 nodes of IoT in the Ethereum network, and the IoT nodes were represented by R_{ps}. The specific address was allotted to each IoT node in the blockchain network. The transaction score was computed using the transactions performed by these nodes, using T_{xscore} against the $C_{Threshold}$ confidence threshold value. To evaluate the trust within the proposed model, the score generated was used by calculating R_{ps} for produced transactions. The R_{ps} and T_{xscore} for 1000 transactions are displayed in Fig. 6.1.

The valid transaction values for the available features were used in the model to calculate for ToN-IoT and BoT-IoT datasets, hence, fall in the honest operation grouping. The proposed technique was used to study

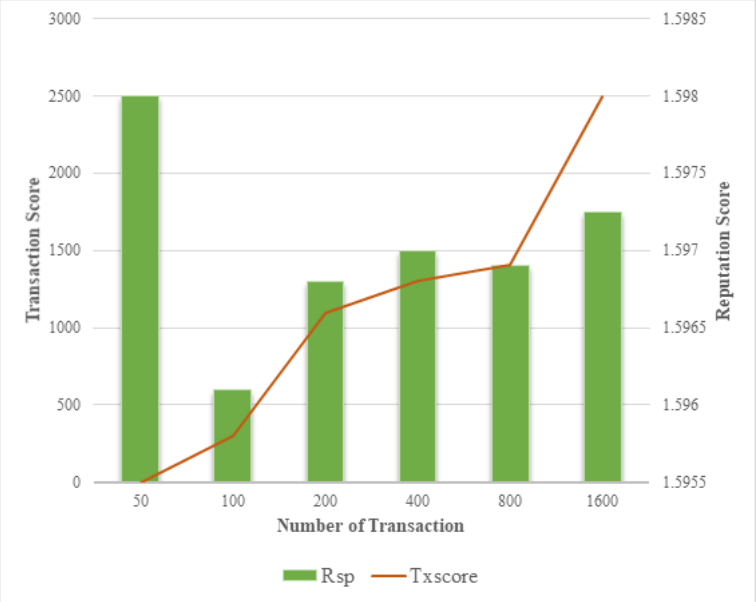

Fig. 6.2: The IoT device Trust Management using Reputation score vs. Transaction score

the execution time-varying number of transactions with respect to computation in the CloudBlock framework. The results show that there are steady increases in the T_{xscore} as the number of transactions increases. Fig.6.2 shows the IoT device trust management using reputation score vs. transaction score.

Fig.6.3 displays the results of varying IoT nodes with various sizes in block creation time using the proposed model. Chronologically ordered the blocks are added to the distributed ledger. Once the collaborating IoT nodes have completed the mining operation. The message digest is published throughout the blockchain network, along with the reputation score. The verifiability and immutability of the transactions signify these chains of blocks. The accessibility of the operation in the blockchain system was shown using block access time. The block access time of the transaction in the blockchain is shown in fig.6.4. The access time of the block for the proposed framework was calculated by varying the number of IoT nodes for KPCA evaluation. The results show that an increase in the number of IoT nodes also rises the access time taken in the network.

6.3. The intrusion detection process experiments results. The performance of the suggested two-level security and confidentiality method is assessed using two prominent IoT smart cities datasets as a function scheme of the intrusion detection based CNN and KPCA was used for features selection. The proposed model was applied to the two datasets in other to be able to identify various attack instances and normal.

The proposed model uses various performance metrics for evaluation. Preprocessing was performed utilizing feature mapping, variable selection employing KPCA, and normalized on both ToN-IoT and BoT-IoT datasets. The most relevant features from the used datasets were selected using the KPCA algorithm. Table 6.1 shows the list of the most relevant features selected for the ToN-IoT dataset in the designed security and privacy models using the CNN algorithm for the smart city.

Table 6.1 shows the detection rate (DR) for the instances in the ToN-IoT using the proposed model. The detection rate of the recorded instances with feature selection is as follows: Benign (100.0%), Backdoor (100.0%), Dos (98.7%), DDoS (97.4%), Injection (98.3%), MiTM (69.2%), Password (98.2%), Ransomware (99.5%), Scanning (99.3%), and XSS (97.2%), respectively. The DR of the recorded instances without feature selection is as follows: Benign (99.30%), Backdoor (99.9%), Dos (98.7%), DDoS (91.9%), Injection (92.4%), MiTM (60.6%), Password (95.8%), Ransomware (98.3%), Scanning (93.4%), and XSS (80.1%), respectively. The DR results for the BoT-IoT dataset using the proposed model are shown in Table 6.2 to determine the performance of the models on the detection of attackers on the dataset without feature selection on class types

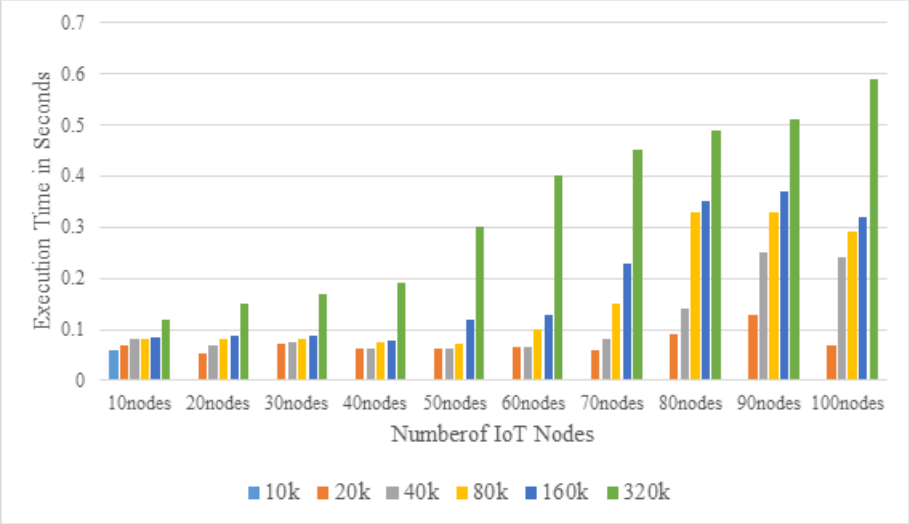

Fig. 6.3: The effects of file size and the number of IoT nodes in a blockchain network on block

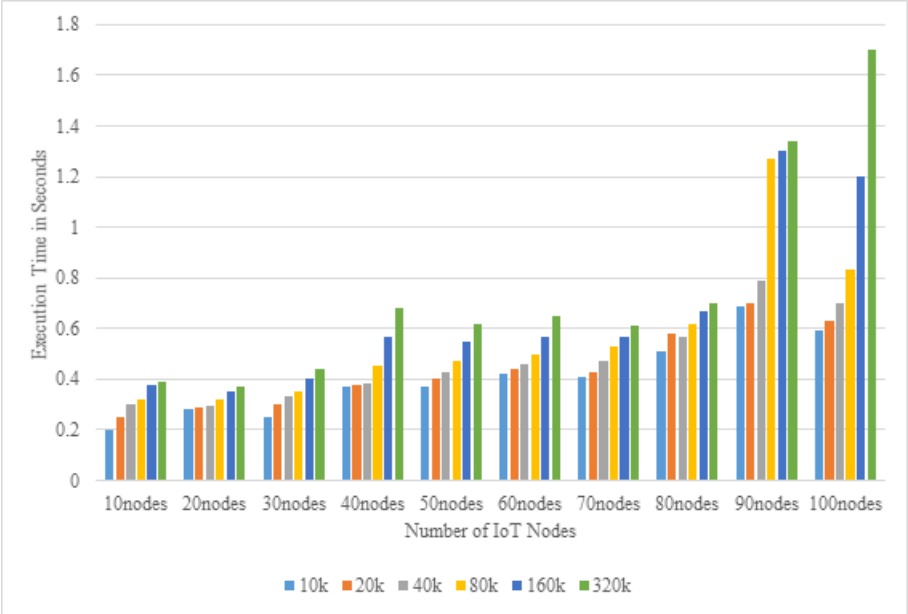

Fig. 6.4: Block access time in a blockchain network with different file sizes and numbers of IoT nodes.

for Benign (78.0.0%), DoS (99.7%), DDos (100.0%), Reconnaissance (100.0%), and Theft (100.0%), respectively. The DR of the recorded instances without feature selection are as follows: Benign (82.6%), DoS (90.2%), DDos (95.7%), Reconnaissance (97.4%), and Theft (0.0%), respectively. The results proposed technique demonstrated high DR for intrusions detection in both datasets and show better performance when compared with recent models. The obtained resulted from the two datasets show that the feature selection technique really works effectively on the datasets for the detection of intrusions attack.

Table 6.3 shows the proposed model performance using both ToN-IoT and BoN-IoT datasets with the aforementioned metrics. The results using the model are very relevant and effective in intrusion detection of

Table 6.1: Detection rates for ToN-IoT datasets with and without Feature Selection

	Dataset Used	
Attack Class	With Feature Selection	Without Feature Selection
Benign	100.0	99.3
Backdoor	100.0	99.9
DoS	98.7	98.7
DDoS	97.4	91.9
Injection	98.3	92.4
MITM	69.2	60.6
Password	98.2	95.8
Ransomware	99.5	98.3
Scanning	99.3	92.4
XSS	97.2	80.1

Table 6.2: Detection rates for BoT-IoT datasets with and without Feature Selection

	Dataset Used	
Attack Class	With Feature Selection	Without Feature Selection
Benign	78.0	82.6
DoS	99.7	90.2
DDoS	100.0	95.7
Reconnaissance	100.0	97.4
Theft	100.0	0.0

Table 6.3: The Proposed Model Evaluation Results.

Dataset	TP Rate	FP Rate	Precision	Sensitivity	F-Measure	ROC	Class
ToN-IoT	99.8	0.1	97.6	99.9	98.9	98.9	Attack
	100.0	0.001	99.8	99.6	97.5	99.8	Normal
BoN-IoT	100.0	0.1	99.3	99.9	99.7	99.7	Attack
	99.9	0.001	100.0	99.3	99.2	99.8	Normal

IoT-based enabled smart cities for the classification and prediction of various attacks with the nodes of the networks.

From the results obtained It can be concluded that the proposed system's performance is satisfactory for the security and privacy of the IoT-based enabled smart city looks promising and work perfectly, especially when the KPCA feature selection is applied to the datasets. The use of blockchain for first-level protection before applying the DL model with KPCA performs very well better than the existing model without the application of blockchain and feature selection algorithms.

6.4. Using Existing Techniques to Compare the Proposed Model. Table 6.4 shows the contrast results of the anticipated models with some current work to really show the efficiency of the KPCA feature selection on the datasets and the classifier detection efficiency. To demonstrate how feature selection influences the discovery performance of a classification procedure, the outcomes show that the suggested model performs better in precision and FPR than other approaches.

The proposed model in the overall accuracy on both datasets has a 99% and the FPR is a very low error percentage. The suggested model also shows a better performance across all evaluation metrics used. The marginal increases in the accuracy may be due to the use of the KPCA algorithm in selecting the most appropriate features for each dataset.

To further prove the efficiency and performance of the proposed framework, a comparison of both non-blockchain and blockchain structures was conducted with other related schemes. These comparisons were based on various parameters like (i) off-chain, (ii) ledger distribution, (iii) IDS, (iv) security, (v) privacy, (vi) trust, (vii) scalability, (viii) decentralized (ix) non-repudiation, (x) verifiability, and (xi) deep learning. The

Table 6.4: The UNSW-NB15 Dataset Performance Comparison Summary

Model	Performance Metrics					
	Accuracy	FPR	F-Score	Sensitivity	Precision	ROC Curve
Wrapper + neurotree [83]	98.38	1.62	98.4	98.0	98.9	99.8
SVM+EML+K-Means [84]	95.75	1.87	94.4	99.7	89.7	98.6
GA +SVM [85]	97.3	0.017	96.6	99.7	93.8	98.1
CNN+LSTM [86]	94.12	-	95.6	98.9	92.5	98.4
Modified KNN [74]	98.7	1.3	99.2	99.6	98.8	99.8
CfsSubsetEval + GA+RuleEval+ANN [38]	98.8	1.2	98.9	98.9	98.9	99.8
DFFNN + Rule-based [20]	98.9	1.1	98.9	99.8	96.7	98.9
Proposed Model	99.8	1.07	99.2	99.9	100	99.8

Table 6.5: Comparison of the proposed model with existing blockchain models

Model	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
RealAlert [28]	x	x	x	√	x	√	x	x	x	x	x
Cryptographic + blockchain [87]	x	√	x	x	√	X	x	√	√	√	x
Fog + Blockchain [88]	x	√		√	√	√		√		√	X
Interplanetary file system + Blockchain [89]	√	√	x	√	√	X	√	√	√	√	x
TP2SF [1]	√	√	√	√	√	√	√	√	√	√	x
TrustChain [67]	x	√	x	√	√	√	x	√	x	√	x
BiLSTM + Blockchain [71]		√	√	√	√			√		√	√
PPAD-CPS [90]	x	x	√	√	√	X	x	√	x	x	√
Proposed Model	√	√	√	√	√	√	√	√	√	√	√

Table 6.6: Comparison of the proposed model with non-blockchain models

Model	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
independent component analysis (ICA) [91]	x	x	√	√	√	X	x	x	x	x	x
SUM, RNN and LSTM [32]	x	x	√	√	x	X	x	x	x	x	√
CST-GR [92]	x	x	√	√	x	X	x	x	x	x	x
TP2SF [93]	√	√	√	√	√	√	√	√	√	√	x
DFFNN + Rule-based [20]	x	x	√	√	x	X	x	x	x	x	√
PCA-firefly + XGBoost [94]	x	x	√	√	x	X	x	x	x	x	x
FGMC-HADS [33]	x	x	√	√	x	X	x	x	x	x	√
bijective soft set [95]	x	x	√	√	x	X	x	x	x	x	x
bijective soft set + CorrACC [96]	x	x	√	√	x	X	x	x	x	x	x
Proposed Model	√	√	√	√	√	√	√	√	√	√	√

scalability of the system is achieved with the off-chain storage, their blockchain memory allocated hashing used for each raw transaction record. The ledger distribution is the capacity of each IoT node to save the matching replica of the ledger and replicate itself in the IoT-based enabled smart city. framework. The IDS was achieved with the use of the AI-based model classifier.

The two-level approach for security and privacy preservation used by the framework addressed the major challenges of security, privacy, and trust in the smart city. The combination of the blockchain paradigm, KPCA algorithm, and AI classifier security and privacy model ensures these features.

The proposed framework ensures the maintainability of non-repudiation with recorded transactions in the ledger since the participant node cannot be denied from a transaction once the transaction gets included in the ledger, and the behavior of the transaction is been protected. The use of timestamp records to audit-trail each transaction proved the verifiability metric in the framework. The CloudBlock framework with EdgeBlock ensured decentralization in the IoT-based enabled smart city. The results of both blockchain and non-blockchain for comparison are presented in Tables 6.5 and 6.6.

A distributed network built on the blockchain is being created to secure transactions in IoT-based smart

cities by confirming the transaction's validity. Blockchain technology is used to transfer data between locations. The blockchain functions in a number of ways, including block production, block broadcast to all network nodes, transaction verification, and transfer request. The transaction will continue with the addition of a new user registration if the verification process is successful; else, all steps must be redone. The fundamental purpose of trusted entities is to validate transactions; hence this is how they are employed. After the transaction has been validated, the verifier must choose between the options yes or no. If the state is accurate, the transaction is finished by adding a block to the Blockchain; if an attack is discovered during the transaction, it is aborted. The sort of assaults can be identified and the transaction can be blocked by utilizing a deep learning-based classifier that is enabled with KPCA. The dataset's features are first extracted using KPCA, and then the extracted features are submitted to CNN for classification.

The creation of an improved Proof of Work (ePoW) method based on blockchain is part of the first level of privacy and trust, and it will be used to authenticate data records and stop data poisoning assaults from changing the original data. The attribute data is subjected to the second level of privacy while the ePow algorithm is running. The datasets for smart cities are referred to by this property. At this level, we choose crucial features in order to safely train and validate a utility model. Utilizing a set of weighted parameters and a feature selection model called a KPCA, an input X is encoded into new data codes.

The proposed framework was able to secure and preserve IoT-based SC with given trust among users and identified attack behaviors efficiently. This can be ascribed to its layered data extraction of the IDS model development. The two-level security and privacy technique of blockchain with smart contact help in achieving better protection against intruders through the validation of data transactions, validation of the IDS model, and the extraction of relevant features from the captured data for processing purposes. The first phase makes use of security and privacy-preserving based on blockchain technology to insured data integrity by verifying and checking records for possible poisoning through the application of hash chain making malevolent modification of records highly exclusive computationally. The second phase makes use of KPCA for feature selection, which includes data preprocessing, converting nominal attributes into numeric using feature mapping, and scaling the attributes into specific ranges by feature normalization. The two-level security and privacy-preserving technique protect sensitive data and information of smart cities nodes network traffic and power systems against exposure in IoT-based applications. The incorporation of CNN and KPCA in the second stage fuses important features into relevant features to be able to discover intrusion attacks in a smart city classifying malicious activities with the IoT nodes in SC using lower and upper boundaries of the normal subsequent likelihoods, and the variations from them should be treated as abnormal discoveries.

The proposed model is very easy to deploy, implement, and in an extremely active and heterogamous network of IoT-based enabled smart cities, the system can be efficiently used to detect recent and most attacks found within network nodes and protect and secure the IoT-based enabled smart city. The proposed framework can competently compute the status score of the participating IoT nodes using the blockchain reputation system and build trustworthiness in the network traffic and transmission. The integration of blockchain, KPCA and CNN approaches for security-privacy preserving, and the dimensionality reduction method helps in preventing inference and poisoning attacks within IoT nodes networks. Therefore, the proposed model improved the overall efficiency and performance of the IoT-based enabled smart city in general. The verifiability, reliability, and traceability were able to be activated with the incorporation of CloudBlock a blockchain paradigm cloud infrastructure. The use of DL algorithms with feature selection techniques also increases the performance of the anticipated structure greatly.

6.5. The benefits and challenges related to deploying the CloudBlock-EdgeBlock architecture in a real-world smart city environment. The proposed architecture has a lot of benefits. The majority of assaults encountered in the highly dynamic and heterogeneous network of an IoT-driven smart city can be efficiently detected by it, and it is first straightforward to implement and deploy. Second, the network becomes more trustworthy thanks to the address-based blockchain reputation system's ability to accurately calculate the reputation score of participating IoT nodes. Third, the two-level privacy-preserving strategy combines PCA-based dimensionality reduction with blockchain technology to thwart inference and poisoning attacks. The performance of the suggested TP2SF architecture has been significantly enhanced by the aforementioned method. Additionally, the incorporation of blockchain technology into cloud and fog infrastructures allows for

verifiability, traceability, and dependability. However, a few issues have been noted, such as the fact that block mining and file uploading times gradually increase as more IoT nodes participate.

A transaction in the blockchain is only confirmed after being approved by/verified by all nodes. There is a risk for cyberattacks because this verification takes a certain amount of time. One of these attacks that takes advantage of the transaction verification time is double-spending. Attackers take advantage of the time required for the authentication of each transaction on the blockchain. The attacker uses the same coin twice during the transaction verification delay since both transactions are being verified at the same time. This makes it simple to copy and fake digital currencies. The blockchain's immutability guarantees data integrity, facilitates message exchanges between all parties, and creates logs and events. It ensures that everyone has access to the deployed smart contract on the blockchain at all times. Additionally, availability guarantees that all services are constantly accessible. The system is also shielded against DoS assaults because to the fact that all transactions are recorded on an Ethereum distributed ledger. So there is no concern about hacking, failure, or compromise. Thousands of reliable mining nodes guard the Ethereum ledger, making it extremely resistant to DoS attacks. Using a permissioned or private blockchain, such as Hyperledger or private Ethereum networks, the criterion of confidentiality is met. In the suggested situation, the proposed solution is built on a blockchain with a permissions network.

Links between transactions and public blockchain addresses can reveal a user's true identity. Systems for managing digital identities centrally are not secure. A new contract deployment for every upgrade raises trust and inconsistency issues. The mart contract is unable to send deterministic outside requests. Smart contracts are unchangeable and aid in building confidence between the parties to a contract. The smart contract code, however, is typically not upgradeable, even in the event of flaws, vulnerabilities, or new business-logic requirements (for example, on the Ethereum Platform). A new instance of the smart contract with a new contract address is typically used to deploy an updated smart contract code, which may cause issues with inconsistency. Delegating calls from the proxy contract to the new logic contract is one workaround for an upgradeable smart contract, nevertheless [5]. While the logic contract performs the new logic, the proxy contract holds the data. With each change, the logic-contract address is updated in the proxy contract. The upgrade has no impact on the smart city service user because the proxy contract protects his data. However, there are trust and decentralization problems with the proxy-contact-delegation-call approach.

Since everyone can typically access user data and user-pseudonymous identities on public blockchains, privacy issues, and identity risks arise. Innovative privacy techniques including double-blind data sharing and zero-knowledge proofs-based distributed permission management can be used for privacy-preserving selective data sharing in mutually anonymous multi-party transactions in a variety of smart city services, according to authors in [19]. While the transaction data itself may be encrypted via symmetric on-chain encryption and other methods. One of the drawbacks is that each of these methods increases network latency.

Nowadays, digital identity management systems run by centralized authorities are used to give user identities for smart city services. Users can completely control their digital identity without the help of a centralized third party using self-sovereign identity (SSI) and decentralized ID (DID). Users can manage how their individually identifiable information and data are shared in this way. Blockchain-enabled SSI and DID can be utilized for decentralized user identification, authentication, and authorization in IoT-enabled smart city services. However, there are a number of problems with SSI and DID, including human reliance (a user could misplace the private key). A significant difficulty is creating safe recovery strategies for SSI and DID.

Every transaction on open blockchains is viewable by anybody. The public address of each participating device can be used to identify it. Even though the public address is fictitious, curious, or malicious individuals with knowledge of the background can take advantage of the connections between public addresses and the real-world identities of the transaction users. The privacy concerns in applications for smart cities powered by cryptocurrencies can be reduced by creating a new disposable address for each new payment as well as by deploying mixers that gather and disperse funds to pertinent stakeholders.

7. Conclusion. The increased use of the internet in recent years globally has made it a favorable environment for nefarious activity. Malicious IoT-based systems for SCs are an example of these activities, and they are one of the greatest severe pressures to internet users and smart cities. This rapid development has dramatically increased the number of urbanities that moved to the internet to create a smart city. The fast-

growing in these areas expanded online crimes that run using malicious network nodes. Detection and analysis of these networks became one of the major problems of online space and this is evident in the evolution of SCs. To alleviate the challenges associated with IoT-based enabled SCs like security, privacy, scalability, centralization, and communication latency. This paper proposes a blockchain, KPCA with DL-based technique-oriented infrastructure for a secure IoT-based enabled SC. The communication stage of the IoT-based smart city was secure and established protocols for data forwarding using blockchain technology in the IoT nodes network. The KPCA was used to eradicate unwanted and unrelated features from the dataset. The communication latency, scalability, and the detection of an intrusion were achieved using a DL-based cloud employed at the application level. The suggested model was assessed utilizing two openly accessible transformed and original datasets namely: ToN-IoT and BoN-IoT for the security mechanism since both datasets have various IoT-based attacks like DoS, Ransomware, normal vectors, MITM, and Theft as mentioned earlier, and are publicly available. The results show a higher level of performance in terms of accuracy and increase the security, privacy, and maintainability concerns of IoT-based enabled SCs applications. In terms of accuracy, recall, precision, detection rate, and F1-score, the proposed systems' experimental results outperform other existing state-of-the-art models when compared. Both blockchain and non-blockchain systems demonstrated the advantage of the proposed system against existing frameworks. Finally, the proposed system enabled IoT-based enabled smart city high-performance computing resources, and cost-effective applications like smart waste management, smart grid, smart agriculture, and smart healthcare. The future scope will extend the proposed system by integrating cryptography techniques that will further secure the cloud from cyberattacks and give privacy to the users' data. The implementation of a protocol that will verify the overall system to recognize security restrictions. These will further enhance the overall security and privacy necessity in SC. The utilization of the anticipated model increases automatic data analysis and the advanced communication bandwidth of smart cities.

REFERENCES

[1] Park, E., Del Pobil, A. & Kwon, S. The role of Internet of Things (IoT) in smart cities: Technology roadmap-oriented approaches. *Sustainability*. **10**, 1388 (2018)

[2] Zhang, X. The trends, promises and challenges of urbanisation in the world. *Habitat International*. **54** pp. 241-252 (2016)

[3] Singh, S., Sharma, P., Yoon, B., Shojafar, M., Cho, G. & Ra, I. Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustainable Cities And Society*. **63** pp. 102364 (2020)

[4] Tabane, E., Ngwira, S. & Zuva, T. Survey of smart city initiatives towards urbanization. *2016 International Conference On Advances In Computing And Communication Engineering (ICACCE)*. pp. 437-440 (2016)

[5] Zhuang, P., Zamir, T. & Liang, H. Blockchain for cybersecurity in smart grid: A comprehensive survey. *IEEE Transactions On Industrial Informatics*. **17**, 3-19 (2020)

[6] Arowolo, M., Ayegba, P., Yusuff, S. & Misra, S. A Prediction Model for Bitcoin Cryptocurrency Prices. *Blockchain Applications In The Smart Era*. pp. 127-146 (2022)

[7] Awotunde, J., Folorunso, S., Ajagbe, S., Garg, J. & Ajamu, G. AiIoMT: IoMT-based system-enabled artificial intelligence for enhanced smart healthcare systems. *Machine Learning For Critical Internet Of Medical Things: Applications And Use Cases*. pp. 229-254 (2022)

[8] Othman, S., Almalki, F., Chakraborty, C. & Sakli, H. Privacy-preserving aware data aggregation for IoT-based healthcare with green computing technologies. *Computers And Electrical Engineering*. **101** pp. 108025 (2022)

[9] Khatua, P., Ramachandaramurthy, V., Kasinathan, P., Yong, J., Pasupuleti, J. & Rajagopalan, A. Application and assessment of internet of things toward the sustainability of energy systems: Challenges and issues. *Sustainable Cities And Society*. **53** pp. 101957 (2020)

[10] Silva, B., Khan, M. & Han, K. Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sustainable Cities And Society*. **38** pp. 697-713 (2018)

[11] Nayyar, A., Rameshwar, R. & Solanki, A. Internet of Things (IoT) and the digital business environment: a standpoint inclusive cyber space, cyber crimes, and cybersecurity. *The Evolution Of Business In The Cyber Age*. **10** pp. 9780429276484-6 (2020)

[12] Ogundokun, R., Arowolo, M., Misra, S. & Awotunde, J. Machine learning, IoT, and blockchain integration for improving process management application security. *Blockchain Applications In The Smart Era*. pp. 237-252 (2022)

[13] Ogundokun, R., Arowolo, M., Misra, S. & Damasevicius, R. An Efficient Blockchain-Based IoT System Using Improved KNN Machine Learning Classifier. *Blockchain Based Internet Of Things*. pp. 171-180 (2022)

[14] Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C. & Faruki, P. Network intrusion detection for IoT security based on learning techniques. *IEEE Communications Surveys and Tutorials*. **21**, 2671-2701 (2019)

[15] Khan, K., Mehmood, A., Khan, S., Khan, M., Iqbal, Z. & Mashwani, W. A survey on intrusion detection and prevention in wireless ad-hoc networks. *Journal Of Systems Architecture*. **105** pp. 101701 (2020)

[16] Awotunde, J., Chakraborty, C. & Folorunso, S. A secured smart healthcare monitoring systems using Blockchain Technology.

Intelligent Internet Of Things For Healthcare And Industry. pp. 127-143 (2022)
[17] Awotunde, J., Jimoh, R., Folorunso, S., Adeniyi, E., Abiodun, K. & Banjo, O. Privacy and security concerns in IoT-based healthcare systems. *The Fusion Of Internet Of Things, Artificial Intelligence, And Cloud Computing In Health Care*. pp. 105-134 (2021)
[18] Da Costa, K., Papa, J., Lisboa, C., Munoz, R. & Albuquerque, V. Internet of Things: A survey on machine learning-based intrusion detection approaches. *Computer Networks*. **151** pp. 147-157 (2019)
[19] Bhaskaran, K., Ilfrich, P., Liffman, D., Vecchiola, C., Jayachandran, P., Kumar, A., Lim, F., Nandakumar, K., Qin, Z., Ramakrishna, V. & Others Double-blind consent-driven data sharing on blockchain. *2018 IEEE International Conference On Cloud Engineering (IC2E)*. pp. 385-391 (2018)
[20] Awotunde, J., Chakraborty, C. & Adeniyi, A. Intrusion detection in industrial internet of things network-based on deep learning model with rule-based feature selection. *Wireless Communications And Mobile Computing*. **2021** pp. 1-17 (2021)
[21] Hassan, M., Rehmani, M. and Chen, J. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Generation Computer Systems*. **97** pp. 512-529 (2019)
[22] Elrawy, M., Awad, A. & Hamed, H. Intrusion detection systems for IoT-based smart environments: a survey. *Journal Of Cloud Computing*. **7**, 1-20 (2018)
[23] Singh, S., Sharma, P., Moon, S., Moon, D. & Park, J. A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions. *The Journal Of Supercomputing*. **75** pp. 4543-4574 (2019)
[24] Bostami, B., Ahmed, M. & Choudhury, S. False data injection attacks in internet of things. *Performability In Internet Of Things*. pp. 47-58 (2019)
[25] Illiano, V. & Lupu, E. Detecting malicious data injections in wireless sensor networks: A survey. *ACM Computing Surveys (CSUR)*. **48**, 1-33 (2015)
[26] Altaf, A., Abbas, H., Iqbal, F. & Derhab, A. Trust models of internet of smart things: A survey, open issues, and future directions. *Journal Of Network And Computer Applications*. **137** pp. 93-111 (2019)
[27] Awotunde, J., Bhoi, A. and Barsocchi, P. Hybrid cloud/Fog environment for healthcare: an exploratory study, opportunities, challenges, and future prospects. *Hybrid Artificial Intelligence And IoT In Healthcare*. pp. 1-20 (2021)
[28] Mohiyuddin, A., Javed, A., Chakraborty, C., Rizwan, M., Shabbir, M. & Nebhen, J. Secure cloud storage for medical IoT data using adaptive neuro-fuzzy inference system. *International Journal Of Fuzzy Systems*. **24**, 1203-1215 (2022)
[29] Behera, S., Pradhan, A. & Dash, R. Deep Neural Network Architecture for Anomaly Based Intrusion Detection System. *2018 5th International Conference On Signal Processing And Integrated Networks (SPIN)*. pp. 270-274 (2018)
[30] Dash, S., Chakraborty, C., Giri, S., Pani, S. & Frnda, J. BIFM: Big-data driven intelligent forecasting model for COVID-19. *IEEE Access*. **9** pp. 97505-97517 (2021)
[31] Farnaaz, N. & Jabbar, M. Random forest modeling for network intrusion detection system. *Procedia Computer Science*. **89** pp. 213-217 (2016)
[32] Koroniotis, N., Moustafa, N., Sitnikova, E. & Turnbull, B. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Generation Computer Systems*. **100** pp. 779-796 (2019)
[33] Haider, W., Moustafa, N., Keshk, M., Fernandez, A., Choo, K. & Wahab, A. FGMC-HADS: Fuzzy Gaussian mixture-based correntropy models for detecting zero-day attacks from linux systems. *Computers and Security*. **96** pp. 101906 (2020)
[34] Moustafa, N. A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. *Sustainable Cities And Society*. **72** pp. 102994 (2021)
[35] Ogundokun, R., Awotunde, J., Misra, S., Abikoye, O. & Folarin, O. Application of machine learning for ransomware detection in IoT devices. *Artificial Intelligence For Cyber Security: Methods, Issues And Possible Horizons Or Opportunities*. pp. 393-420 (2021)
[36] Cui, F. Deployment and integration of smart sensors with IoT devices detecting fire disasters in huge forest environment. *Computer Communications*. **150** pp. 818-827 (2020)
[37] Benke, K. & Benke, G. Artificial intelligence and big data in public health. *International Journal Of Environmental Research And Public Health*. **15**, 2796 (2018)
[38] Ayo, F., Folorunso, S., Abayomi-Alli, A., Adekunle, A. & Awotunde, J. Network intrusion detection based on deep learning model optimized with rule-based hybrid feature selection. *Information Security Journal: A Global Perspective*. **29**, 267-283 (2020)
[39] Mohammadi, M., Al-Fuqaha, A., Sorour, S. and Guizani, M. Deep learning for IoT big data and streaming analytics: A survey. *IEEE Communications Surveys and Tutorials*. **20**, 2923-2960 (2018)
[40] Singh, S., Rathore, S. & Park, J. Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Generation Computer Systems*. **110** pp. 721-743 (2020)
[41] Atitallah, S., Driss, M., Boulila, W. & Ghézala, H. Leveraging Deep Learning and IoT big data analytics to support the smart cities development: Review and future directions. *Computer Science Review*. **38** pp. 100303 (2020)
[42] Dorri, A., Kanhere, S. & Jurdak, R. Towards an optimized blockchain for IoT. *Proceedings Of The Second International Conference On Internet-of-Things Design And Implementation*. pp. 173-178 (2017)
[43] Panarello, A., Tapas, N., Merlino, G., Longo, F. & Puliafito, A. Blockchain and iot integration: A systematic survey. *Sensors*. **18**, 2575 (2018)
[44] Kim, M., Hilton, B., Burks, Z. & Reyes, J. Integrating blockchain, smart contract-tokens, and IoT to design a food traceability solution. *2018 IEEE 9th Annual Information Technology, Electronics And Mobile Communication Conference (IEMCON)*. pp. 335-340 (2018)
[45] Sharma, A., Podoplelova, E., Shapovalov, G., Tselykh, A. & Tselykh, A. Sustainable smart cities: convergence of artificial

intelligence and blockchain. *Sustainability*. **13**, 13076 (2021)
[46] Balakrishna, C. Enabling technologies for smart city services and applications. *2012 Sixth International Conference On Next Generation Mobile Applications, Services And Technologies*. pp. 223-227 (2012)
[47] Obaidat, M. & Nicopolitidis, P. Smart cities and homes: Key enabling technologies. (Morgan Kaufmann,2016)
[48] Trencher, G. Towards the smart city 2.0: Empirical evidence of using smartness as a tool for tackling social challenges. *Technological Forecasting And Social Change*. **142** pp. 117-128 (2019)
[49] Chib, A., Alvarez, K. & Todorovic, T. Critical Perspectives on the Smart City: Efficiency Objectives vs Inclusion Ideals. *Journal Of Urban Technology*. **29**, 83-99 (2022)
[50] SwarnaSudha Detecting Website Defacement using Machine Learning Techniques. Journal of Next Generation Technology . *JNxtGenTech*. **1**, 47-55 (2021)
[51] Hassan, R., Zeebaree, S., Ameen, S., Kak, S., Sadeeq, M., Ageed, Z., AL-Zebari, A. & Salih, A. State of art survey for iot effects on smart city technology: challenges, opportunities, and solutions. *Asian Journal Of Research In Computer Science*. **8**, 32-48 (2021)
[52] Lohokare, J., Dani, R., Rajurkar, A. and Apte, A. An IoT ecosystem for the implementation of scalable wireless home automation systems at smart city level. *TENCON 2017-2017 IEEE Region 10 Conference*. pp. 1503-1508 (2017)
[53] Grycan, W. Legislative support for improving sustainable and smart electricity consumption in polish residential sector. *Journal Of Cleaner Production*. **266** pp. 121995 (2020)
[54] Abiodun, M., Adeniyi, E., Awotunde, J., Bhoi, A., AbdulRaheem, M. and Oladipo, I. A framework for the actualization of green cloud-based design for smart cities. *IoT And IoE Driven Smart Cities*. pp. 163-182 (2021)
[55] Oladipo, I., AbdulRaheem, M., Awotunde, J., Bhoi, A., Adeniyi, E. & Abiodun, M. Machine learning and deep learning algorithms for smart cities: a start-of-the-art review. *IoT And IoE Driven Smart Cities*. pp. 143-162 (2021)
[56] Allam, Z. & Jones, D. Future (post-COVID) digital, smart and sustainable cities in the wake of 6G: Digital twins, immersive realities and new urban economies. *Land Use Policy*. **101** pp. 105201 (2021)
[57] AbdulRaheem, M., Balogun, G., Abiodun, M., Taofeek-Ibrahim, F., Tomori, A., Oladipo, I. & Awotunde, J. An enhanced lightweight speck system for cloud-based smart healthcare. *Applied Informatics: Fourth International Conference, ICAI 2021, Buenos Aires, Argentina, October 28–30, 2021, Proceedings 4*. pp. 363-376 (2021)
[58] Dang, L., Kyeong, S., Li, Y., Wang, H., Nguyen, T. and Moon, H. Deep learning-based sewer defect classification for highly imbalanced dataset. *Computers and Industrial Engineering*. **161** pp. 107630 (2021)
[59] Chen, D., Wawrzynski, P. & Lv, Z. Cyber security in smart cities: a review of deep learning-based applications and case studies. *Sustainable Cities And Society*. **66** pp. 102655 (2021)
[60] Jaw, E. & Wang, X. Feature selection and ensemble-based intrusion detection system: an efficient and comprehensive approach. *Symmetry*. **13**, 1764 (2021)
[61] Liang, Y., Li, H., Guo, B., Yu, Z., Zheng, X., Samtani, S. & Zeng, D. Fusion of heterogeneous attention mechanisms in multi-view convolutional neural network for text classification. *Information Sciences*. **548** pp. 295-312 (2021)
[62] Mokhtari, S., Abbaspour, A., Yen, K. & Sargolzaei, A. A machine learning approach for anomaly detection in industrial control systems based on measurement data. *Electronics*. **10**, 407 (2021)
[63] Quincozes, S., Mossé, D., Passos, D., Albuquerque, C., Ochi, L. & Santos, V. On the performance of GRASP-based feature selection for CPS intrusion detection. *IEEE Transactions On Network And Service Management*. **19**, 614-626 (2021)
[64] Limon-Cantu, D. & Alarcon-Aquino, V. Multiresolution dendritic cell algorithm for network anomaly detection. *PeerJ Computer Science*. **7** pp. e749 (2021)
[65] Yue, Y., Li, S., Legg, P. & Li, F. Deep learning-based security behaviour analysis in IoT environments: A survey. *Security And Communication Networks*. **2021** pp. 1-13 (2021)
[66] Chen, J., Tian, Z., Cui, X., Yin, L. & Wang, X. Trust architecture and reputation evaluation for internet of things. *Journal Of Ambient Intelligence And Humanized Computing*. **10** pp. 3099-3107 (2019)
[67] Malik, S., Dedeoglu, V., Kanhere, S. & Jurdak, R. Trustchain: Trust management in blockchain and iot supported supply chains. *2019 IEEE International Conference On Blockchain (Blockchain)*. pp. 184-193 (2019)
[68] Chai, H., Leng, S., Zhang, K. & Mao, S. Proof-of-reputation based-consortium blockchain for trust resource sharing in internet of vehicles. *IEEE Access*. **7** pp. 175744-175757 (2019)
[69] Zhuang, Q., Liu, Y., Chen, L. & Ai, Z. Proof of reputation: A reputation-based consensus protocol for blockchain based systems. *Proceedings Of The 1st International Electronics Communication Conference*. pp. 131-138 (2019)
[70] Calvaresi, D., Mattioli, V., Dubovitskaya, A., Dragoni, A. & Schumacher, M. Reputation management in multi-agent systems using permissioned blockchain technology. *2018 IEEE/WIC/ACM International Conference On Web Intelligence (WI)*. pp. 719-725 (2018)
[71] Alkadi, O., Moustafa, N., Turnbull, B. & Choo, K. A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. *IEEE Internet Of Things Journal*. **8**, 9463-9472 (2020)
[72] Kolias, C., Kambourakis, G., Stavrou, A. and Gritzalis, S. Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset. *IEEE Communications Surveys and Tutorials*. **18**, 184-208 (2015)
[73] Hamza, A., Gharakheili, H., Benson, T. & Sivaraman, V. Detecting volumetric attacks on lot devices via sdn-based monitoring of mud activity. *Proceedings Of The 2019 ACM Symposium On SDN Research*. pp. 36-48 (2019)
[74] Naeem, H., Guo, B., Naeem, M., Ullah, F., Aldabbas, H. and Javed, M. Identification of malicious code variants based on image visualization. *Computers and Electrical Engineering*. **76** pp. 225-237 (2019)
[75] Kalash, M., Rochan, M., Mohammed, N., Bruce, N., Wang, Y. & Iqbal, F. Malware classification with deep convolutional neural networks. *2018 9th IFIP International Conference On New Technologies, Mobility And Security (NTMS)*. pp. 1-5 (2018)
[76] Kumar, R., Xiaosong, Z., Khan, R., Ahad, I. & Kumar, J. Malicious Code Detection Based on Image Processing Using

Deep Learning. *Proceedings Of The 2018 International Conference On Computing And Artificial Intelligence*. pp. 81-85 (2018)
[77] Alharbi, A., Alosaimi, W., Alyami, H., Rauf, H. & Damaševičius, R. Botnet attack detection using local global best bat algorithm for industrial internet of things. *Electronics*. **10**, 1341 (2021)
[78] Azeez, N., Odufuwa, O., Misra, S., Oluranti, J. & Damaševičius, R. Windows PE malware detection using ensemble learning. *Informatics*. **8**, 10 (2021)
[79] Toldinas, J., Venčkauskas, A., Damaševičius, R., Grigaliūnas, Š., Morkevičius, N. & Baranauskas, E. A novel approach for network intrusion detection using multistage deep learning image recognition. *Electronics*. **10**, 1854 (2021)
[80] Eden, S. The work of environmental governance networks: Traceability, credibility and certification by the Forest Stewardship Council. *Geoforum*. **40**, 383-394 (2009)
[81] Abikoye, O., Ojo, U., Awotunde, J. & Ogundokun, R. A safe and secured iris template using steganography and cryptography. *Multimedia Tools And Applications*. **79** pp. 23483-23506 (2020)
[82] Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V. & Others Scikit-learn: Machine learning in Python. *The Journal Of Machine Learning Research*. **12** pp. 2825-2830 (2011)
[83] Stein, G., Chen, B., Wu, A. & Hua, K. Decision tree classifier for network intrusion detection with GA-based feature selection. *Proceedings Of The 43rd Annual Southeast Regional Conference-Volume 2*. pp. 136-141 (2005)
[84] Goswami, S., Das, A., Chakrabarti, A. & Chakraborty, B. A feature cluster taxonomy based feature selection technique. *Expert Systems With Applications*. **79** pp. 76-89 (2017)
[85] Aslahi-Shahri, B., Rahmani, R., Chizari, M., Maralani, A., Eslami, M., Golkar, M. & Ebrahimi, A. A hybrid method consisting of GA and SVM for intrusion detection system. *Neural Computing And Applications*. **27** pp. 1669-1676 (2016)
[86] Hsu, C., Hsieh, H., Prakosa, S., Azhari, M. & Leu, J. Using long-short-term memory based convolutional neural networks for network intrusion detection. *Wireless Internet: 11th EAI International Conference, WiCON 2018, Taipei, Taiwan, October 15-16, 2018, Proceedings 11*. pp. 86-94 (2019)
[87] Lin, C., He, D., Zeadally, S., Kumar, N. & Choo, K. SecBCS: a secure and privacy-preserving blockchain-based crowdsourcing system. *Science China Information Sciences*. **63** pp. 1-14 (2020)
[88] Kochovski, P., Gec, S., Stankovski, V., Bajec, M. & Drobintsev, P. Trust management in a blockchain based fog computing platform with trustless smart oracles. *Future Generation Computer Systems*. **101** pp. 747-759 (2019)
[89] Kumar, R. & Tripathi, R. Blockchain-based framework for data storage in peer-to-peer scheme using interplanetary file system. *Handbook Of Research On Blockchain Technology*. pp. 35-59 (2020)
[90] Keshk, M., Sitnikova, E., Moustafa, N., Hu, J. & Khalil, I. An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems. *IEEE Transactions On Sustainable Computing*. **6**, 66-79 (2019)
[91] Keshk, M., Moustafa, N., Sitnikova, E. & Benjamin Turnbull Privacy-preserving big data analytics for cyber-physical systems. *Wireless Networks*. **28** pp. 1241–1249 (2018)
[92] Soe, Y., Feng, Y., Santosa, P., Hartanto, R. & Sakurai, K. Towards a lightweight detection system for cyber attacks in the IoT environment using corresponding features. *Electronics*. **9**, 144 (2020)
[93] Kumar, P., Gupta, G. and Tripathi, R. TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. *Journal Of Systems Architecture*. **115** pp. 101954 (2021)
[94] Bhattacharya, S., Maddikunta, P., Kaluri, R., Singh, S., Gadekallu, T., Alazab, M. and Tariq, U. A novel PCA-firefly based XGBoost classification model for intrusion detection in networks using GPU. *Electronics*. **9**, 219 (2020)
[95] Shafiq, M., Tian, Z., Sun, Y., Du, X. and Guizani, M. Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. *Future Generation Computer Systems*. **107** pp. 433-442 (2020)
[96] Shafiq, M., Tian, Z., Bashir, A., Du, X. and Guizani, M. IoT malicious traffic identification using wrapper-based feature selection mechanisms. *Computers and Security*. **94** pp. 101863 (2020)

Edited by: Kumar Abhishek
Special Issue on: Machine Learning and Block-chain based Solution for Privacy and Access Control in IoT
Received: May 11, 2023
Accepted: Aug 18, 2023