International Journal of Safety and Security Engineering
Vol. 15, No. 7, July, 2025, pp. 1415-1426
Journal homepage: http://iieta.org/journals/ijsse

Key Node Authentication Model Using Asymmetric Cryptography for Smart Cities

Nalluri Brahma Naidu*, Gondi Lakshmeewari

Department of Computer Science and Engineering, GITAM School of Technology, Gandhi Nagar, Rushikonda, Andhra Pradesh, Visakhapatnam 530045, India

Corresponding Author Email: nbrahmanaidu02@gmail.com

https://doi.org/10.18280/ijsse.150709

Received: 2 June 2025
Revised: 8 July 2025
Accepted: 18 July 2025
Available online: 31 July 2025

Keywords:
Internet of Things, data security, node authentication, node access control, asymmetric cryptography, smart city, Network Security

ABSTRACT

The Internet of Things (IoT) is rapidly expanding into a massive network with numerous applications, with an expected 41 billion devices linked by 2025 and creating around 79 zettabytes of data. The heterogeneous network will leverage communication and cloud technologies to bring a range of digital services that will drive smart city applications. Since these services are accessible remotely in a pervasive environment over public channels, securing user communication is of utmost importance. Internet of Things (IoT) networks need sufficient resources to deal with the growing number of security threats. Because of the exponential growth of IoT services, security measures need to be put in place right away. One typical issue with the security of their intercommunication is improper authentication between devices and people. The device access control system has to have reliable components that enable secure communication between devices and users. Cryptography, namely asymmetric methods for key generation and precise node authentication, is usually utilized to solve these security challenges. Crucial characteristics include the ability to access sensitive data, manage key secrecy, monitor, and safeguard sensors. Collaborative data processing and sharing is one scenario where the Internet of Things could be useful. In this case, the security of user-to-user communication depends on an effective authentication mechanism. This research proposes a Dual Key Authentication model using asymmetric cryptography model with Dual Access Control (DKA-AC-DAC) mechanisms in a smart city application. The proposed model, when contrasted with the traditional model, performs better in the node authentication and access control model. The proposed model achieved 99.1% accuracy in Dual Access Controlling and 98.8% accuracy in Node Authentication.

1. INTRODUCTION

Smart cities, made possible by the IoT, may be efficiently managed and have many possible uses, such as disaster prevention, environmental preservation, and tourism. On the other hand, since the IoT has connected them to networks, city management systems are more likely to be the target of hackers [1]. If a smart city infrastructure were to be attacked in this way, vital urban services might become useless. Furthermore, it is critical to efficiently handle this data because the smart city deals with both public and private data, some of which contains sensitive personal information [2]. The term IoT describes a rapidly developing system of linked computing devices, sensors, and other tangible objects that can collect, analyze, and disseminate data [3]. Globally, more and more people are incorporating the IoT paradigm into their everyday lives to make them better. Education, smart farming, logistics, manufacturing, medical applications, advertising, and urban planning are just a few examples of these industries. These applications significantly affect people's daily lives [4]. The smart city based on IoT is a critical application that affects people's lives and where unchecked security flaws could cause serious harm. The IoT is a cutting-edge new technology that enables the linking of physical items with digital services offered by the web [5]. Many industries and types of businesses rely on it now because it is an integral part of the fourth industrial revolution [6]. The IoT offers numerous capabilities, such as detection, identification, data processing, and communication, to various sectors, including transportation, healthcare, business, and agriculture [7]. The IoT enabled smart city model is shown in Figure 1.

Despite the proliferation of IoT devices, several security risks have emerged from careless planning for IoT rollouts [8]. Each of the three main tiers that comprise the IoT is susceptible to its own distinct set of dangers. Attacks such as replay attacks, phony nodes, distributed denial-of-service (DDoS), and denial-of-service (DoS) might affect the perception layer. Data accessibility, privacy, authentication, and application layer efficiency are all impacted by network layer attacks such as man-in-the-middle (MITM), eavesdropping, sniffing, and routing [9]. Thus, security vulnerabilities could appear at any point in the system, including data processing, storage, or communications between devices. To address these security challenges, the IoT design incorporates several security requirements [10]. To protect against different kinds of attacks, authentication and permission are crucial requirements that must be satisfied at every level. Multiple frameworks have been proposed as answers to the problems of user-device authentication, authorization, and access control in the IoT [11].

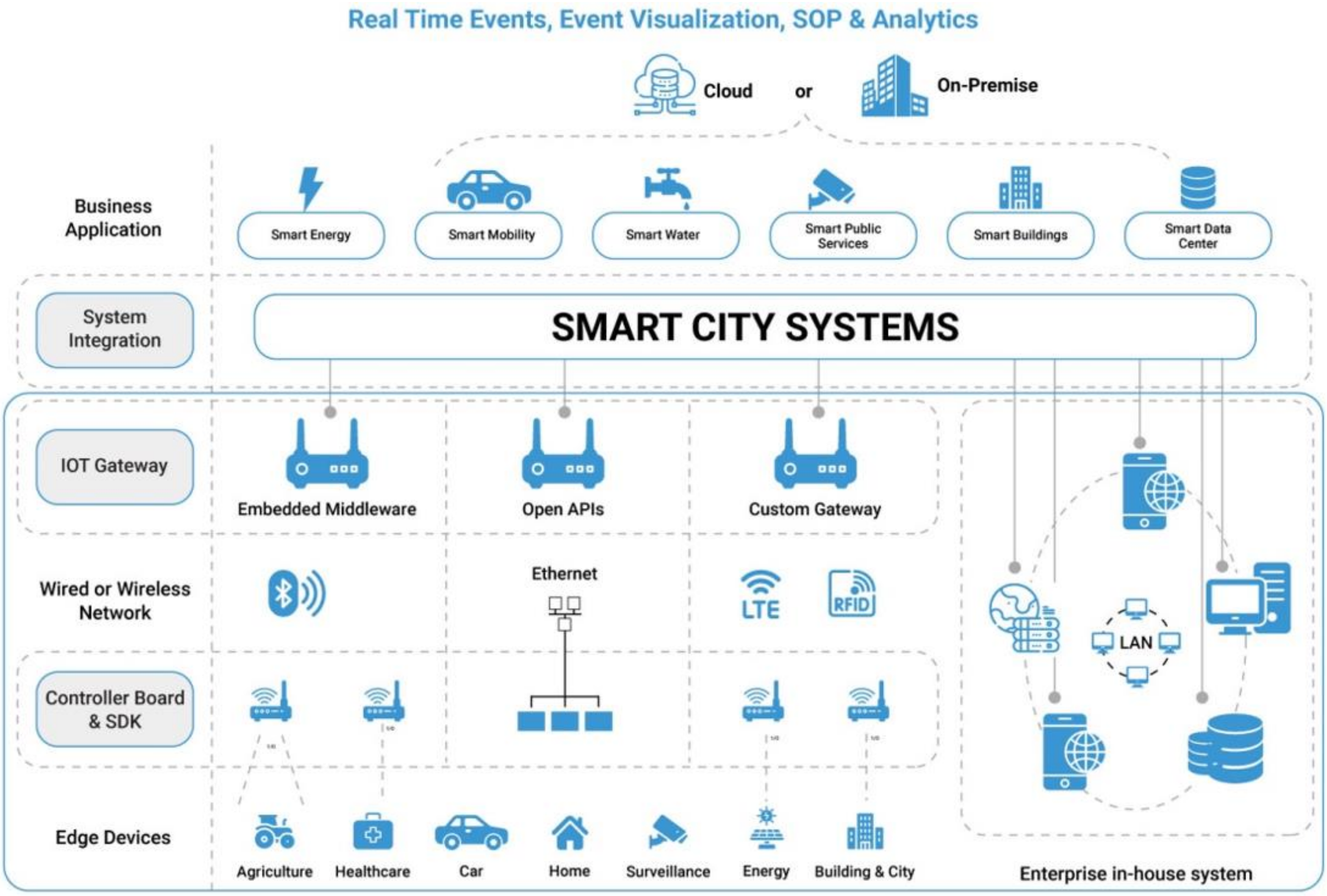

Figure 1. IoT enabled smart city

Various methods for verifying the identity of users or devices have been proposed as potential options for implementing efficient access control in an IoT setting. A number of studies have made use of OAuth, an open standard framework for web-wide authorization [12], to delegate authorization in IoT contexts. An effective authorization management system, IoT-OAuth makes use of centralized servers and the tokens they provide [13]. However, the central server acts as a single point of failure and may be susceptible to various security threats. To mitigate this risk, various studies have investigated the feasibility of decentralized systems as a substitute for centralized authorization servers [13]. Preventing security risks created by granting rights to unauthorized parties inside access control mechanisms requires ensuring the authenticity of authentication methods and granting access exclusively to authorized users. Authentication in the context of access control management requires extreme caution. Considering authentication as a presumption for authorization is fraught with threat [14]. The general process of IoT node authentication is shown in Figure 2.

Information gathered from IoT devices can be transmitted using a variety of protocols, including message queue telemetry transport (MQTT) and constrained application protocols (CoAPs). An abundance of transmission protocols exists that can enhance the link between networks and IoT devices [15]. The more traditional sensors utilized in smart cities or homes to gauge fan speed or temperature are different from IoT devices and sensors due to the requirement for precision and safety. In urban areas, pipes, power sources, sewage, garbage cans, temperature, and tall mountains can all create physical access issues with devices that are meant to be part of the IoT [16]. Even simple tasks like changing batteries or updating software can require a lot of operational work in some places, making it hard or expensive to accomplish the task quickly. New security methods and layers are required to enable message transmission across IoT devices and applications because this expected scenario renders the built-in security mechanisms useless. Data mining in urban areas typically makes use of IoT devices that gather information from a broad range of sources [17].

There are several issues with data security, device authentication, and access control that arise from the fast growth of the IoT, especially in smart city settings. Problems with resource scarcity [18], device heterogeneity, and susceptibility to impersonation, replay, and man-in-the-middle attacks are just a few of the ways in which traditional authentication methods fail to adequately protect IoT devices [19]. To improve the authentication and access control mechanisms tailored to smart city IoT applications, this research presents a new model called Dual Key Authentication with Dual Access Control. The model makes use of asymmetric cryptography. To enhance node verification and secure resource utilization, the suggested model proposes generating and distributing a set of three keys: one for authentication, one for access control, and one for data protection [20]. This technique differs from previous centralized or single-key systems. To improve the safety and efficiency of the network, the system chooses a high-performance central node to oversee and control all authentication processes [21]. IoT smart city infrastructures are now far more reliable and resilient with this model.

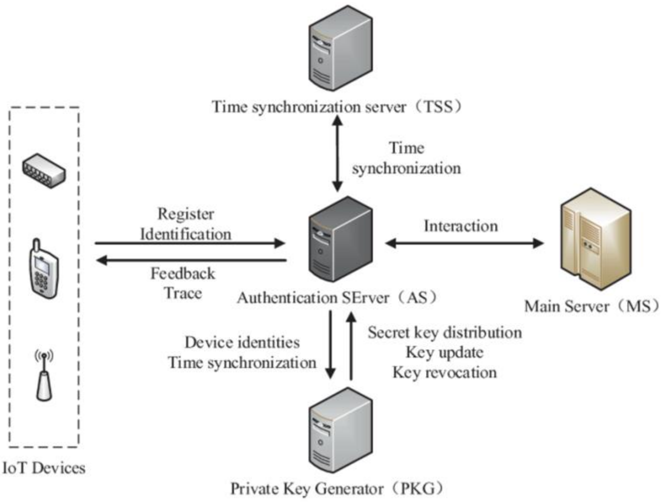

Figure 2. General procedure of IoT node authentication

Since data transmission occurs via an unprotected and vulnerable medium, it is crucial to protect data from threats such as unlawful eavesdropping, tampering, and unauthorized access [22]. In order to access sensitive information, hackers will often impersonate legitimate users and manipulate data by adding, deleting, or editing it [23]. The majority of these concerns could be mitigated by using suitable authentication techniques that are consistent with the architecture of the IoT [24]. Mutual authentication is vital for determining the device's and application's integrity. For the IoT, several solutions have been created to ensure secure key exchange and mutual authentication. In order to safeguard the IoT node from different security risks and to lessen the communication and computational demands, a reliable and efficient authentication method should be set up [25]. The strategy should also guarantee that the data is accessible, intact, and kept confidential. This research proposes a Dual Key Authentication model using asymmetric cryptography model with Dual Access Control (DKA-AC-DAC) mechanisms in a smart city application.

2. LITERATURE SURVEY

The proliferation of smart cities and the subsequent demand for a diverse array of drones has piqued the interest of both academics and industry leaders in the concept of the Internet of Drones (IoD). The IoT, infrastructure offers a wide range of services, such as monitoring traffic and the environment, and managing disasters. Still, in IoD-based smart city settings, drone-to-drone communication could pose security risks owing to the transmission of sensitive data across apps across an unsecured channel. Since IoDs can function in unsupervised settings with minimal human intervention, physical capture attacks can target smart devices integrated into these designs. Since drones have limited resources in the fields of processing and communication, public key cryptography (PKC) is impractical to employ. Yu et al. [1] created SLAP-IoD, a compact and safe authentication protocol for the IoT that utilizes a physical unclonable function (PUF), to guarantee reliable and useful services in smart city environments.

Smart city networks and the broad use of automobiles have increased scholarly interest in the IoV in recent years. The problem is that safeguarding such a network is among the most challenging and time-consuming tasks in the contemporary world. In order to achieve this goal, the improvement of the privacy and security of smart city systems, conventional works have created numerous networking frameworks and methodologies. There are still significant downsides, such as algorithms that are difficult to create, longer processing times, less maintenance, and no effective authenticity checking. Khadidos et al. [2] provided a novel approach to smart city Network Security. Here, the Collaborative Mutual Authentication (CMA) procedure, a user's private key, public key, session key, and the resulting hash function are all that's needed to confirm their identity. Additionally, the author employed the Meta-heuristic Genetic Algorithm - Random Forest (MGA-RF) technique to detect network attacks in order to guarantee the smart city's security.

Smart city projects rely heavily on intelligent transportation systems, which are made possible in large part by the Internet of Vehicles (IoV), a subset of the larger IoT. Because the IoV requires connectivity everywhere and at all times, conventional networking solutions aren't up to the task. The space-air-ground-integrated network (SAGIN) is widely believed to be the best infrastructure for connecting IoV. Lam et al. [3] presented a framework for understanding the security issues of complex IoT systems and proposed a security reference architecture for assessing security risks and satisfying security requirements. The author offered an activity-network-things (ANT) centric security reference architecture based on the three architectural approaches utilized to study IoT systems: device, Internet, and semantic. The author's focus here is on the problems with the existing models for IoT system design, which are largely based on corporate system architecture with some tweaks made to account for features specific to IoT networks. This solution can simplify the management of security risks by identifying the mission-critical functions performed by different IoT microperimeters. To account for the business and application-level security concerns raised by the IoT, the suggested architecture uses a methodical approach to understanding security requirements and selecting specific parameters for individualized security controls.

Smart buildings, smart cities, and electric vehicle charging are just a few of the many new uses for the rapidly evolving smart grid (SG) technology, which makes good use of complex communication architecture. However, because to the public channel running below, these services are extremely vulnerable. There have been some security measures proposed recently to deal with these dangers. Since some of these methods are vulnerable to key compromise impersonation (KCI) and related attacks, a reliable authentication mechanism is necessary for the SG infrastructure. An innovative method of protecting SG communication is presented by Chaudhry et al. [4] to enable smart meter and neighborhood area network gateway direct device-to-device authentication. Compared to related schemes, the proposed system is more secure and completes the authentication procedure with the least communication cost. It is designed to withstand KCI and related assaults.

The official announcement states that the IPv4 address architecture will no longer be used due to the rapid expansion of the IoT. The industry's needs for next-generation communication technologies have been fully met by IPv6. A smart home is an innovative style of dwelling that enhances human life by integrating numerous electronic gadgets onto the internet through the IoT. Many low-power smart devices are connected with 6LoWPAN so that the smart home can be controlled remotely. Security issues, especially those related to authentication, arise because cellular communication makes use of vulnerable communication paths. A trustworthy and transportable remote authentication method is necessary to guarantee secure communication in the next-generation smart home environment. There have been a lot of new authentication systems introduced recently, however they all rely on the same slow mathematical protocols that are a drain on resources like communication and processing. Ashraf et al. [5] proposed a reliable and portable technique of remote authentication for the next generation of Internet-of-Things smart homes. Both informal and rigorous security assessments utilizing the AVISPA tool determine the resilience of our suggested approach. In addition, this authentication system was implemented on a Linux-based client-server network architecture using Android programming.

Regardless of fluctuations in user density, the scalability of services in smart city applications can be facilitated by the IoT. Many customers require a variety of safety procedures to ensure that application services are reliable and efficient. In this case, a PDoS (permanent denial of service) happened because the user identification was not reliable. Alsayaydeh et al. [6] discussed service-dependent application authentication (SRAA), a method for defending smart cities against DDoS attacks. Using the controlled access distribution mechanism, this authentication solution guarantees the application's safety. The user's app and device's synchronization capabilities are utilized by the monitored access distribution. Backpropagation (BP) learning is the best method for error detection when dealing with user devices, implementation, and verification connections. In order to reduce the given weights, BP learning employs anomalies learned during the first access distribution phase. Now that the irregularity has been identified in the order of previous training eras, coordinated permission for distributed services can be achieved. As a result of PDoS, fewer weights lose service, which in turn reduces the frequency of service failures for connected devices.

The smart grid utilizes the IoT to improve metering capabilities, dependability, and management, which benefits both power customers and generators. The security of the fast expanding smart home and smart city industries is becoming more important as data networks are becoming more reliant on energy networks. The safety of the smart house must be guaranteed. An authentication method based on ChaCha20-Poly1305 Authentication with Associated Data (AEAD) and the most recent LoRa 2.4 GHz technology a robust and highly adaptable transmission protocol are both used by Kane et al. [7] for Home Area Network (HAN) design. Ultimately, this results in a network that protects users' privacy while encrypting and authenticating them with symmetric keys, achieving an excellent performance-to-security ratio. A performance investigation is conducted utilizing a real-world test bench to determine the impact of the proposed security measures on the LoRa network. The suggested secure design in the study barely affects packet transmission time when contrasted with a network that employs no security mechanisms at all.

Making sure that messages sent via smart city vehicular communications are safe is still a challenging challenge. The vast majority of studies that addressed the topic of data security relied on CRLs and the Public Key Infrastructure. This endeavor was not without its flaws, though. The lengthy validation procedure and enormous size of CRLs are the first issues. Two, connecting Basic Safety Messages (BSMs) that aren't encrypted poses a risk of tracing attacks. Thirdly, a malicious actor may be able to obtain secret keys from the storage areas of parked vehicles or RSUs. To address these issues, Othman et al. [8] provided Secret Sharing, a physically secure method of privacy-preserving message authentication that makes use of the Physical Unclonable Function (PUF). The suggested approach protects users against both active and passive threats, and it does so even if memory leaks. By reassembling a secret polynomial-share using their PUF, entitiescan establish pairwise temporal secret keys (PTKs) with other entities. This approach encrypts BSMs alongside existing protocols to further enhance security and thwart vehicle tracing attacks. It is not necessary for RSU to broadcast CRLs in order to revoke a vehicle. Only RSU distributes a secure offset key for threshold Secret Sharing.

The rapid advancement of IoT technology has made the security of sensitive data a top priority in many resource-asymmetric smart environments, such as smart homes, smart farms, and others. The user and device sides of a system would be in a resource-asymmetry situation if they had limited access to the gateway side's availability of resources. Consequently, a secure and practical method for establishing authentication keys for these smart environments is urgently required. In resource-asymmetric smart environments, most of the recently developed authentication and key establishment schemes do not adequately address resource excesses at the gateway, do not guarantee user anonymity, and are excessively burdensome on both the user and the smart device. Due to the large difference in the time required to encrypt and decrypt, the Rabin cryptosystem is ideal for developing authentication and key establishment systems in resource-asymmetric smart environments. So, using the Rabin cryptosystem as a foundation, Bai et al. [9] offered a fresh, realistic approach to smart environment authentication and key establishment in the context of resource asymmetry. This method ensures user anonymity, achieves lightweight operations on devices and users alike, and makes greater use of the rich resources of gateways. By combining Proverif with BAN logic, the author showed that this system is completely secure and anonymous.

There are a number of proposed frameworks in the field of Internet of Things security that aim to solve the problems of smart city access control and device authentication. Authentication protocols like OAuth and IoT-OAuth, which are based on central servers and use single keys, have been the mainstay of traditional systems. These methods work in some situations, but they have a major flaw: if one of the central servers or keys gets compromised, the entire network might be at risk. For example, in smart city environments based on the IoT, the SLAP-IoD protocol improves device security by using Physical Unclonable Functions for authentication. However, it still has problems guaranteeing scalability and flexibility in real-time applications, particularly in the extremely dynamic IoT networks.

Collaboration between users for mutual authentication employing session keys, private/public keys, and meta-heuristic algorithms for attack detection is proposed in subsequent studies. For time-sensitive smart city applications, these models still have a ways to go before they can address the resource limitations of IoT devices and the communication latency problems that plague them. However, they do help to increase authentication accuracy and decrease security threats. In low-power devices or diverse IoT contexts, these models generally struggle to balance compute costs with security strength.

To overcome these shortcomings, the DKA-AC-DAC model proposes asymmetric cryptography for dual key generation, which entails assigning three separate keys, one for authentication, one for access control, and one for data security to each device in the smart city network. The current solutions usually depend on a single key or centralized authentication, therefore this is a big change. This architecture stands out due to its dual access control method, which blocks unwanted users and makes sure data stays confidential and intact by limiting network resource access to authenticated nodes based on dynamic permission levels. Having a centralized node assessment head that watches how nodes are behaving and chooses the most trustworthy ones to communicate with greatly improves trust management in the network.

Because it incorporates real-time authentication and access control with little computational cost, the DKA-AC-DAC model is more flexible and robust than other existing models. This makes it an ideal choice for resource-constrained IoT devices. The experimental results show that the suggested model beats the traditional systems in terms of dual access control, key distribution efficiency, and node authentication accuracy.

Proposed Model Uniqueness

1. By utilizing three keys, one for authentication, one for access control, and one for data security, the DKA-AC-DAC paradigm provides superior security compared to conventional models that rely on a single key for authentication.
2. Enhancing granularity and dynamic security management, the dual-level access control system grants nodes secure access based on authentication and authorization.
3. The model incorporates a central node assessment head (CNAH) to keep an eye on how nodes are behaving and choose the most reliable ones to communicate with, which strengthens the network even more.
4. The suggested approach guarantees minimum computational overhead, which makes it appropriate for resource-limited IoT devices while yet ensuring excellent security, allowing for efficient use of resources.

3. PROPOSED MODEL

As one of the most cutting-edge technological developments in the last several years, the IoT has piqued the curiosity of academics and IT experts alike. According to experts, establishing mutual authentication between IoT devices and IoT servers is essential for ensuring the security of the entire IoT system [26]. Relying on a single password for authentication makes the system vulnerable to dictionary and side-channel attacks. IoT authentication is only a paradigm for establishing confidence in the identifiers of IoT servers and devices [27]. Data transmission across an unsecured network, such as the internet, can be better regulated and protected with this. It is critical to have strong IoT authentication in place to protect data from control orders that could be sent by hostile actors or unauthorized machines [28]. Protecting sensitive data from hackers who pose as official IoT services or devices is another critical use case for authentication [29]. A number of researchers have attempted to ascertain the best way to accomplish the necessary level of authentication for IoT servers and devices. Centralized, distributed, two-way, and one-way authentication are all types that fit within this category. Keep in mind that the IoT is not just one technology, but rather a network of interrelated things that may function independently of humans [30]. The objective of the IoT authorization procedure is to lay the groundwork for confirming the genuineness of every endpoint inside the larger IoT system. As a common practice, when enrollment is entered, the certification method is set up to educate service providers how to confirm the system's identity when registering [31]. The primary goal of machine identity management is, thus, to regulate and build confidence in machine identities. These devices can communicate with gateways, apps, clouds, and other devices.

IoT gadgets like smart plugs, lights, and speakers, as well as mobile devices, home security systems, surveillance cameras, engine control units for automobiles and factories, and countless more could be the reason behind this. Each IoT device should have its own unique digital identity that it may utilize when connecting to the main server or gateway; this will assist prevent unauthorized individuals from gaining access to the system [32]. Each IoT device has its own unique cryptographic key, which we use to associate identities with them. Methods for managing machine identities are crucial when attempting to ascertain the credentials used by various devices. System administrators are able to keep tabs on IoT servers and devices by assigning them unique identifiers. This allows for secure communication, lifetime monitoring, and the prevention of harmful program execution. When any IoT server or device starts behaving strangely, system administrators can simply disable it.

This shift in dynamics necessitates an extremely natural approach to smart city development in order to maximize synergies. The Internet of Things platform has been receiving constant modifications over the last many years. The ever-increasing practicality and applicability of the technology has benefited numerous fields, including smart cities, public health, and environmental monitoring. With the advent of the IoT, the emphasis has shifted from one-on-one communication between humans to the internet as a whole, which can handle any type of data transfer. While this has served its purpose, it has also introduced certain risks and challenges. Information privacy, security, and access control has become increasingly important in recent years. Cybercriminals and other bad actors find the IoT platform irresistible because it opens up new possibilities for them to conduct crimes and launch more extensive attacks. One challenge with IoT security is that, depending on their use cases, requirements for IoT servers and devices must handle issues related to information availability, integrity, and confidentiality. More importantly, improving authentication mechanisms to safeguard IoT servers and devices has not been a primary emphasis of current research.

The quantity of servers and devices that comprise the IoT has increased at an exponential rate. Because of the limitations and requirements of these interconnected devices, there has been an increasing number of related problems, the most of which revolve on inadequate authentications. This becomes an even bigger deal when users think about how limited the resources are that the IoT is using. This is due to the fact that traditional security measures are ineffective. Concerns over the security of the IoT are far from overdue due to the widespread use of IoT devices and servers as well as their incorporation into mission-critical applications, the latter of which could amplify the consequences of a security breach. The ideal scenario would be for an IoT network's security architecture to solely take into account the authentication, integrity, confidentiality, and availability needs of the applications it supports. If users want IoT servers and devices to run smoothly, authentication is the one thing they need, according to experts. Trusting these IoT devices is crucial for constructing a dependable network. Reason being, malicious actors could use a single infected node to cause system-wide failure or other disasters. When it comes to servers and devices connected to the IoT, traditional authentication approaches are either impractical or inappropriate. In order to utilize IoT devices and the numerous applications that operate on them, service users must enroll in the IoT and have access to it. It has legal title to the resources that the IoT intends to use. The proposed model framework is shown in Figure 3.

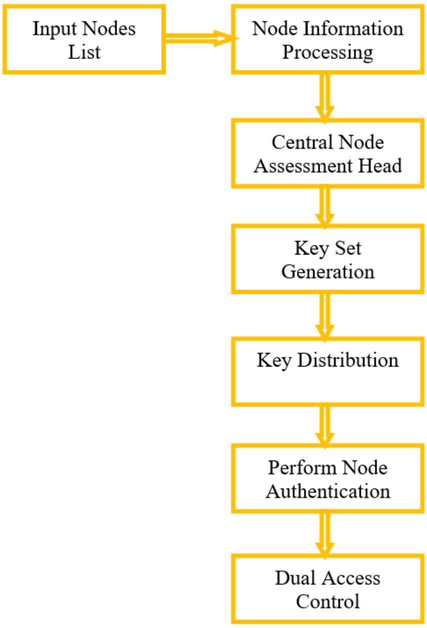
Input Nodes List
Node Information Processing
Central Node Assessment Head
Key Set Generation
Key Distribution
Perform Node Authentication
Dual Access Control

Figure 3. Proposed model framework

The network paradigm, in which physical things, including sensor-based devices, communicate via wireless or wired connections and gather data on critical interactions within the network, is directly tied to the vulnerability of applications built on the IoT. Important security flaws, including as man-in-the-middle and denial-of-service attacks, can manifest in the data that is transmitted, processed, and stored. Smart city security and privacy could be seriously compromised if data collection and transfer through IoT infrastructure is not adequately protected. This research proposes a Dual Key Authentication model using asymmetric cryptography model with Dual Access Control mechanisms in smart city application.

Algorithm DKA-AC-DAC

{

Input: Nodes List {Nlist}

Output: Authorized Nodes List {ANlist}, Access Granted Nodes List {AGlist}

Step-1: The nodes information will be considered for all the registered nodes in the smart city. Each node information helps in detection of nodes and also for correspondence during transmission. The node information processing and Node Immutable Token (NIT) is allocated to each registered node. The process of NIT allocation is performed as:

$$Ninfo[M] = \sum_{n=1}^{T} getnodeaddr(n) + \gamma\big(Nlist(n)\big) + \tau\big(Nlist(n)\big)$$

$$NITalloc[M] = \sum_{n=1}^{T} getVal\big(Ninfo(n)\big) + TI\big(Ninfo(n)\big) + \max\big(\gamma(n)\big) + NTh$$

Here γ indicates the transmission range, τ represents energy allocated.

Step-2: The proposed model considers a Central Node Assessment Head (CNAH) node to monitor all the nodes in the network. This CNAH node will monitor the properties of all nodes and maintains a log report. The node which has the best properties are considered as CNAH node that is performed as:

$$CNAH[M] = \prod_{n=1}^{T} \max\,(PDR(n)) + \max\,(\gamma\big(Ninfo(n)\big) + \max\,(\tau(Ninfo(n)))$$

Step-3: The proposed model uses asymmetric cryptography model and generates key set. The proposed model generates key set that contains 3 keys in the set. A key for authentication and a key for data security and a key for access control. The key generation and key distribution is performed as:

$$R[M] = \sum_{n=1}^{T} getrandVal(n)$$

$$KeyP[M] = \sum_{n=1}^{T} getVal(n)$$

$$KeyPr[M] = \sum_{n=1}^{T} getPrimeVal(n) > KeyP(n)$$

$$S[M] = \sum_{n=1}^{T} KeyP(n) \oplus KeyPr(n)|R$$

$$KeyPub[M] = \sum_{n=1}^{T} \left(\frac{KeyPr(n)}{KeyP} + S(n) \ll 2\right)|(S(n) \oplus KeyPr(n))\,|R(n)$$

$$KeyPri[M] = \sum_{n=1}^{T} \left(\frac{KeyPr(n)}{S} + KeyP(n) \ll 4\right) \oplus (S(n)|KeyPr(n))\,\&R(n)$$

Step-4: The generated keys will be distributed to the requested nodes so that access control can be granted to requested nodes. The node authentication will be performed using the key in the key set, and only authenticated nodes will be involved in communication. The node authentication is performed as:

$$NodeAuthen[M] = \sum_{n=1}^{T} getVal\big(KeyPub(n)\big) + CNAH\big(NITalloc(n)\big) + \delta\big(NITalloc(n)\big)\begin{cases} NodeAuthen(n) \leftarrow 1\ if\ \ N(KeyPub) == getkey(KeyPub(n)) \\ NodeAuthen(n) \leftarrow 0 \qquad\qquad\qquad\qquad Otherwise \end{cases}$$

Step-5: Access control is the procedure of granting and revoking access to a set of available resources in the smart city. The nodes access control will be granted based on the request and based on the key provided. The dual level access control is performed as:

$$Daccess[M] = \sum_{n=1}^{T} NITalloc(n) + getVal\big(KeyPri(n)\big) + NodeAuthen(n) + getVal(KeyPub(n))\begin{cases} DAccess(n) \leftarrow 1\ if\ N(KeyPri) == getkey(KeyPub(n)) \\ DAccess(n) \leftarrow 0 \qquad\qquad\qquad\qquad Otherwise \end{cases}$$

}

To improve the safety and performance of smart city networks that rely on the IoT, the DKA-AC-DAC paradigm was developed. Triple access control, node authentication, and key generation are the model's primary tenets. The production of cryptographic keys is the most computationally intensive step, with a time complexity of O(n log n), where n is the number of bits utilized in the key. Asymmetric cryptography necessitates modular exponentiation, which is why this occurs. For every given network node m, the temporal complexity of the key distribution process, which entails transmitting keys to those nodes, is O(m). However, for large-scale installations, this phase could use up some network traffic, despite its efficiency. Since these procedures include straightforward cryptographic operations, such as digital signature verification and access control checks, the dual access control and node authentication algorithms have a constant time complexity of O(1) for every node following key distribution.

The model's architecture prioritizes efficiency in resource-constrained IoT contexts. Due to the complexity of asymmetric cryptography, key generation uses CPU time and memory. Network capacity is not a concern during the key distribution phase, but bigger networks may encounter congestion if not handled correctly. Devices with little processing capacity are well-suited for node authentication and access control since these processes consume little resources. They primarily include verifying digital signatures and looking up entries in access control lists. Because of its compact architecture, the model can function efficiently on low-powered Internet of Things devices without sacrificing security.

4. RESULTS

There is a lot of data produced by IoT devices, and some of it is sensitive. Protecting the devices and the data they gather is critical to keeping the IoT system running smoothly, as it relies on sensed data for all of its important decisions. If any malicious device were to have access to the IoT network, it may disrupt normal system operation and lead to disastrous effects. Several components of security for the IoT include data aggregation, non-repudiation, availability, confidentiality and integrity. Conversely, authentication and access control are the main safeguards that guarantee data access is limited to authorized users. Data privacy and authenticity are ensured in secure IoT systems through the use of mutual authentication between devices and other systems. Data corruption, theft, and unauthorized access are just some of the security dangers that these systems face if this isn't done. The idea behind decentralized, minimum-delay IoT systems is that they will make data interchange and valuable service provision easier. This means that dispersed security measures are required to keep these systems safe.

In order to assess how well the DKA-AC-DAC model performed in IoT scenarios with limited resources, the experiments were implemented in Python and run using Google Colab, a cloud-based platform that was both convenient and scalable. Key generation, authentication, and node communication were all significantly accelerated by the hardware setup at Google Colab, which comprises NVIDIA Tesla T4 GPUs and Intel Xeon CPUs. Even in the face of massive network loads and IoT simulations, the model maintained efficiency with the GPU acceleration, which drastically cut down on the processing time required to handle cryptographic operations. The software tools used in Google Colab for implementing the DKA-AC-DAC model included Python 3.8, with libraries such as PyCryptodome for asymmetric encryption and cryptographic key management, and Flask for managing the Central Node Assessment Head (CNAH).

Authentication procedures and other IoT devices cannot use existing security measures due to their inability to scale and their reliance on centralized. Methods for delay-sensitive authentication and access control are more necessary than ever before due to the heterogeneity, limited resources, and mission-critical conditions in which many IoT devices must operate. An aerial drone that runs on batteries, for example, may need to rapidly authenticate with many command stations before it can send data that is time-sensitive. Nodes reduce latency by relocating control, storage, communication, and management to the network's periphery rather than constructing dedicated channels to a remote infrastructure that is more centrally located. Access control is necessary to ensure the privacy of residents, which is directly related to the security of the smart city's systems and subsystems. For instance, if an intruder gains access to smart home gadgets, they might potentially eavesdrop on users privacy and security issues surrounding smart homes.

Urban areas that are integrated, livable, and sustainable can be achieved through the intelligent and coordinated application of all available resources; this is what the smart city concept is all about. In order to alleviate possible environmental issues or limitations, it would be beneficial to make cities smart by making good use of the abundance of new, inventive technologies and paradigms. In addition to their importance in addressing environmental issues, smart cities strive to enhance the quality of life for citizens and maximize the efficiency of public services by maximizing the use of resources and minimizing expenses. A number of procedures and technologies pertaining to communication and networking, real-time control, and big data analytics form the bedrock of smart city applications. The efficient provision of services to inhabitants depends on the proper and seamless integration of these components of a smart city infrastructure. Every enabling technology possesses distinct characteristics. There are new concerns about privacy and security brought about by the interconnection and interaction of the various components of smart cities and their individual attributes. For smart city security to be guaranteed, it is important to permit access to these components. This research proposes a Dual Key Authentication model using asymmetric cryptography model with Dual Access Control (DKA-AC-DAC) mechanisms in smart city application. The proposed model is compared with the traditional Secure and Lightweight Authentication Protocol Using Physical Unclonable Functions for Internet of Drones in Smart City Environments (SLAP-IoD) and Intelligent Security Framework Based on Collaborative Mutual Authentication Model for Smart City Networks with Meta-heuristic Genetic Algorithm – Random Forest (CMA-MGA-RF) technique. The proposed model exhibits better results when compared with the traditional models.

The proposed model maintains the complete information of nodes in the network. Each node's information will help to communicate with the node and also for node recognition. Table 1 and Figure 4 show the Node Information Accessing Accuracy Levels.

Table 1. Node information accessing accuracy levels

Nodes in the Network	Models Considered		
	DKA-AC-DAC Model	SLAP-IoD Model	CMA-MGA-RF Model
50	97.7	93.9	92.5
100	97.8	94.1	92.7
150	97.9	94.3	92.9
200	98.1	94.4	93.1
250	98.3	94.6	93.3
300	98.4	94.7	93.5

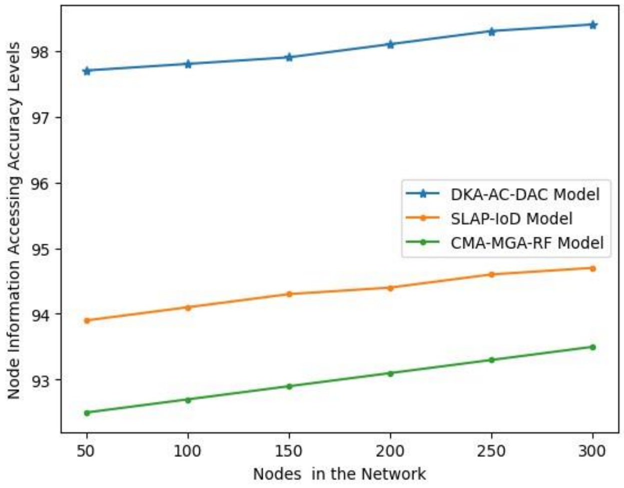

Figure 4. Node information accessing accuracy levels

The proposed model selects a node that is best in its performance as the central node for assessing the nodes in the network. The nodes' transmission process and changes in patterns will be monitored by the central node. The Central Node Assessment Head Selection Accuracy Levels are indicated in Table 2 and Figure 5.

Table 2. Central node assessment head selection accuracy levels

Nodes in the Network	Models Considered		
	DKA-AC-DAC Model	SLAP-IoD Model	CMA-MGA-RF Model
50	97.9	93.4	94.0
100	98.1	93.6	94.2
150	98.3	93.8	94.5
200	98.5	94.0	94.6
250	98.7	94.1	94.8
300	98.9	94.3	95

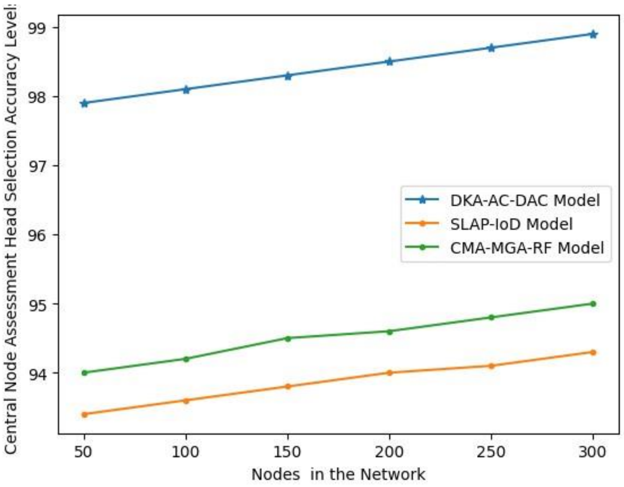

Figure 5. Central node assessment head selection accuracy levels

Table 3. Key generation time levels

Nodes in the Network	Models Considered		
	DKA-AC-DAC Model	SLAP-IoD Model	CMA-MGA-RF Model
50	12.1	17.0	21.0
100	12.3	17.2	21.2
150	12.5	17.4	21.4
200	12.7	17.6	21.6
250	12.8	17.9	21.8
300	13	18	22

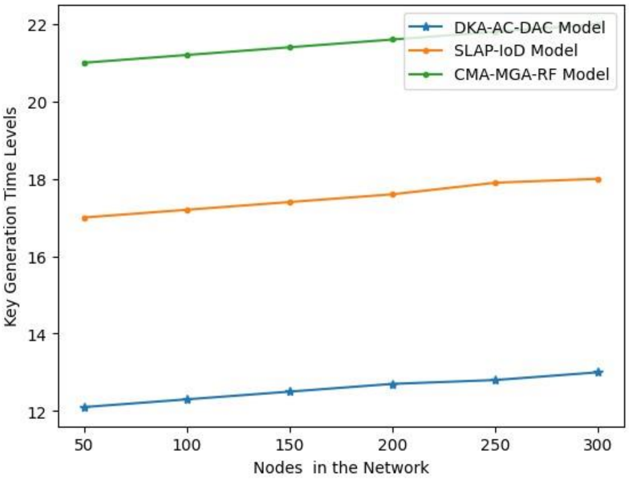

Figure 6. Key generation time levels

The proposed model generates the keys for node authentication and also for granting access to the network resources. The proposed model generates a key set that contains 3 keys. One key is used for authentication, another key for access control, and the last key for data security. The Key Generation Time Levels are indicated in Table 3 and Figure 6.

The proposed model distributes the generated keys to the registered nodes in the network. The keys shared will be used for one time only. The distributed keys are used for authentication and access control in the smart city network. The Key Distribution Accuracy Levels are indicated in Table 4 and Figure 7.

Table 4. Key distribution accuracy levels

Nodes in the Network	Models Considered		
	DKA-AC-DAC Model	SLAP-IoD Model	CMA-MGA-RF Model
50	98.2	94.3	93.7
100	98.4	94.5	93.9
150	98.6	94.7	94.0
200	98.8	94.9	94.2
250	99.0	95.1	94.4
300	99.2	95.3	94.6

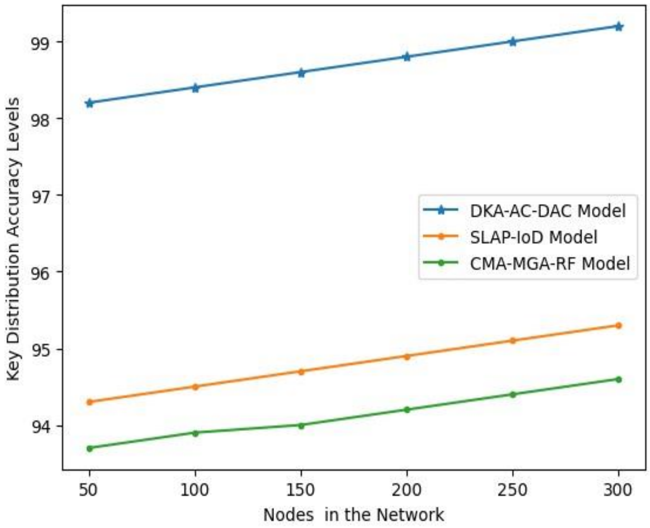

Figure 7. Key distribution accuracy levels

Table 5. Node authentication accuracy levels

Nodes in the Network	Models Considered		
	DKA-AC-DAC Model	SLAP-IoD Model	CMA-MGA-RF Model
50	97.8	93.7	95.0
100	98.0	93.8	95.2
150	98.2	93.9	95.4
200	98.4	94.0	95.6
250	98.6	94.3	95.8
300	98.8	94.5	96

Node authentication is the process of identifying whether a node is a genuine node that has normal behaviour or not. The node authentication is performed by a key in the key set. The nodes that are authenticated only will be allowed to request access. The Node Authentication Accuracy Levels are shown in Table 5 and Figure 8.

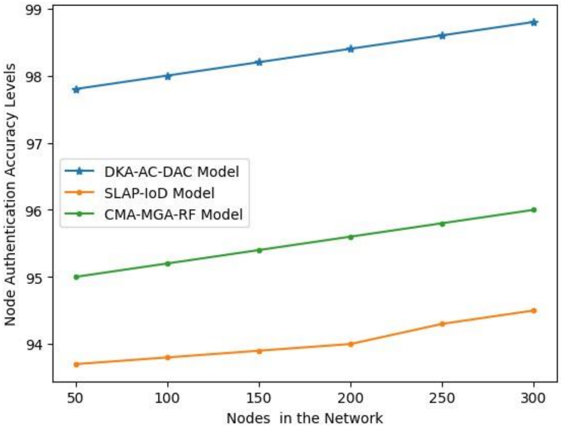

Figure 8. Node authentication accuracy levels

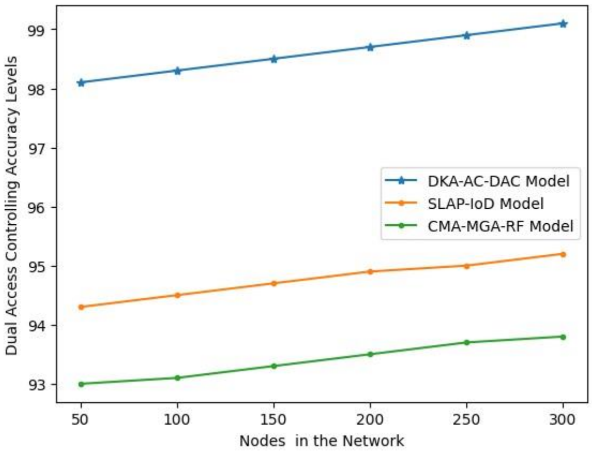

Figure 9. Dual access controlling accuracy levels

Table 6. Dual access controlling accuracy levels

Nodes in the Network	Models Considered		
	DKA-AC-DAC Model	SLAP-IoD Model	CMA-MGA-RF Model
50	98.1	94.3	93.0
100	98.3	94.5	93.1
150	98.5	94.7	93.3
200	98.7	94.9	93.5
250	98.9	95.0	93.7
300	99.1	95.2	93.8

Table 7. Network Security levels

Nodes in the Network	Models Considered		
	DKA-AC-DAC Model	SLAP-IoD Model	CMA-MGA-RF Model
50	97.9	93.9	92.3
100	98.1	94.0	92.5
150	98.3	94.2	92.7
200	98.5	94.4	92.9
250	98.7	94.6	93.0
300	98.9	94.8	93.2

The proposed model allows for granting dual access control for accessing the resources and for transmitting the data in the network. The dual access control will increase the security levels in the network. The Dual Access Controlling Accuracy Levels are depicted in Table 6 and Figure 9.

The proposed model strictly authenticates the nodes using the generated keys, and only authenticated nodes will be allowed to participate in communication. The access control is also provided to authorized nodes and only to those nodes that requested any access. The Network Security Levels are indicated in Table 7 and Figure 10.

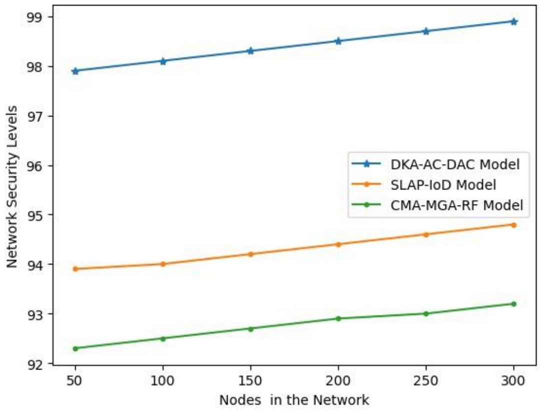

Figure 10. Network Security levels

When tested against other models of Internet of Things security, the DKA-AC-DAC model proved to be the best in all three areas: node authentication, key distribution, and dual access control. Node authentication and security in smart city IoT applications are often handled by more conventional models like SLAP-IoD and CMA-MGA-RF. The outcomes, including authentication accuracy (98.8%) and dual access control effectiveness (99.1%), demonstrate a noticeable improvement over these models.

Node Authentication Accuracy Comparison

DKA-AC-DAC Model: Achieved an impressive 98.8% authentication accuracy across different scales (50 to 300 nodes), demonstrating the model's ability to securely authenticate IoT devices within a large-scale network.

SLAP-IoD: The SLAP-IoD model, which uses PUFs for authentication in smart city IoT environments, performed slightly lower, with authentication accuracy of 93.9% for 50 nodes, and progressively improving as the network size grew. However, its performance still lags behind the DKA-AC-DAC model due to scalability issues and reliance on a centralized system for key management.

CMA-MGA-RF: The CMA-MGA-RF technique, which combines collaborative mutual authentication and a meta-heuristic genetic algorithm for attack detection, achieved 92.5% authentication accuracy at 50 nodes. While it offers strong attack detection capabilities, its node authentication accuracy is still inferior to the DKA-AC-DAC model, especially when scaled to larger networks.

This comparative analysis shows that the DKA-AC-DAC model provides higher accuracy in authenticating IoT nodes, benefiting from its dual key mechanism and asymmetric cryptography, which ensure more reliable and flexible authentication compared to the PUF-based SLAP-IoD or the mutual authentication approach in CMA-MGA-RF.

Key Distribution Efficiency Comparison

DKA-AC-DAC Model: The key distribution efficiency was evaluated by examining the time required for key distribution and accuracy of key delivery. The DKA-AC-DAC model demonstrated low distribution time, with a key distribution accuracy of 99.2%, making it highly efficient for large-scale IoT networks.

SLAP-IoD: While SLAP-IoD uses PUFs to enhance security, it has limitations in key distribution. Its key distribution accuracy was 94.3%, lower than that of DKA-AC-DAC, likely due to the central server's reliance and potential bottlenecks in large-scale deployments.

CMA-MGA-RF: The key distribution in CMA-MGA-RF showed 94.0% accuracy, lower than both SLAP-IoD and DKA-AC-DAC, as the genetic algorithm approach does not effectively address the dynamic key distribution challenges in IoT networks, particularly for large-scale deployments.

5. CONCLUSION

With the help of the IoT, smart cities are able to upgrade their infrastructure, transportation systems, and public services, thereby raising the standard of living for all residents. As smart city apps provided by the Internet of Things gain popularity, it will be necessary to put measures in place to meet the varied needs of these applications. Cyber assaults and breaches are becoming more common as the number of linked devices grows. In order to prevent assaults that could affect citizens and institutions, it is essential to secure these systems. Interoperability issues, expense, and complexity exist on top of memory, processor, and energy usage limits. Testing and analysis on-site is necessary for designing and implementing the right security controls for the devices and services. In comparison to previous approaches such as SLAP-IoD and CMA-MGA-RF, the experimental results show that the propsoed DKA-AC-DAC model greatly enhances the security of IoT networks in smart city settings. The suggested approach is well-suited for large-scale, real-time applications in smart cities due to its use of asymmetric cryptography and dual key mechanisms, which allow for more secure node communication, faster key distribution, and granular access control. In order to facilitate safe communication between devices inside the same IoT system as well as between devices in other IoT systems, this research suggests a novel authentication and access control mechanism for the IoT. This research proposes a Dual Key Authentication model using asymmetric cryptography model with Dual Access Control mechanisms in smart city application. The proposed model achieved 99.1% accuracy in Dual Access Controlling and 98.8% accuracy in Node Authentication.

Future Work

Integrating methods for periodic key rotation and dynamic key generation is an encouraging research concept for future research that could aid in adapting the model to evolving smart city user behavior and network conditions. To improve the model's response to security risks, real-time key updates could be included. This would allow for the replacement of compromised keys without interrupting ongoing conversations. Additionally, the system's resistance against persistent threats, such as replay attacks and man-in-the-middle attacks, would be enhanced by this.

The wide variety of smart city applications such as healthcare, energy systems, and traffic management necessitates further study into improving the DKA-AC-DAC paradigm to individual use cases. A similar level of real-time key distribution and low-latency authentication is crucial for smart traffic systems. To make sure it can adapt to the individual needs of different IoT-driven services in smart cities, it could be helpful to develop scalable and modular versions of the model. In future, dynamic size keys generation and time-limited access control models can be designed to increase the Quality of Service levels and also to increase security levels in smart cities.

REFERENCES

[1] Yu, S., Das, A.K., Park, Y., Lorenz, P. (2022). SLAP-IoD: Secure and lightweight authentication protocol using physical unclonable functions for internet of drones in smart city environments. IEEE Transactions on Vehicular Technology, 71(10): 10374-10388. https://doi.org/10.1109/TVT.2022.3188769

[2] Khadidos, A.O., Shitharth, S., Manoharan, H., Yafoz, A., Khadidos, A.O., Alyoubi, K.H. (2022). An intelligent security framework based on collaborative mutual authentication model for smart city networks. IEEE Access, 10: 85289-85304. https://doi.org/10.1109/ACCESS.2022.3197672

[3] Lam, K.Y., Mitra, S., Gondesen, F., Yi, X. (2021). ANT-centric IoT security reference architecture—Security-by-design for satellite-enabled smart cities. IEEE Internet of Things Journal, 9(8): 5895-5908. https://doi.org/10.1109/JIOT.2021.3073734

[4] Chaudhry, S.A., Nebhan, J., Yahya, K., Al-Turjman, F. (2021). A privacy enhanced authentication scheme for securing smart grid infrastructure. IEEE Transactions on Industrial Informatics, 18(7): 5000-5006. https://doi.org/10.1109/TII.2021.3119685

[5] Ashraf, Z., Sohail, A., Hameed, A., Farhan, M., Alotaibi, F.A., Alnfiai, M.M. (2023). Robust and lightweight remote user authentication mechanism for next-generation IoT-based smart home. IEEE Access, 11: 137899-137910. https://doi.org/10.1109/ACCESS.2023.3336763

[6] Alsayaydeh, J.A.J., Ali, M.F., Al-Andoli, M.N.M., Herawan, S.G. (2024). Improving the robustness of IoT-powered smart city applications through service-reliant application authentication technique. IEEE Access, 12: 19405-19417. https://doi.org/10.1109/ACCESS.2024.3361407

[7] Kane, L., Liu, V., McKague, M., Walker, G.R. (2022). Network architecture and authentication scheme for LoRa 2.4 GHz smart homes. IEEE Access, 10: 93212-93230. https://doi.org/10.1109/ACCESS.2022.3203387

[8] Othman, W., Fuyou, M., Xue, K., Hawbani, A. (2021). Physically secure lightweight and privacy-preserving message authentication protocol for VANET in smart city. IEEE Transactions on Vehicular Technology, 70(12): 12902-12917. https://doi.org/10.1109/TVT.2021.3121449

[9] Bai, L., Hsu, C., Harn, L., Cui, J., Zhao, Z. (2022). A practical lightweight anonymous authentication and key establishment scheme for resource-asymmetric smart environments. IEEE Transactions on Dependable and Secure Computing, 20(4): 3535-3545. https://doi.org/10.1109/TDSC.2022.3203874

[10] Mandal, S., Bera, B., Sutrala, A.K., Das, A.K., Choo, K.K.R., Park, Y. (2020). Certificateless-signcryption-based three-factor user access control scheme for IoT environment. IEEE Internet of Things Journal, 7(4): 3184-3197. https://doi.org/10.1109/JIOT.2020.2966242

[11] Yu, S., Lee, J., Park, K., Das, A.K., Park, Y. (2020). IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment. IEEE Access, 8: 167875-167886. https://doi.org/10.1109/ACCESS.2020.3022778

[12] Khan, M.A., Ullah, I., Kumar, N., Oubbati, O.S., Qureshi, I.M., Noor, F., Khanzada, F.U. (2021). An efficient and secure certificate-based access control and key agreement scheme for flying ad-hoc networks. IEEE Transactions on Vehicular Technology, 70(5): 4839-4851. https://doi.org/10.1109/TVT.2021.3055895

[13] Das, A.K., Bera, B., Wazid, M., Jamal, S.S., Park, Y. (2021). iGCACS-IoD: An improved certificate-enabled generic access control scheme for internet of drones deployment. IEEE Access, 9: 87024-87048. https://doi.org/10.1109/ACCESS.2021.3089871

[14] Narayana, V.L., Sujatha, V., Prasanna, T.V.N., Pavani, V., Ranganarayana, K. (2025). An efficient blockchain model for improving data transmission rate in ad hoc networks. International Journal of Wireless and Mobile Computing, 28(4): 407-415. https://doi.org/10.1504/ijwmc.2025.146632

[15] Mishra, B., Garg, D., Narang, P., Mishra, V. (2020). Drone-surveillance for search and rescue in natural disaster. Computer Communications, 156: 1-10. https://doi.org/10.1016/j.comcom.2020.03.012

[16] Yahuza, M., Idris, M.Y.I., Ahmedy, I.B., Wahab, A.W.A., Nandy, T., Noor, N.M., Bala, A. (2021). Internet of drones security and privacy issues: Taxonomy and open challenges. IEEE Access, 9: 57243-57270. https://doi.org/10.1109/ACCESS.2021.3072030

[17] Ismagilova, E., Hughes, L., Rana, N.P., Dwivedi, Y.K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. Information Systems Frontiers, 24(2): 393-414. https://doi.org/10.1007/s10796-020-10044-1

[18] Narayana, V.L., Bharathi, C.R. (2023). Efficient route discovery method in MANETs and packet loss reduction mechanisms. International Journal of Advanced Intelligence Paradigms, 25(1-2): 129-140. https://doi.org/10.1504/IJAIP.2023.130818

[19] Kisseleff, S., Martins, W.A., Al-Hraishawi, H., Chatzinotas, S., Ottersten, B. (2020). Reconfigurable intelligent surfaces for smart cities: Research challenges and opportunities. IEEE Open Journal of the Communications Society, 1: 1781-1797. https://doi.org/10.1109/OJCOMS.2020.3036839

[20] Wang, D., Bai, B., Lei, K., Zhao, W., Yang, Y., Han, Z. (2019). Enhancing information security via physical layer approaches in heterogeneous IoT with multiple access mobile edge computing in smart city. IEEE Access, 7: 54508-54521. https://doi.org/10.1109/ACCESS.2019.2913438

[21] Ali, Z., Chaudhry, S.A., Ramzan, M.S., Al-Turjman, F. (2020). Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles. IEEE Access, 8: 43711-43724. https://doi.org/10.1109/ACCESS.2020.2977817

[22] Shitharth, S., Prasad, K.M., Sangeetha, K., Kshirsagar, P.R., Babu, T.S., Alhelou, H.H. (2021). An enriched RPCO-BCNN mechanisms for attack detection and

classification in SCADA systems. IEEE Access, 9: 156297-156312. https://doi.org/10.1109/ACCESS.2021.3129053

[23] Singh, S., Sharma, P.K., Yoon, B., Shojafar, M., Cho, G.H., Ra, I.H. (2020). Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. Sustainable Cities and Society, 63: 102364. https://doi.org/10.1016/j.scs.2020.102364

[24] Tian, Y., Wang, Z., Xiong, J., Ma, J. (2020). A blockchain-based secure key management scheme with trustworthiness in DWSNs. IEEE Transactions on Industrial Informatics, 16(9): 6193-6202.

[25] Haque, A.B., Bhushan, B., Dhiman, G. (2022). Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends. Expert Systems, 39(5): e12753. https://doi.org/10.1111/exsy.12753

[26] Peneti, S., Sunil Kumar, M., Kallam, S., Patan, R., Bhaskar, V., Ramachandran, M. (2021). BDN-GWMNN: Internet of Things (IoT) enabled secure smart city applications. Wireless Personal Communications, 119(3): 2469-2485. https://doi.org/10.1007/s11277-021-08339-w

[27] Chen, W., Xiao, S., Liu, L., Jiang, X., Tang, Z. (2020). A DDoS attacks traceback scheme for SDN-based smart city. Computers & Electrical Engineering, 81: 106503. https://doi.org/10.1016/j.compeleceng.2019.106503

[28] Singh, D., Pati, B., Panigrahi, C.R., Swagatika, S. (2020). Security issues in IoT and their countermeasures in smart city applications. In Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2018. Springer, Singapore, pp. 301-313. https://doi.org/10.1007/978-981-15-1483-8_26

[29] Saadi, M., Noor, M.T., Imran, A., Toor, W.T., Mumtaz, S., Wuttisittikulkij, L. (2020). IoT enabled quality of experience measurement for next generation networks in smart cities. Sustainable Cities and Society, 60: 102266. https://doi.org/10.1016/j.scs.2020.102266

[30] Ranaweera, P., Jurcut, A.D., Liyanage, M. (2021). Survey on multi-access edge computing security and privacy. IEEE Communications Surveys & Tutorials, 23(2): 1078-1124. https://doi.org/10.1109/COMST.2021.3062546

[31] Qi, S., Yang, X., Yu, J., Qi, Y. (2023). Blockchain-aware rollbackable data access control for IoT-enabled digital twin. IEEE Journal on Selected Areas in Communications, 41(11): 3517-3532. https://doi.org/10.1109/JSAC.2023.3310061

[32] Hamad, M., Finkenzeller, A., Liu, H., Lauinger, J., Prevelakis, V., Steinhorst, S. (2022). SEEMQTT: Secure end-to-end MQTT-based communication for mobile IoT systems using secret sharing and trust delegation. IEEE Internet of Things Journal, 10(4): 3384-3406. https://doi.org/10.1109/JIOT.2022.3221857