International Journal of Medical Toxicology & Legal Medicine Volume 27, No. 2, 2024
e-ISSN: 0974-4614
p-ISSN: 0972-0448

Dual Key Authentication Model with Cryptography enabled Data Transmission Model in Smart Cities

V.Pavani[1], V.Lakshman Narayana[2], Suryaprakash Nalluri[3], Adapa Srinivasa Rao[4] , Murali Mohan Malyala[5]

[1,2] Vignan's Nirula Institute of Technology and Science for Women, Peda Palakaluru, Guntur, Andhra Pradesh, India.
[3]Senior Vice President, Information Security Operations Group Manager, Information, Security, University of Cumberland, Williamsburg, USA
[4] Department of Artificial intelligence & data science, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India.
[5] Vice President, Information Security Lead, Computer Science Department, Osmania University, Telangana, India.
Email: manojpavani81@gmail.com[1],lakshmanv58@gmail.com[2],spnalluri@gmail.com[3], asr.unguturu@gmail.com[4], mohanmalyala@gmail.com[5]

Received: 15.08.2024 Revised: 10.09.2024 Accepted: 06.10.2024

ABSTRACT
The high pace at which smart cities are developing introduce numerous challenges which should be addressed to fully secure all interconnected and data-driven infrastructure. The security aspect mandates a more advanced security paradigm which would help keep all sensitive information within the jurisdiction of its creators and ensure secure communication between all devices. Thus, this research will advance a dual-key authentication model designed to ensure the safeguarded transmission of data within smart cities by including asymmetric encryption. The model is designed to advance a security paradigm which bases the security of the well-proven efficiency of symmetric encryption of the data which is then distributed among authorized users and the optimal security in case of asymmetric encryption for key exchange and user authentication. Specifically, the data is encrypted by a symmetric key and then roasted across the authorized bridge to the nearest authorized user. The key used to encrypt the data is shared through public medium and private key is securely maintained. Therefore, the symmetric key which is raised to transfer the data across the bridge is encrypted using the public key before sending it to a remote user who decrypts using their private key. Asymmetric encryption is optimal for sending a symmetric key because it is subjected to encryption algorithms which utilize symmetric encryption execute faster and are more economically viable thus optimal for transferring large volumes of data fast. This research proposes a Dual Key Authentication Model with Cryptography enabled Data Transmission Model in Smart Cities (DKAM-CDTM). Since the data is sent across the bridge, while asymmetric encryption is optimal for key exchange, authentication and transmission. Therefore, the model will mitigate against the most common security vulnerabilities in smart city context including interception and acquisition of the key, hacking into the system and key management. It secures the transmission and utilization of the key. Finally, the proposed model will be tested through a simulation to establish the encryption of the time taken to secure data, and authenticate potential security threats. The factorial tests conducted applications that have proven that the dual-key is by fact an optimal way of transferring data in a smart city. The proposed model achieved 98.8% accuracy in Dual Key Authentication, 98.9% accuracy in Key Generation and 99.4% accuracy in providing Data Security. The proposed model efficiently provides security to the smart city model that is used for secure data transmission.

keywords: Smart Cities, Cryptography, Dual-Key Authentication, Symmetric Encryption, Asymmetric Encryption, Key Pair, Secure Data Transmission.

1. INTRODUCTION

The traffic congestion, environmental deterioration, resource scarcity, and deterioration of people' quality of life that are consequences of urbanization have grown in prominence alongside the ever-increasing city populations and the establishment of new urban agglomerations. The idea of smart cities was put up to help cities achieve sustainable growth. There is a global tendency toward faster and faster development in information and communication technology. Beginning with the concept proposal and ending with the application landing, a number of critical technologies are implemented, including 5G networks, the Internet of Things (IoT), cloud

computing, big data analysis, and new generation geographic information systems. With the advent of these technologies, new possibilities for smart city development is in raise, such as novel approaches to urban administration and a plethora of new urban application scenarios.

The ability to intelligently perceive one's physical surroundings is provided by the terminal perception layer in smart city architecture. This layer also makes it possible to identify, collect data about, monitor, and control the city's infrastructure through sensor networks and devices. Smart meters, cameras, smart embedded devices, home automation systems, and other terminal devices are becoming commonplace as a result of the fast growth of mobile communication technologies and the IoT. The proliferation of IoT terminal devices has improved people's lives, but it has also given cybercriminals more opportunities to launch attacks. Most of the data acquired by the IoT devices in smart cities is sensitive; as a result, there is a real risk that attackers may eavesdrop on or otherwise manipulate this data for their own gain, which might have devastating effects. Wearable embedded devices gather physiological data from people, which might put their lives in jeopardy if it were to leak or be manipulated with during transmission; smart meters gather data on electricity use, which could reveal the user's life behavior track if it were to leak. Terminal communication services in smart cities must be protected from eavesdropping and tampering with data transmitted by IoT devices. Damage or major security incidents resulting from data leakage or tampering can cripple smart city business applications. Therefore, end-to-end encryption and device authentication are essential.

The notion of smart cities has rapidly transitioned from a science-fiction vision to a tangible reality across many regions of the world. Smart cities refer to urban areas that utilize technology, data analytics, and interconnected devices to enhance the quality of life of residents, optimize resource utilization, and ensure sustainability. Internet of Things (IoT) devices, connected infrastructure, digital communication networks, and data-driven services constitute the core elements of smart cities. However, as cities grow increasingly smarter and more interconnected, the demand for robust security solutions becomes necessary to safeguard sensitive data and guarantee the dependability and safety of services. Indeed, one of the critical aspects challenging the creation of smart cities is the security and privacy of the massive volumes of data produced and transmitted across systems. Such cities gather data from an array of sources, including traffic sensors, surveillance cameras, utility meters, and public systems. Moreover, the info will frequently be exchanged between devices and used to extract information that can be used to enhance the decision-making process. The general process of using cryptography for data security is shown in Figure 1.

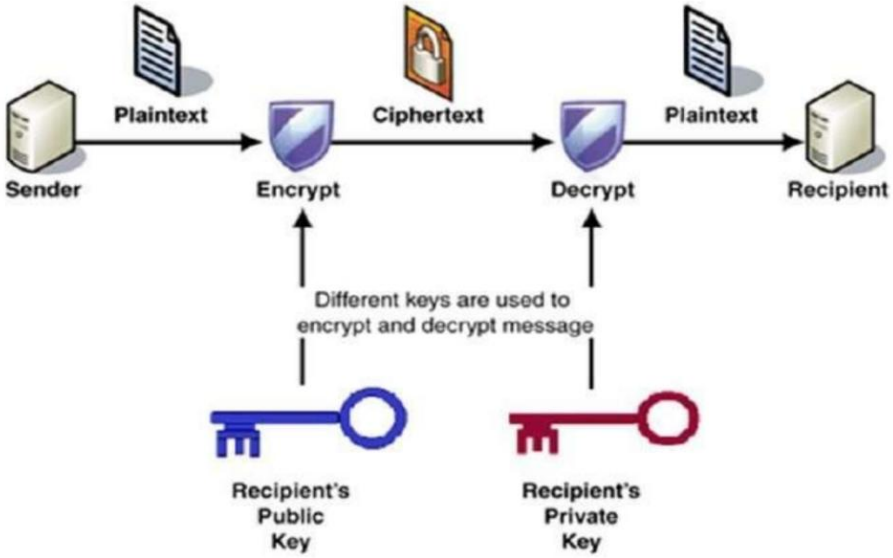

Fig 1: Cryptography General Process

This inherently creates a wide surface of assault, making smart cities susceptible to various types of cyber-attacks, access protocols, data breaches, and other forms of cyber threats. Therefore, encryption and authentication are necessary components for ensuring such data security. While encryption ensures that information conveyed across networks stays confidential, authenticating data ensures the identity of all included parties in the communication process. Commonly, current security protocols are based on symmetric or asymmetric methods for encryption. Specifically, the symmetric approach is characterized by speed and effectiveness but necessitates secure key management and distribution. On the other hand, asymmetric security is known for its robust authentication capabilities and key sharing, but it is hampered by limited speed due to its

high computational complexity. Hence, this research outlines a cryptography-enabled data communication system with novel dual key authenticated model, specifically for smart cities to address these concerns. Indeed, the proposed model utilizes asymmetric technique.

Secure key exchange employs asymmetric encryption, while rapidity of data transmission is ensured by symmetric encryption. It guarantees that sensitive data cannot be accessed and reduces or eliminates unauthorized entry, allowing the model to be scalable and adaptable to multiple smart city needs. Because it is typically applicable, this model is admissible to many unique scenarios: secure communication among IoT devices, encrypted data exchange among smart city infrastructures, and protected entry to authenticated city services. Smart Cities have emerged as a solution to counter the complicated phenomenon of cities in the contemporary world of rapid urbanization and modern technology advancement. Smart Cities take advantage of different existing technologies to optimize the management of resources, enhanced public service delivery and, in turn, the life quality of the citizens. However, the Smart City integrates all the digital systems and IoT infrastructure, creating substantial issues regarding the security of data and data processing. Data transmission and authentication are among the most vital aspects of any Smart City. The password-based data processing system is insecure because of the numerous attacks and insecurity, such as brute attacks. Dare transmission in the open platform is prone to interception and authorization. To improve security, this research proposes to improve the data transmission system using a Dual Key Authentication Model integrated with the Cryptography-enabled Data Transmission Model to be used in a Smart City. The dual key authentication model is external security enhancements on top of the advances in the IoT systems of Smart City. The public and private keys in the proposed approach will be processed using the public-key cryptography that uses large public keys. The public keys will be paired with the private keys in a public-key cryptography system to create secure data transmission channels.

2. LITERATURE SURVEY

The Internet of vehicles has gained umpteen interest due to its variety of benefits, such as vehicle emergence, accidents, pollution level, and traffic congestion. The need for a variety of cars and the concept of smart cities give rise to it. In addition, IoV offers a variety of services in smart cities. This is made possible by linking Vehicle ad-Hoc network and the IoT. Regrettably, in an IoV-based smart city assemblage, communicating important messages on an insecure route causes vehicle-to-vehicle communication to be easily assaulted in several security areas. Consequently, in order to offer a variety of IoV services in a smart city assemblage, the transmission of messages in an encrypted way for information is required. A secure message authentication protocol was presented by S. Yu et al. [1] for Internet of Vehicle communication in smart cities. Impersonation, secret key exposure, and off-line guessing assaults are just a few of the vulnerabilities found in the examined scheme. The authentication is not assured in the examined scheme. Moreover, a novel protocol named IoV-SMAP is designed. The unique protocol administers the employed scheme’s examined vulnerabilities.

The Internet of automobiles is of interest to a growing amount of scholars since the formation of smart city systems and increasing automobile usage. However, security for such a network is one of the most difficult and most time-consuming tasks now in existence. Many networking architectures and technology were produced for this purpose by conventional works, all with the goal of improving the security and privacy of urban information systems. However, there is insufficient authenticity verification, greater design complexity, a longer processing time, and less maintenance. As a result, an innovative security framework using a variety of strategies for smart city networks is the primary goal of this work performed by A. O. Khadidos et al. [2]. The Cooperative Complementary Authentication (CMA) mechanism is utilized to authenticate users, using the developed hash function, private key, public key, and session key to evaluate the user identity. The security of the smart city is provided by the Meta-heuristic genetic algorithm – Random Forest method (MGA-RF) to detect network threats.

As we delve farther into smart cities, the interplay between various IoT sensors and devices grows increasingly complex and vulnerable across the Internet. The massive amounts of data generated by these diverse gadgets leave them open to a wide range of harmful attacks. Secure processing and analysis of the collected data is required for informed decision-making. The massive amounts of data produced by the IoT are making smart urban planning a reality. In this article, H. Zhang et al. [3] showcased SafeCity, a new architectural framework that brings to light the smart city ecosystem that comprises of physical devices such as cameras and sensors. There are three levels to SafeCity's architecture: data security, data computation, and decision-making. To prevent unauthorized parties from accessing sensitive information, the first layer employs payload-based symmetric encryption to ensure that only legitimate data is exchanged between physical devices. Computing encrypted data makes advantage of the second layer. The last layer is responsible for gleaning insights from the data. The author used Raspberry Pi boards to guarantee data interchange security and the Hadoop framework to evaluate data computation on reliable datasets.

The most up-to-date tech-driven solutions for improving urban dwellers' quality of life through the development of more environmentally friendly, efficient, and linked communities are smart city apps built on the IoT. For

sustainable city performance improvement, communication nodes are networked autonomously to monitor situations that necessitate higher energy efficiency and security. Security breaches in smart cities applications are common due to the large number of connected devices; these breaches can have devastating effects on a city's infrastructure, citizens' safety, and economic growth. Although computing at the edge and Green IoT greatly improve network performance in processing and data storage, low-powered sensors still have constraints in battery life, transmission spectrum, and security problems. So, for sustainable cities, it's crucial to have a cutting-edge method for transmitting data securely from energy resources. Consequently, R. R. Irshad et al. [4] suggested an IoT platform for smart cities called Intelligent Buffalo-based Maintain Edge-enabled Computing (IB-SEC). The goal of this framework is to improve the efficiency and reliability of communication while reducing energy consumption and data transmission latency. To improve the efficiency, protection, and reliability of data transmission in connected to the internet of smart city networks, the developed IB-SEC platform uses a combination of the African Buffalo Optimisation (ABO) algorithm and a Global Hash function-based security algorithm.

It is still a tough task to ensure secure message delivery in smart city vehicular communications. To guarantee security and privacy, the majority of the associated work used the Public Key Infrastructure and Certification Revocation Lists (CRLs). But there were a few problems with these works, including: 1) the lengthy inspection process and the large size of CRLs; 2) traceability attacks using linked unencrypted Fundamental Safety Messages (BSMs); and 3) an adversary's ability to steal secret keys from parked vehicles or RSU storage. W. Othman et al. [5] provided a physically safe privacy-preserving message authentication mechanism called Secret Sharing that utilizes Physical Unclonable Function (PUF) to solve the problems highlighted before. Security and privacy are guaranteed by the proposed protocol, even in the face of memory leakage, against passive and aggressive attacks. In order to establish pairwise temporally secret keys (PTKs) with other entities, the entities use their PUF to reassemble a secret polynomial-share. To further increase security and prevent vehicle traceability attacks, this protocol encrypts BSMs in addition to existing protocols (using PTKs). No broadcasting of CRLs is necessary for RSU to revoke a vehicle. Rather, RSU solely uses threshold Secret Sharing to distribute a secure offset key. A result of this is that the revocation checking procedure has O(1) computational complexity.

Advanced metering features, enhanced dependability, and administration are just a few of the numerous advantages that energy consumers and producers reap from the smart grid that is based on the Internet of Things. Because data networks are running parallel to electricity networks, security is becoming more of an issue with the proliferation of smart cities and smart homes. It is of utmost importance to ensure that a smart house is secured using excellent procedures. Using the new LoRa 2.4 GHz technology, a strong and highly adjustable transmission standard, L. Kane et al. [6] suggested a design for a Home Area Network (HAN) and an authentication system based on ChaCha20-Poly1305 Secure Encryption with Attached Data (AEAD). By utilizing asymmetrical key-based encryption and authentication strategy, this leads to a network that strikes a balance between performance considerations and the provision of confidentiality, integrity, and authenticity. To find out how the suggested security measures affect the LoRa network, a performance investigation is carried out using a real-world test bench. In comparison to an unprotected network, the suggested secure architecture in this model significantly reduces packet transmission times.

Modern innovations in cyberspace, such as the cloud and the IoT, have changed the way people use the internet for good. The Maritime Transport System (MTS) is just one of many uses for them; they are particularly prevalent in cities that are smart and all that makes them tick. One possible solution to the increasing difficulties of modern maritime transportation is the IoT enabled MTS. In order to acquire Big Data in IoT-enabled MTS, the most important and vital exercise is to securely access data in real-time from a large number of smart IoT devices. To address this issue, K. Mahmood et al. [7] had created an authenticated key agreement system based on PUF. In order to facilitate real-time data exchange or transmission in IoT-enabled MTS, this solution allows the mobile user or IoT nodes to mutually authenticate one another via Cloud-Gateway.

In order to implement feedback control, the IoT, in smart cities gathers and sends a flood of data that is sensitive to both time and space. It connects the virtual and physical worlds, breaking down barriers between the two. When it comes to the information-based feature, the trustworthiness of the data source is crucial to the credibility and safety of the IoT. Due to their role in data collection and transmission, sensing nodes must be appropriately identified and validated. On the other hand, no prior effort has attempted to categorize or quantify the veracity of multidimensional sensing nodes in real time. Neither of the earlier trust-proof solutions was able to adequately secure the critical data. In order to tackle these issues, B. Gong et al. [8] suggested a trusted computing environment-based multi-dimensional and fine-grained dynamic measuring method. Next, the author offered a model for the classification of sensing nodes' trustworthiness, and created a mechanism to group nodes with varying degrees of trustworthiness in order to spot malevolent ones. In conclusion, the author offered a trust certification scheme for information source authentication based on threshold ring signatures. With full anonymity and traceability, it can sufficiently safeguard the attestation node's privacy information. Additionally,

the method is well-suited for sensing nodes with low computer resources due to its brief signature and great computational efficiency.

As smart communication and wireless medical sensors continue to advance, the Internet of Medical Things (IoMT) for short, is rapidly becoming an integral aspect of health surveillance from afar. In order to offer round-the-clock patient health monitoring, medical facilities utilize healthcare applications that are based on the Internet of Things. But the vast amounts of healthcare data are too much for modern smart medical equipment to manage. Concerns about safety, confidentiality, anonymity, and compatibility are just a few of the obstacles that the IoMT must overcome. Protecting the confidentiality of patients' health records during data aggregation and transmission is no easy feat. So, to get around the problems with previous studies, the author came up with a good plan. Improving aggregation efficiency while ensuring data security is the goal of this model's Efficient and Secure Transmission of Data and Aggregation (ESDTA) scheme.By utilizing the Secure Messaging Decryption (SMD) method at the Fog Node (FN) and the Secure Messaging Aggregation (SMA) method at the Mobile Node (MN), this model enables the safe conveyance of healthcare parameters and the aggregation of data from many sources. From a security standpoint, the suggested method safeguards against data manipulation and replay attacks while also maintaining data integrity.

3. PROPOSED METHOD

Smart cities are urban planning units that excel in all facets of city life, including transportation, commerce, education, administration, and social services. Their strong relationship to the many facets of information security stems from the fact that they offer a massive platform for data interchange. Proper encryption of the biometric or template data is required. Keeping it safe prevents nefarious users from tampering with the template database. The whole point of traditional authentication models will be undermined by this. Therefore, it is necessary to encrypt the template database. The situation with marketing analysis is very similar. Each smart city will have its own electronic commerce log. The purchase history will be kept in this log. Only employees of the company are authorized to access this information due to its sensitive nature. Because of this, data encryption is crucial. When it comes to the safety of his data in such a risky setting, the user has many concerns. The proposed mdoel framework is shown in Figure 2.

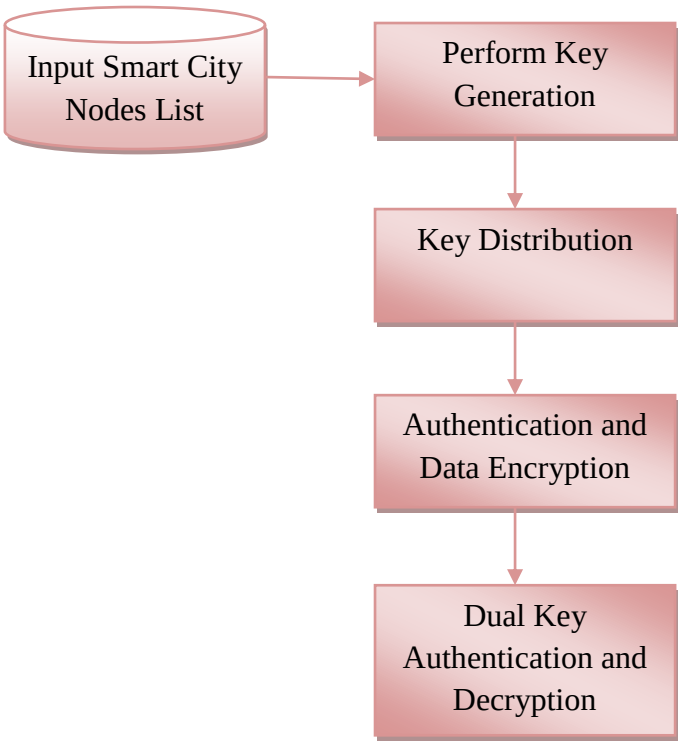

Fig 2: Proposed Model Framework

Any security breach should be communicated to the user as well. If the user is in the business world, he likely cares about the security of his data and wants to grow his company by providing his customers with affordable and adaptable services. When it comes to intelligent and effective data sharing across society's various sectors, the smart city is seen as a potentially fruitful urban environment. Using sensors or smart devices, the government, organizations, and businesses coordinate a plethora of services. These groups work together to

create a multi authority environment that generates vast amounts of data on a daily basis. Security and privacy concerns over data sharing are heightened by the massive exchange. Transforming and storing data in an encrypted form is necessary to prevent such data loss, which could lead to physical and financial issues for citizens. A number of assaults can be launched by an evil user if the data is not transmitted securely. The whole point of creating a smart city will be undermined because of this. Therefore, the safe transfer of data must be our primary concern. This research proposes a Dual Key Authentication Model with Cryptography enabled Data Transmission Model in Smart Cities. The process of dual key generation and authentication using strong cryptography model is discussed.

3.1 Key Generation and Distribution

Dual-Key Authentication model is used based on the principle of key generation and distribution for creating a reliable cryptographic method. There are two types of keys; Symmetric and Asymmetric.

Public Key (PubK): Key for encrypting and decrypting the actual data, which can exist at both the sender and receiver.

Private Key (PriK): There are two types of an asymmetric key pair, and they are a public key and a private key. The public key is used to encrypt the symmetric key and the private key is used to decrypt the public key. For generating the key pair, the following equations are mentioned below:

K_{priv} = \text{RSA.generate_private_key}(e, n)

Where e is the public exponent, typically set to 65537, and n is the key size (commonly 2048 or 3072 bits).

The public key is derived from the private key:

Kpub=Kpriv.publickey()

The symmetric key is generated using a secure random function:

Ks=os.urandom(32)

This generates a 256-bit key, commonly used with Advanced Encryption Standard (AES) for symmetric encryption.

3.2 Secure Key Exchange

To securely transmit the symmetric key to the receiving party, it is encrypted with the public key (Kpub). This ensures that only the intended recipient, who possesses the corresponding private key (Kpriv), can decrypt it:

Encrypting the Symmetric Key:

Ekey=Encrypt(Kpub,Ks)

Using a secure asymmetric encryption algorithm such as RSA, with appropriate padding (e.g., OAEP with SHA-256).

3.3 Authentication and Encryption for Data Transmission

Once the symmetric key is shared in a secure manner, it is used to encrypt the actual data for transmission. Because this type of encryption is effective with large amounts of data, it is particularly well suited to real-time communications such as those that occur among various intelligent city components

Encrypting the Data:

Es=Encrypt(Ks,M)

M is the message of the data to be encrypted. Common use symmetric encryption algorithm such as AES in GCM mode is used, with encryption and integrity check. The encrypted message Es and the symmetric key are then transmits encrypted as well.

3.4 Authentication and Decryption

When the recipient receives the original message and the encrypted symmetric key, he or she should decrypt the symmetric key and use the decrypted key to decrypt the data.

Decrypting the Symmetric Key:

Ks=Decrypt(Kpriv,Ekey)

The aim of the mentioned step is to ensure that only the recipient who has the private key will reveal the symmetric key.

Decrypting the Data:

M=Decrypt(Ks,Es)

This expression suggests that the data can be finally decrypted when the symmetric key is reached. At this moment, the original message will finally be accessible.

Algorithm DKAM-CDTM

Initialize the smart city users set as $\{SC_1, SC_2, \ldots, SC_M\}$
Perform allocation of user identity to all the users in the smart city application so that they can be identified in communication.
For each user in $\{SC_M\}$
$Uinfo \leftarrow getaddr(SC_{user})$
$attr[M] \leftarrow getVal(user)$
$UID[M] \leftarrow Uinfo(user) + attr + Th$
End for
For K in range (UID)
$Ks1 \leftarrow getPrimeval(K)$
$Ks2 \leftarrow getVal(K)$ where $Ks2 > Ks1$
$Ks3 \leftarrow rand(Ks1, Ks2)$
$PubK \leftarrow (Ks1 \oplus Ks3) \ll Ks2$
$PriK \leftarrow (Ks1||Ks2) \ll Ks3$
End for
For I in range(UID)
$Ukey \leftarrow getKey(I)$
if($Ukey == PubK$)
do
$Authentic \leftarrow 1$
Emsg←Encrypt(Data, UID)
done
Else
$Authentic \leftarrow 0$
For I in range(UID)
$Ukey \leftarrow getKey(I)$
if($Ukey == PriK$)
do
$Authentic \leftarrow 1$
Dmesg←Decrypt(Emsg)
done
Else
$Authentic \leftarrow 0$

4. RESULTS

A smart city is one that makes better use of data and technology to improve residents' quality of life, make the city more sustainable, and make city services easier to access. Various parts of a smart city can benefit from these ideas when it comes to symmetry and asymmetry. A smart city is symmetrical if its services and resources are evenly distributed throughout the entire city. All residents, regardless of where they live, would have the same opportunities to use the city's public transit, schools, and healthcare systems in an ideal symmetrical city. On the other hand, imbalances between neighborhoods and populations could arise in an asymmetrical city due to the uneven allocation of resources and services. Symmetry, in the context of city planning and architecture, can mean an optical harmony between buildings and public areas, whereas asymmetry can mean a deliberate discordance. Urban planners should think about how their design decisions will affect the health and happiness of its residents as a whole, even if symmetrical and asymmetrical layouts can both serve practical and aesthetic purposes. It is also possible to utilize technology in smart cities to rectify asymmetry and bring about symmetry. By improving traffic flow and decreasing congestion, smart transportation systems can help distribute resources more evenly across a city. On the other hand, data analysis can assist identify places where resources are not distributed equally and develop solutions to solve these discrepancies.

Cyber security is the practice of preventing unauthorized parties from gaining access to data in transit. Unauthorized data access results from inadequate security measures. The cost to an organization utilizing IoT for unauthorized access to sensitive data goes beyond just financial losses. Several methods exist for protecting information from attackers, such as robust authentication, data encryption, monitoring software, etc. When it comes to end-to-end security, data encryption is a top choice. The technical limitations of nodes in an IoT network, such as low processing power and limited memory, make the application of conventional encryption algorithms unfeasible. Hence, alternative methods of encryption, such as stream ciphers or lightweight block ciphers, work well in these kinds of settings. To meet performance objectives while also meeting varying security requirements in software and hardware systems, security techniques are essential. For sensor nodes with

limited resources, lightweight algorithms are ideal because of their speed and ease of application. This research proposes a Dual Key Authentication Model with Cryptography enabled Data Transmission Model in Smart Cities (DKAM-CDTM). The proposed model is compared with the traditional Secure and Efficient Message Authentication Protocol for IoV in Smart City Environment (IoV-SMAP) and Intelligent Security Framework Based on Collaborative Mutual Authentication Model (ISFbCMA) for Smart City Networks

Encryption and Transmission Speed: the second evaluation criterion examined the efficiency of the proposed dual-key authentication model in encrypting and transmitting data. The results reported in the next section showed that the symmetric encryption of cryptographic keys, associated with low encryption overhead levels, facilitated high-speed transmission of large datasets within Smart City networks. Additionally, latency measurements as discussed next indicated the time taken to encrypt, transmit, and decrypt the data with maximum allowable, secure interactions amongst these networked devices.

Latency Analysis: thus, low latency was associated with the nature of encryption overhead implied by the symmetric encryption approach to allow real-time communication and response in Smart City infrastructures.

Security Analysis: the final evaluation criterion analyses the security coefficients associated with the dual-key authentication model. Common cybersecurity threats, such as intercepting, accessing, or altering data, were performed in the subject test, intending to compromise the confidential, integrity, and authenticated nature of the transmitted data.

2. Scalability and Adaptability

Resource efficiency: the model's resource-efficient design enabled its scalability and flexibility to accommodate the varying network loads and data volumes typical in Smart City environments. It proved that it could handle increased data traffic without sacrificing efficiency and security.

Compatibility: compatibility testing was performed to determine how well the proposed model combined with existing Smart City infrastructures and platforms. The model combined perfectly with various IoT devices, communication networks, and data management systems, demonstrating that it can be used in different types of urban settings.

Key Generation Accuracy Levels

The graph below shows key generation accuracy levels of three models (DKAM-CDTM, IoV-SMAP and ISFbCMA) for corresponding number of users increasing from 500 to 3000. The DKAM-CDTM Model always performs the best with an accuracy beginning at 97.9% up to a value of 98.9%. The next highest accuracy levels achieved over the same range follow is that of the ISFbCMA Model with its levels peaking at 96.3%. This is the slowest increment seen by all of them but, IoV-SMAP Model holds least accuracy from amongst three with an increase starting from 94.7% and reaches to 95.7%. Better than the DKAM-CDTM Model in Key generation accuracy across different user counts. The Table 1 and Figure 3 show the key generation accuracy levels.

Table 1: Key Generation Accuracy Levels

No.of Users	Models Considered		
	DKAM-CDTM Model	IoV-SMAP Model	ISFbCMA Model
500	97.9	94.7	95.3
1000	98.1	94.9	95.5
1500	98.3	95.0	95.7
2000	98.4	95.2	95.9
2500	98.7	95.4	96.1
3000	98.9	95.7	96.3

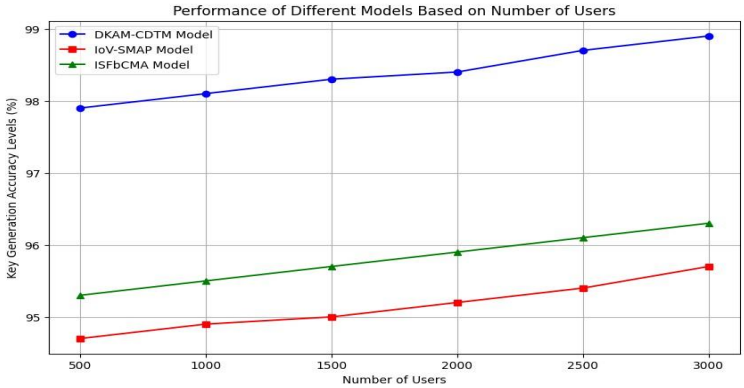

Fig 3: Key Generation Accuracy Levels

Key Distribution Time Levels

The below figure shows the time levels of key distribution for three models DKAM-CDTM, IoV-SMAP and ISFbCMA as a function on number of users from 500 to 3000. The key distribution time required by the DKAM-CDTM Model is consistently at a minimum, beginning at 11.1 units for as low as 500 users up to marginally increasing until it reaches 12.0 unit once the number of customers has reached maximum level (3000). The key distribution time of IoV-SMAP Model is slightly large starting at 15.9 units with the number of users, increasing to 17.0 units The key distribution times are the longest for ISFbCMA Model, with minimum of 21.5 units and increasing to a maximum of 22.3 units when Rs is greater than just one users. The Table 2 and Figure 4 is to show how DkAM-CDTM model is very efficient in key distribution time with others model.

Table 2: Key Distribution Time Levels

No.of Users	Models Considered		
	DKAM-CDTM Model	IoV-SMAP Model	ISFbCMA Model
500	11.1	15.9	21.5
1000	11.4	16.1	21.7
1500	11.6	16.3	21.9
2000	11.7	16.5	22.0
2500	11.9	16.8	22.1
3000	12	17	22.3

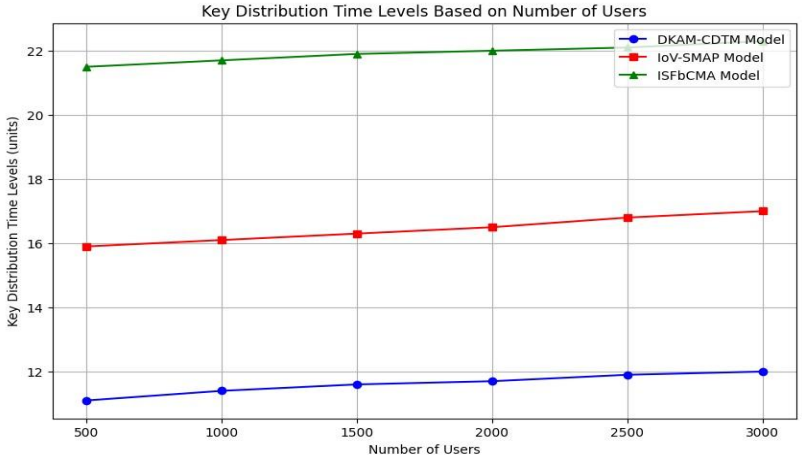

Fig 4: Key Distribution Time Levels

Authentication

The graph below represents the level accuracy of authentication for the three models, with their comparison based on the number of users, which ranged from 500–3000. The DKAM-CDTM Model exhibits the highest, starting at 97.7% for 500 users and 98.7% for 3000 users, respectively. The IoV-SMAP also demonstrates a steady progress from 95.1% for 500 users to 96.2% for 3000 users as illustrated. On the other hand, the ISFbCMA-Model was found to be lagging with the least range across all user levels, from 94.5% to 95.5%. The figure graph, therefore, compares the three models on the authentication level with different levels, as represented by the number of users. In all the models, DKAM-CDTM was the model with a comparably higher level of authentication. The Authentication Accuracy Levels is represented in Table 3 and Figure 5.

Table 3: Authentication Accuracy Levels

No.of Users	Models Considered		
	DKAM-CDTM Model	IoV-SMAP Model	ISFbCMA Model
500	97.7	95.1	94.5
1000	97.9	95.3	94.7
1500	98.1	95.7	94.9
2000	98.3	95.9	95.1
2500	98.5	96.0	95.3
3000	98.7	96.2	95.5

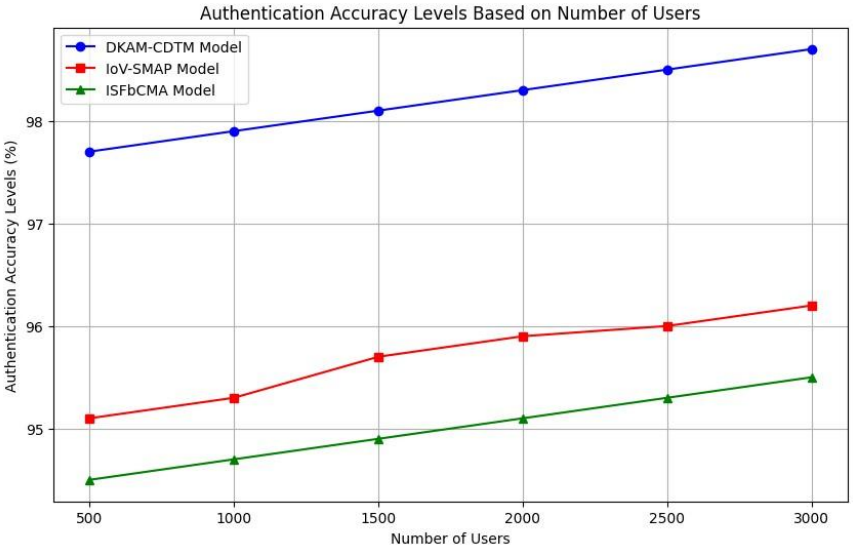

Fig 5: Authentication Accuracy Levels

Encryption Time Levels

The graph below shows the encryption time levels for three models (DKAM-CDTM, IoV-SMAP and ISFbCMA) under number of users 500 to 3000. The DKAM-CDTM Model has the lowest encryption time at almost all performance points beginning with 7.1 units for 500 users and increasing to about 8.0 units of time through (3000) users. On all communication models, the IoV-SMAP Model also requires more encryption times (17.0 units to 18.0 units for encryption time with respect to number of users in from 500 usersto3Kusers). The ISFbCMA Model calculation time, demonstrates the longest encryption exposure starting at 19.5 units and increasing to 20.4 as u rises The efficiency in encryption time of the DKAM-CDTM Model is further emphasized by this visualization than other models. The Table 4 and Figure 6 shows the Encryption Time Levels.

Table 4: Encryption Time Levels

No.of Users	Models Considered		
	DKAM-CDTM Model	IoV-SMAP Model	ISFbCMA Model
500	7.1	17.0	19.5
1000	7.2	17.2	19.7
1500	7.4	17.4	19.8
2000	7.6	17.6	20.1
2500	7.9	17.9	20.2
3000	8	18	20.4

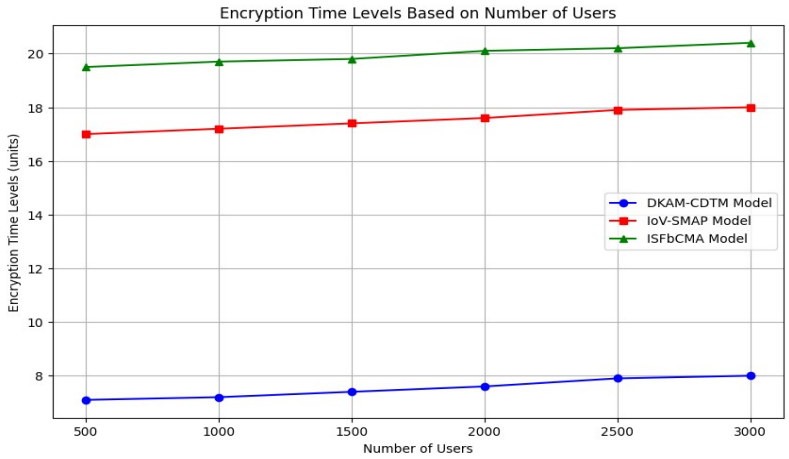

Fig 6: Encryption Time Levels

Dual Key Authentication Accuracy Levels

The graph below indicates the accuracy rate against number of users for three models (DKAM-CDTM, IoV-SMAP and ISFbCMA) based on dual key authentication approach. The highest accuracy was achieved by the DKAM-CDTM Model which started from 97.8% for 500 users upto to reach consecutively an accuracy of up to as high as like a total user count reaching into massive numbers of over more than at 3000. The accuracy with the IoV-SMAP Model becomes lower compared to DKAM-CDTM, and it is 93.5-94.5% for simulations of different numbers up to 3000 users Conversely, the ISFbCMA Model has FNs in between with 94.9% accuracy when serving one user and remaining stable at 95.7% acc as more users are supported by the number of users. This visualization primarily highlight the superior dual key authentication accuracy performance of DKAM-CDTM Model over different user counts. The Table 5 and Figure 7 represent the Dual Key Authentication Accuracy Levels.

Table 5: Dual Key Authentication Accuracy Levels

No.of Users	Models Considered		
	DKAM-CDTM Model	IoV-SMAP Model	ISFbCMA Model
500	97.8	93.5	94.9
1000	98.1	93.7	95.0
1500	98.2	93.9	95.1
2000	98.4	94.1	95.3
2500	98.6	94.3	95.5
3000	98.8	94.5	95.7

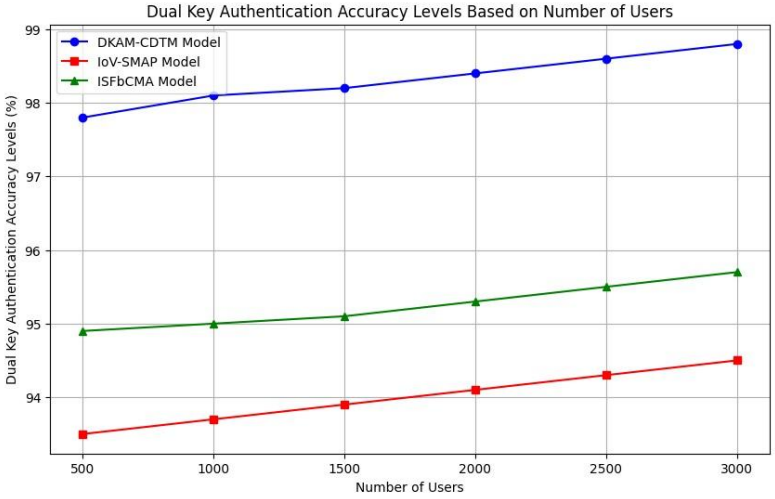

Fig 7: Dual Key Authentication Accuracy Levels

Data Security Levels

The below graph shows data security with respect to the number of users from 500 unites to 3000 units for the three models. With the increase in the number of users in all the domains, the DKAM-CDTM exceeds the other models. DKAM-CDTM has the same data security percentages, with 98.5 % and 99.4%, whereas, for IOV-SMAP and ISFbCMA, data security achieved includes 94.3% and 95.2% up to 3000 users and 95.2% and 96.3% for IOV-SMAP and ISFbCMA, respectively. Therefore, as portrayed in the visual, DKAM-CDTM ensures high data security when the number of users also increase. The Table 6 and Figure 8 depicts the Data Security Levels.

Table 6: Data Security Levels

No.of Users	Models Considered		
	DKAM-CDTM Model	IoV-SMAP Model	ISFbCMA Model
500	98.5	94.3	95.2
1000	98.7	94.5	95.4
1500	98.9	94.6	95.7
2000	99.1	94.8	95.9
2500	99.2	95.0	96.1
3000	99.4	95.2	96.3

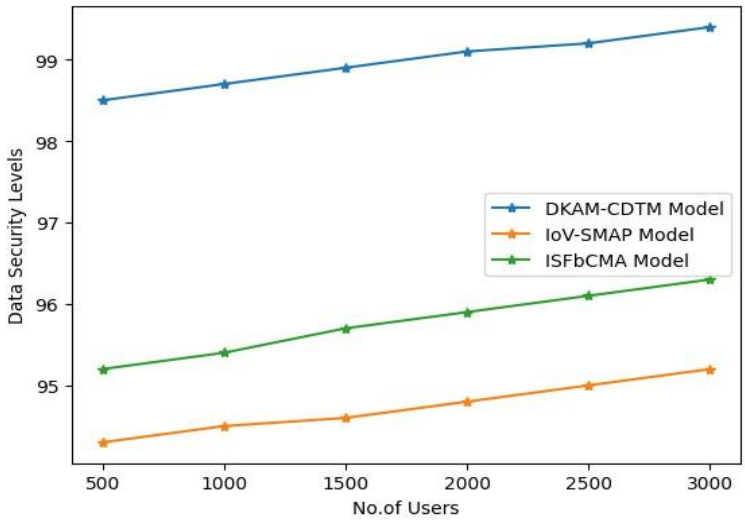

Fig 8: Data Security Levels

5. CONCLUSION

Among the most fundamental features of the contemporary world are smart cities. Enhancing people's and services' quality of life is smart cities' principal objective. Smart city infrastructure is mostly composed of information and communication technologies and IoT devices. There are a lot of people worried about their privacy in smart city communications due to ICTs and IoT devices. Many fascinating applications in sustainable digital cities and societies rely on the IoT. These include smart industry, smart transportation, and additive factories. On the other hand, data transmission security measures might not work in a smart city setting. Transferring raw data from one device to another opens the door to the possibility of data manipulation, and this risk is amplified when sending data that has not been processed. The raw data must be compressed and encrypted before transmission across the network to prevent data manipulation and cyber attacks. This research proposes a Dual Key Authentication Model with Cryptography enabled Data Transmission Model in Smart Cities (DKAM-CDTM) that is an effective and feasible solution to the Smart Cities' existing security challenges. The model ensures data security and eliminates considerable latency and resource overhead to realize real-time Smart City applications. This model is effective for securing secured data for any Smart City context. The model is equally suitable for a Big City as well as a remote environment since it offers secured and managed the risk of data that include Smart City. Additionally, the model is scalable to any Smart City projects, and the proposed model is promising for several applications. Data protection a vital role in making the Digital Age the era of Smart, Safe, and Resilient Recovery. The proposed model achieved 98.8% accuracy in Dual Key Authentication, 98.9% accuracy in Key Generation and 99.4% accuracy in providing Data Security. In future, multiple parameters can be considered in key generation and transmission and also complex instructions can be implemented for authentication and access control in smart cities.

REFERENCES

1. S. Yu, J. Lee, K. Park, A. K. Das and Y. Park, "IoV-SMAP: Secure and Efficient Message Authentication Protocol for IoV in Smart City Environment," in IEEE Access, vol. 8, pp. 167875-167886, 2020, doi: 10.1109/ACCESS.2020.3022778.
2. O. Khadidos, S. Shitharth, H. Manoharan, A. Yafoz, A. O. Khadidos and K. H. Alyoubi, "An Intelligent Security Framework Based on Collaborative Mutual Authentication Model for Smart City Networks," in IEEE Access, vol. 10, pp. 85289-85304, 2022, doi: 10.1109/ACCESS.2022.3197672.
3. H. Zhang, M. Babar, M. U. Tariq, M. A. Jan, V. G. Menon and X. Li, "SafeCity: Toward Safe and Secured Data Management Design for IoT-Enabled Smart City Planning," in IEEE Access, vol. 8, pp. 145256-145267, 2020, doi: 10.1109/ACCESS.2020.3014622.
4. R. R. Irshad et al., "An Intelligent Buffalo-Based Secure Edge-Enabled Computing Platform for Heterogeneous IoT Network in Smart Cities," in IEEE Access, vol. 11, pp. 69282-69294, 2023, doi: 10.1109/ACCESS.2023.3288815.
5. W. Othman, M. Fuyou, K. Xue and A. Hawbani, "Physically Secure Lightweight and Privacy-Preserving Message Authentication Protocol for VANET in Smart City," in IEEE Transactions on Vehicular Technology, vol. 70, no. 12, pp. 12902-12917, Dec. 2021, doi: 10.1109/TVT.2021.3121449.
6. L. Kane, V. Liu, M. McKague and G. R. Walker, "Network Architecture and Authentication Scheme for LoRa 2.4 GHz Smart Homes," in IEEE Access, vol. 10, pp. 93212-93230, 2022, doi: 10.1109/ACCESS.2022.3203387.

7. K. Mahmood, J. Ferzund, M. A. Saleem, S. Shamshad, A. K. Das and Y. Park, "A Provably Secure Mobile User Authentication Scheme for Big Data Collection in IoT-Enabled Maritime Intelligent Transportation System," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 2, pp. 2411-2421, Feb. 2023, doi: 10.1109/TITS.2022.3177692.
8. B. Gong, J. Liu and S. Guo, "A Trusted Attestation Scheme for Data Source of Internet of Things in Smart City Based on Dynamic Trust Classification," in IEEE Internet of Things Journal, vol. 8, no. 21, pp. 16121-16141, 1 Nov.1, 2021, doi: 10.1109/JIOT.2020.3006349.
9. M. Azeem et al., "FoG-Oriented Secure and Lightweight Data Aggregation in IoMT," in IEEE Access, vol. 9, pp. 111072-111082, 2021, doi: 10.1109/ACCESS.2021.3101668.
10. S. U. Jan, I. A. Abbasi, F. Algarni and A. S. Khan, "A Verifiably Secure ECC Based Authentication Scheme for Securing IoD Using FANET," in IEEE Access, vol. 10, pp. 95321-95343, 2022, doi: 10.1109/ACCESS.2022.3204271.
11. F. Wu, X. Li, L. Xu, P. Vijayakumar and N. Kumar, "A Novel Three-Factor Authentication Protocol for Wireless Sensor Networks With IoT Notion," in IEEE Systems Journal, vol. 15, no. 1, pp. 1120-1129, March 2021, doi: 10.1109/JSYST.2020.2981049.
12. M. T. Ahvanooey et al., "Modern Authentication Schemes in Smartphones and IoT Devices: An Empirical Survey," in IEEE Internet of Things Journal, vol. 9, no. 10, pp. 7639-7663, 15 May15, 2022, doi: 10.1109/JIOT.2021.3138073.
13. H. Tahir, K. Mahmood, M. F. Ayub, M. A. Saleem, J. Ferzund and N. Kumar, "Lightweight and Secure Multi-Factor Authentication Scheme in VANETs," in IEEE Transactions on Vehicular Technology, vol. 72, no. 11, pp. 14978-14986, Nov. 2023, doi: 10.1109/TVT.2023.3286187.
14. W. Yang, S. Wang, X. Yin, X. Wang and J. Hu, "A Review on Security Issues and Solutions of the Internet of Drones," in IEEE Open Journal of the Computer Society, vol. 3, pp. 96-110, 2022, doi: 10.1109/OJCS.2022.3183003.
15. J. Cao, S. Li, R. Ma, Y. Han, Y. Zhang and H. Li, "RPRIA: Reputation and PUF-Based Remote Identity Attestation Protocol for Massive IoT Devices," in IEEE Internet of Things Journal, vol. 9, no. 19, pp. 19174-19187, 1 Oct.1, 2022, doi: 10.1109/JIOT.2022.3164174.
16. X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar and N. Kumar, "A Lightweight Privacy-Preserving Authentication Protocol for VANETs," in IEEE Systems Journal, vol. 14, no. 3, pp. 3547-3557, Sept. 2020, doi: 10.1109/JSYST.2020.2991168.
17. M. Umar, S. H. Islam, K. Mahmood, S. Ahmed, Z. Ghaffar and M. A. Saleem, "Provable Secure Identity-Based Anonymous and Privacy-Preserving Inter-Vehicular Authentication Protocol for VANETS Using PUF," in IEEE Transactions on Vehicular Technology, vol. 70, no. 11, pp. 12158-12167, Nov. 2021, doi: 10.1109/TVT.2021.3118892.
18. J. Li et al., "A Secured Framework for SDN-Based Edge Computing in IoT-Enabled Healthcare System," in IEEE Access, vol. 8, pp. 135479-135490, 2020, doi: 10.1109/ACCESS.2020.3011503.
19. S. H. Alsamhi et al., "Drones' Edge Intelligence Over Smart Environments in B5G: Blockchain and Federated Learning Synergy," in IEEE Transactions on Green Communications and Networking, vol. 6, no. 1, pp. 295-312, March 2022, doi: 10.1109/TGCN.2021.3132561.
20. R. Goyat, G. Kumar, M. Conti, T. Devgun, R. Saha and R. Thomas, "BENIGREEN: Blockchain-Based Energy-Efficient Privacy-Preserving Scheme for Green IoT," in IEEE Internet of Things Journal, vol. 10, no. 18, pp. 16480-16493, 15 Sept.15, 2023, doi: 10.1109/JIOT.2023.3268325.
21. M. A. Saleem, X. Li, M. F. Ayub, S. Shamshad, F. Wu and H. Abbas, "An Efficient and Physically Secure Privacy-Preserving Key-Agreement Protocol for Vehicular Ad-Hoc Network," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 9, pp. 9940-9951, Sept. 2023, doi: 10.1109/TITS.2023.3266030.
22. C. Kong, K. Zheng, S. Wang, A. Rocha and H. Li, "Beyond the Pixel World: A Novel Acoustic-Based Face Anti-Spoofing System for Smartphones," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 3238-3253, 2022, doi: 10.1109/TIFS.2022.3202115.
23. A. Alharthi, Q. Ni and R. Jiang, "A Privacy-Preservation Framework Based on Biometrics Blockchain (BBC) to Prevent Attacks in VANET," in IEEE Access, vol. 9, pp. 87299-87309, 2021, doi: 10.1109/ACCESS.2021.3086225.
24. A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang and K. -K. R. Choo, "An Energy-Efficient SDN Controller Architecture for IoT Networks With Blockchain-Based Security," in IEEE Transactions on Services Computing, vol. 13, no. 4, pp. 625-638, 1 July-Aug. 2020, doi: 10.1109/TSC.2020.2966970.
25. H. Chourabi et al., "Understanding Smart Cities: An Integrative Framework," 2012 45th Hawaii International Conference on System Sciences, Maui, HI, USA, 2012, pp. 2289-2297, doi: 10.1109/HICSS.2012.615.