Mesopotamian journal of Cybersecurity
Vol.5,No.1, **pp**. 256–272
DOI: https://doi.org/10.58496/MJCS/2025/017; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Enhancing Traffic Data Security in Smart Cities Using Optimized Quantum-Based Digital Signatures and Privacy-Preserving Techniques

Tuqa Ghani Tregi[1], Mishall Al-Zubaidie[1,*]

[1] *Department of Computer Sciences, Education College for Pure Sciences University of Thi-Qar, Nasiriyah 64001, Iraq.*

ARTICLEINFO

Article history
Received 06 Jan 2025
Accepted 10 Mar 2025
Published 06 Apr 2025

Keywords
BB84
FTA
Masking
Pseudonym
Post Quantum Signatures
Sybil

ABSTRACT

Securing big data in power plants is an important and fundamental step in the infrastructure of smart cities. In addition, it becomes a barrier if it is not controlled from the beginning. Security must be a combination of fast and robust properties. This research presents a traffic security system (TSS) in a smart city (SC). It is a novel paradigm meant to improve data security and integrity by means of a multilayered method. Advanced fault analysis, dual-stage pseudonymizing, quantum key distribution via the BB84 protocol, and Falcon signatures (FS) are combined in the proposed system. TSS enhances data security by enhancing privacy, supporting resilience against quantum computing threats, and not burdening the network with complex and large keys. The proposed system has been tested against several recently known attacks, such as replay, supply chain, Sybil, blackhole, eavesdropping, advanced persistent threat (APT), tampering, ransomware identity fraud, and desynchronization, and it has been proven to overcome them. In terms of performance evaluation, the average signing time was approximately 0.002 milliseconds. In comparison, the average signature verification time was approximately 0.004 milliseconds, with an average execution time of approximately 0.54 milliseconds and a precision of approximately 93.6 %, a recall of approximately 97.8 %, and an F1_score of approximately 95.6 %, which are considered low compared with those of state-of-the-art research. Thus, the proposed TSS system is highly acceptable for power plant applications. This work lays the groundwork for future developments in safe, privacy-conscious urban systems by presenting a multilayered approach to secure energy data in smart cities.

1. INTRODUCTION

As smart cities grow rapidly, transportation systems depend more on big data as well. Often sensitive, these data include traffic pattern information and are thus prone to hackers. Thus, strong security solutions are desperately needed to guarantee information security and safeguard the gathered data from smart traffic systems [1]. Likewise, they address increasing security issues, as service centers depend more on AI technologies connected to the Internet of Things for Smart Cities (IoSCT) and the digital infrastructure. These difficulties include data privacy violations, cyberattacks aimed against vital infrastructure, and the emergence of quantum computers, thereby endangering smart cities [2].

Despite significant progress in smart city technologies, significant security gaps remain when massive amounts of data collected from traffic systems are protected [3]. Many current systems rely on classical encryption, in which quantum attacks could render useless in the future, leaving traffic data vulnerable to hacking. Furthermore, most current solutions lack robust privacy mechanisms, as individuals can still be identified through data analysis, even when outdated masking techniques are used [1]. To overcome these problems, an integrated security system capable of securing data exchange between system components in a way that is resistant to quantum attacks and analysing data quality before exploitation is needed [4]. This ensures the effectiveness of smart traffic systems while protecting us at the same time. Therefore, the data collected by sensors, including traffic, must be kept safe from cyber attacks. While smart applications such as smart transportation require strong security measures to protect user data and ensure service integrity, data analytics is an essential component of data management systems that aim to improve service delivery [5]. The big data transmitted over wireless networks need to be protected, as they can be used illegally. One must protect the data from leaks. Critical security solutions work mostly through

*Corresponding author. Email: mishall_zubaidie@utq.edu.iq

digital data signatures, where the data and services provided to citizens are protected from hacking. Among the many security concerns faced by smart cities are privacy breaches, cyberattacks, hardware vulnerabilities, data manipulation, and system failure [5, 6]. The purpose of this study is to design a security system to protect traffic data in smart cities by integrating modern encryption techniques and quantum computing resistance, making our security system future-proof for citizens' data.

Data collected by (IoSCT) devices that are vulnerable to leakage or illegal use also have several drawbacks. Sometimes, open communication channels help hackers intercept or alter data. Many vulnerabilities in smart devices can put human safety at risk. Data manipulation can lead to false conclusions or incorrect assessments. Perceived system disruptions can render vital services useless; technology cannot prevent impending disasters because it relies mostly on the accuracy of data obtained from outside [7][47]. Figure 1 shows security challenges in smart cities.

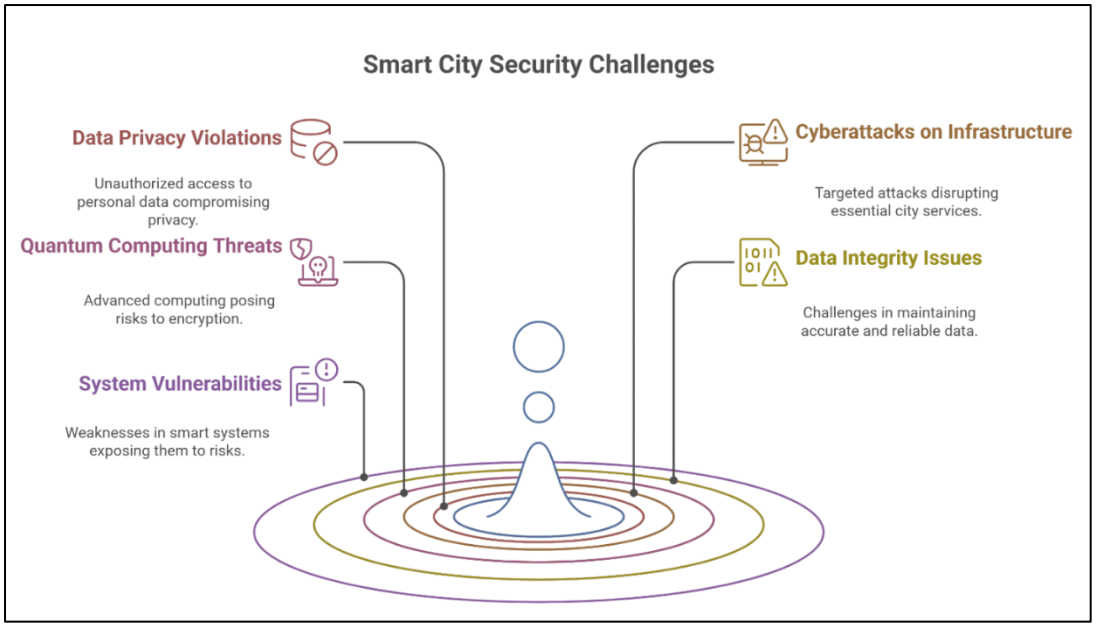

Fig. 1. Smart city security challenges.

Digital technology is increasingly reliant and has both positive and negative consequences in many areas of life. However, new technologies also present legal dilemmas related to security rights issues. Despite these challenges, the clear benefits of digital technology require a delicate balance between exploiting its advantages and addressing the corresponding problems [6]. Data manipulation and information security flaws in how data are collected, transmitted, and stored create significant security risks for smart cities that can lead to data breaches and losses resulting from inadequate protection measures and the absence of unified systems to stop exploitation [7]. They are of great social and financial importance. Strong data protection encourages vulnerable areas, and therefore, data protection is vital to any effective cybersecurity strategy; breaches generate mistrust between residents and authorities, thus hampering the activities of smart cities.

As quantum computers can solve difficult problems faster than classical computers do, significantly impacting traditional cryptographic methods, they represent a technological revolution. The rapid compromise of existing cryptography, which compromises the security of traditional systems, can come from quantum computing devices [8]. In both wired and wireless networks, security is now at the forefront. Network features present opportunities and challenges for achieving security goals, including confidentiality, authentication, integrity, availability, access control, and nonrepudiation [9]. Through innovative cryptographic techniques such as BB84, which ensures secure communications via quantum physics concepts, quantum computing has the potential to improve security. These solutions can improve the security of critical data transmitted between devices and infrastructure in smart cities, thereby reducing the risk of cyberattacks and increasing customer confidence in these innovative systems. The increasing adoption of technology and the proliferation of smart grids, including IoSCT, underscore the importance of establishing effective security protocols to address growing concerns and ensure the preservation of critical data. On the basis of the development of technology, security solutions must be adaptable. Define precise guidelines and practices for smart grid security [10][48]. Most existing studies rely on traditional or incomplete security solutions, making them incapable of countering future quantum attacks. Furthermore, many studies do not address the importance of preliminary data analysis before processing it for security purposes. In this paper, we present a new methodology that addresses these gaps by combining error analysis, quantum-resistant signatures, and quantum key generation. In this work, we aim to shed light on the TSS system methodology and its mechanism of action in protecting and

analysing data, with a focus on the balance between ensuring privacy and maintaining the usability of data in highly sensitive environments such as smart cities. It mostly helps by:

- This work uses fault tree analysis (FTA) to methodically identify faults in traffic systems throughout the data collection process, thereby guaranteeing better data accuracy prior to implementing additional security.
- The proposed system employs the BB84 quantum key distribution protocol to generate keys among infrastructures. This mechanism enables secure data signing via the FALCON signature while mitigating and preventing potential network breaches where attackers might attempt to manipulate data.
- To protect sensitive information, advanced masking techniques are applied to prevent data leakage. This ensures that data, even if intercepted, remain untraceable to real users.

We provide an overview of the research organization here. A comprehensive introduction is provided in Section 1. We review recent studies on related work in Section 2. The history of quantum signatures and pseudonyms is described in Section 3. A research technique for electrical station data protection is presented in Section 4. Section 5's proposed TSS was examined via a security analysis. In Section 6, the TSS performance analysis is described in detail. Section 7 presents the findings of the investigation.

2. LITERATURE REVIEW

This subsection discusses the literature survey related to the proposed work.

The Internet of Smart City Things (IoSCT) has been the subject of several research papers that have examined literature surveys. These surveys have identified a variety of security and privacy concerns, such as authentication, integrity, centralization, latency, and others, and have also considered potential solutions for SC applications. For example, Chen et al. [11] presented SC blockchain-based proven data possession (PDP) for decentralized, secure data storage. This study does not address data and device authentication issues. Ismagilova et al. [12] focused on several studies on risks within smart cities, highlighting threats related to information security and challenges facing smart city infrastructure in managing and processing personal data. Their study analysed many of these challenges, provided a review of several key issues, and provided a direction for future studies. This research, on the other hand, did not give any specific answers to the problems that were highlighted, nor did it have any practical applications. Ahmad et al. [13] analysed and examined data and algorithmic challenges such as security, robustness, and interpretability to effectively use artificial intelligence (AI) in human-centric applications inside smart cities, offering solutions. Nonetheless, these technologies are adequate for ensuring security in human-centric systems. Al-Turjman et al. [14] highlighted SC applications, including smart grids, smart transportation, smart energy, and smart health, while addressing security and privacy concerns and evaluating current solutions.

Gharehchopogh et al. [15] developed quantum-inspired macroscopic algorithms by incorporating quantum computing (QC) concepts into macroscopic algorithms. Macroscopic algorithms are a research area that incorporates elements of mathematics, physics, and computing. This feature helps in finding solutions to the problems of improving security in smart cities. In this work, quantum-inspired metaheuristic algorithms were used in the optimization areas. However, they did not use digital signatures that guarantee data integrity. Nomaan et al. [16] used quantum key distribution (QKD) to exchange secure keys between communicating parties. The key obtained through QKD is then used to encrypt data via a convolutional neural network. However, the need to integrate quantum systems with neural networks increases the complexity of implementing the system on a large scale in infrastructure. Gabriel Rossi et al. [17] devised a LoRaWAN protocol that facilitates data transmission from IoT endpoints to application servers for analysis and storage. LoRaWAN security is dependent on the AES-128 encryption technique, which is vulnerable to quantum computing threats. Consequently, they suggested an enhancement to the LoRaWAN security protocol by using the Kyber KEM-1024 algorithm to fortify the system against quantum computing threats. Nevertheless, it was often intricate and required more infrastructure expenditures. Das et al. [18] subsequently deliberated on prospective research problems in SC applications to enhance performance in terms of security and privacy. However, these open research challenges are inadequate for ensuring a secure environment in an SC. For the current solutions for safe SCs, there are many challenges in the SC, such as large amounts of data, high-definition communication, privacy, latency, and security. However, security and privacy have become the most important concerns for SC applications today. Peivandizadeh et al. [19] proposed a security protocol that focuses on enhancing the security properties and protecting IoT nodes. By leveraging the security features provided by elliptic curve cryptography (ECC) and using the elliptic curve difference–Hellman (ECDH) key exchange mechanism, the complexity of the protocol prevents its widespread implementation.

TABLE I. PREVIOUS STUDIES ON SECURING SMART CITIES

Researchers	Techniques and Algorithms Used	Study Proposal	Unsolved Problems
Chen et al. [11] 2020	Blockchain for secure data storage	Blockchain-based dynamic provable data possession	High cost and complexity of blockchain implementation
Ismagilova et al. [12] 2022	Literature review, smart city interaction framework	Security, privacy, and risk analysis in smart cities	No specific technical solutions provided
Ahmad et al. [13] 2022	Critical analysis of smart city security and data management	Human-centered smart city development with ethical considerations	Lack of technical solution proposals
Al-Turjman et al. [14] 2022	IoT security and privacy review	Challenges and opportunities in smart city IoT security	No direct technical solutions proposed
Gharehchopogh et al. [15] 2023	Quantum-inspired metaheuristic algorithms	Comprehensive classification of quantum algorithms	No practical comparison of algorithms
Nomaan et al [16] 2023	Quantum cryptography in CNN for smart cities	Combining AI and quantum encryption for security	Limited real-world applications
Gabriel et al. [17] 2024	Post quantum key encapsulation for LoRaWAN	Enhancing security of LoRaWAN networks	Implementation complexity and hardware requirements
Das et al. [18] 2025	Secure and privacy-aware data sharing for smart electric vehicles	Secure method for vehicle-to-vehicle data exchange	Needs real-world testing and validation
Peivandizadeh et al. [19] 2024	Secure key exchange and authentication protocol	Secure IoT communication authentication mechanism	Potential performance issues on low-power devices

3. BACKGROUND

This section has subsections that elucidate FTA and pseudonymization procedures, with specifics on quantum key distribution using the BB84 protocol and the FS quantum-resistant signature method.

3.1 Fault Tree Analysis

Fault tree analysis (FTA) is a systematic analysis technique that determines whether a system is reliable enough in the event of hardware failure. The goal of FTA is to analyse the possible causes of undesirable events, such as system-level failures, by identifying component-level faults. System analysis requires translation into an FT. It is a graphical model that is used to evaluate system reliability [20].

FTA techniques can be divided into qualitative and quantitative methods. The method qualitatively identifies the possible causes of system-level failures, such as the failure of multiple system components, on the basis of the structure of the FT. Quantitative FTA calculates values such as failure probabilities for an FT. It evaluates the probability of the highest event on the basis of the failure probabilities at the component level [21]. FT is a tree-like model consisting of nodes and edges. Nodes can be system components, conditions, gates, or the highest event. The system components form the system and are the leaves of the FT. An event is the failure of a subsystem or an individual component. An event is called "intermediate" when it is triggered by one or many other events or is otherwise called "primary". The top event is the root of the tree and is an undesirable event. For example, if the power supply to the system fails, it may cause the system to shut down, which may have disastrous consequences. Avoiding these undesirable events is the purpose of the analysis [22]. Algorithm 1 describes fault tree analysis ٥t starts by identifying the final event T (logic tree) where the relationships between events are added via logic gates G. The tree is traced to identify the root causes R by expanding the tree until it reaches the system components C. A quantum analysis can be performed to calculate the probability T on the basis of the probabilities of the sub events before the results are output.

ALGORITHM 1: FTA

***Input**:*
T: Top Event (final failure to analyse)
C: Components of the system
G: Logical gates

***Output**:*
R: Root causes of the failure
P(T): Probability of T

1. *Begin*
2. *Tree ← {T}*
3. *For each T, identify contributing events: Tree ← Tree ∪ G (Contributing Events)*
4. *Traverse Tree to Root Causes:*
5. *While Events ≠ ∅ If Event is a component (C) then R ← R ∪ {Event} Else Expand using G.*
6. *Compute Probabilities: For each event E connected by G: P(E) = f(P(Sub-Events))*
7. *Return R, P(T)*
8. *End*

3.2 Pseudonymization

Data anonymization is the process of replacing all personal identifiers (such as names, addresses, and account numbers) with pseudonyms: artificially generated words or codes that may serve as convincing representations of the original data. "Strong" anonymization focuses on "pseudo-identifier" attributes (device ID), and the codes are assigned randomly and independently of the original values (although they may still eventually be associated with each other). Data anonymization is an approach that provides a traceable form of anonymity and requires legal, regulatory, or technical procedures. Consequently, the association can be made only under specific, controlled conditions. Notably, data anonymization is not, as a general rule, sufficient to ensure that the final results of the process do not constitute personal data [23].

Pseudonymization is a data protection methodology that aims to replace sensitive personal identifiers with pseudonyms or masked data. Common techniques include partial masking, where specific parts of the data are masked, and full masking, where the entire data field is replaced with nonidentifiable values. Dynamic masking is an innovative approach that allows for control of the level of visibility on the basis of user privileges, where authorized users can access the full data while limiting exposure to others. These techniques are essential in sensitive sectors such as healthcare and finance, where a delicate balance must be struck between protecting confidentiality and ensuring the effective usability of data, which in turn enhances the security and operational efficiency of systems [24].

3.3 BB84 Protocol

Aiming to provide a shared secret key for encrypting safe communications, BB84 is a quantum mechanical technique utilized for the process of secret key exchange between a sender and a receiver. The process consists of fundamental preparation, transmission, measurement, comparison, and eavesdropping identification. The uncertainty principle holds that some features of a quantum particle cannot be exactly seen simultaneously; the noncloning theorem claims that an unknown quantum state cannot be replicated. A basic component of postquantum cryptography research [25] is that it is necessary for attaining absolute security in communications. Development was highlighted with the first whole procedure (Bennett and Brassard, 1984), which was built on past concepts by Wiesner (Wiesner, 1983). Alice sends bits in the BB84 protocol to Bob from two complement bases of a two-level system [26]. Stated specifically as a security rationale, the noncloning thesis. The sender creates a random key in it and then codes it into qubits, which are delivered to the recipient via a quantum channel. Bob measures the qubits and creates a shared secret key following the result analysis. If a spy agent tries to intercept the qubits, it may use sorting to identify and destroy the compromised qubits, thereby maintaining the integrity of the key. By the use of mistake correction and privacy-enhancing techniques, the sender and receiver may improve the key generation, thereby retaining its security and secrecy [27]. Introduced in 1984 by Charles Bennett and Alain Brassard, BB84 and E91 are QKD systems that exploit four different polarization states of photons.

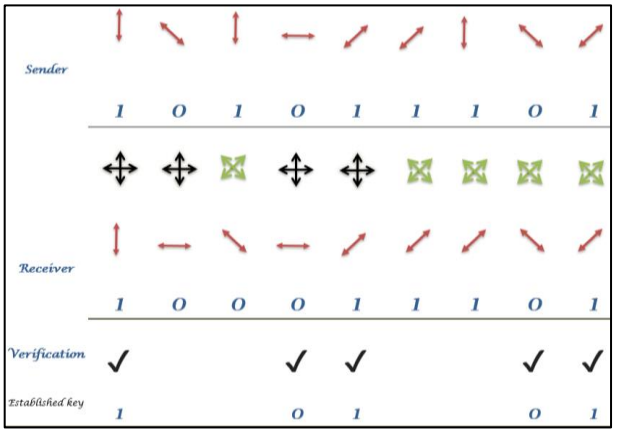

Fig. 2. Sample for Generating a Secure Key via the BB84 Protocol.

ALGORITHM 2: BB84 protocol

***Input**: Seed*
***Output**: Secret Key*

1. *Begin*
2. *$B\_Sender \leftarrow \{B_i \mid B_i \in \{0, 1\}\}$, $\theta\_Sender \leftarrow \{\theta_i \mid \theta_i \in \{R, D\}\}$*
3. *$P\_Encoded \leftarrow \{P_i \mid P_i = F(B_i, \theta_i)\}$*
4. *Receiver Generates Bases and Measures: $\theta\_Receiver \leftarrow \{\theta'_i \mid \theta'_i \in \{R, D\}\}$, $B\_Measured \leftarrow \{M_i \mid M_i = G(P_i, \theta'_i)\}$*
5. *Filter Matching Bases: $\theta\_Shared \leftarrow \{i \mid \theta_i = \theta'_i\}$, $B\_Filtered \leftarrow \{B_i \mid i \in \theta\_Shared\}$*
6. *Verify Errors: E_Error ← (Mismatched Bits)/(Total Bits In B_Filtered)*
7. *Abort If E_Error > E_Threshold.*
8. *Amplify Privacy: Secret Key ← H(B_Filtered)*
9. *End*

Algorithm 2 illustrates the quantum key generated by BB84. First, the sender generates random bits and bases B_Sender, where θ_Sender is a series of random binary values (0,1). Each bit (B_i) is encoded into a photon polarization state (P_i) on the basis of the basis (θ_i). If B_i = 0, then θ_i =$R\rightarrow$ Horizontal polarization; if B_i =1, then θ_i =$D\rightarrow$ 45° polarization. The receiver then generates random bases (θ _Receiver). Each photon is measured via a random base. If the base (θ_i) matches the base used in the measurement (θ'_i), then the measured bits (M_i) match the original bits (B_i). Then, the bases of the transmitter and receiver are compared: θ_Shared ← $\{i \mid \theta_i = \theta'_i\}$. The photons measured via identical bases are kept B_Filtered ← $\{B_i \mid i \in \theta$ _Shared$\}$. When the error rate is calculated if E_Error > E_Threshold, the protocol is stopped. The privacy amplification technique is applied to the raw key to reduce the eavesdropper's potential knowledge of the Secret Key ← H(B_Filtered). Figure 2 depicts the BB84 key generation.

3.4 FALCON Post-Quantum Digital Signature Scheme

Denoted by its full name, "Fast-Fourier lattice-based compact signatures over NTRU," this signature method is based on lattice cryptography and is specially tuned for effective and compact execution over NTRU [28]. The architectural simplicity of FS results from its adherence to the theoretical paradigm set out in a 2008 paper [29] by Gentry, Peikert, and Vaikuntanathan for constructing lattice-based hash-and-sign algorithms. Two basic components are required by this theoretical model: trapdoor sampling, with an FS signature via a novel approach called fast Fourier sampling, and a defined family of cryptographic lattices from which NTRU lattices are chosen. All things considered, FS's signature scheme may be concisely described as the integration of rapid Fourier sampling, NTRU lattices, and the GPV framework. Employing the hash-and-sign technique, the FS signature is a post-quantum lattice-based signature system. Three main processes define the FS signature method: key generation, signing, and signature verification. To generate its coefficients, FS needs sampling both during key generation and signing [30].

ALGORITHM 3: FALCON Key Generation

Input:
P: Monic polynomial in Q[a]
q: Modulus (integer)

Output:
SK: Secret key
PK: Public key
Steps:

1. *Generate random polynomials f, g.*
2. *Solve NTRU equation for F, G.*
3. *Construct lattice matrix A.*
4. *Apply FFT to A → A_trans.*
5. *Compute Gram matrix G_matrix.*
6. *Perform LDL decomposition on G_matrix → T.*
7. *Normalize leaves in T.*
8. *Set secret key SK = (A_trans, T).*
9. *Compute public key PK = g * f^{-1} mod q.*
10. *Return SK, PK.*

Algorithm 3 generates a key pair via a polynomial *P* and a coefficient *q*, thereby generating random polynomial equations *f* and *g* [31]. The NTRU equation is subsequently solved to obtain *F* and *G*. After a fast Fourier transform (*FFT*), a lattice matrix *A* is produced; thereafter, the Gram matrix is constructed, and *LDL* analysis is carried out. Designed for fast calculation of discrete convolutions, the *FFT* operates with a complexity of *O* (*n* log *n*) via the Divide and Conquer approach, and FFT-based multiplication is identified as the most efficient method for polynomial multiplication. Factorizing a symmetric matrix *A* is accomplished mathematically via LDL. LDL factorizing is applied in FS to produce a structured representation during the key generation process. $A = L * D * L^T$. *L* is the lower diagonal triangular matrix equivalent to 1; *D* is the diagonal matrix; and *T* is the transform [32]. The production of the public key *PK* and the secret key *SK* helps authenticate the signatures.

ALGORITHM 4: FALCON signature Generation

Input:
msg: Message to sign
SK: Secret key
β^2: Security bound

Output: *signature: (r, s)*
Steps:

1. *Generate random nonce r and hash point:*

- *hash_point ← HashToPoint(r || msg).*

2. *Compute transformed point T_point using FFT.*
3. *Repeat:*
   - *Generate z using FFSampling.*
   - *Compute s and check if $s^2 \leq \beta^2$.*
4. *Convert back using inverse FFT and compress s2.*
5. *Return signature: (r, s).*

Algorithm 4 generates a digital signature with the secret key *SK* and the message [33]. One generates a random integer *r* and then uses the *FFT* to compute hash_point. Using a fast Fourier sampling advanced technique, *FFS sampling effectively* generates short vectors from a Gaussian distribution in network-based encryption, such as FS. It is based on the *FFT*, which allows calculations to be more rapid and complexity to be lowered. Data signing is aided by FFS sampling. The process continues until a signature *s* satisfies the security condition β^2; after that, the signature (*r*, *s*) is restored following data compression.

ALGORITHM 5: FALCON signature verification

Input:

msg, sig (r, s), PK, q, β^2

***Output**: Valid or Invalid*

Steps:

1. Compute hash point: c = HashToPoint(r || msg).
*2. Transform: T_verify = (1/q) * FFT(c) ⊙ FFT(PK).*
3. Inverse FFT on s: s' = invFFT(s).
4. Verify: If $||s'||^2 \leq \beta^2 \rightarrow$ Return "Valid", else "Invalid".

Algorithm 5 authenticates the digital signature by computing the hash point *c*, then using the *FFT*, and comparing the length of the resultant vector *s*' with the security criterion β^2 [33]. If the criterion is met, the signature is accepted; if not, it is denied.

4. TSS METHODOLOGY

In this section, we present an enhanced security system that analyses and protects the massive amount of traffic circle data collected from smart cities via the BB84, FTA, masking, and FS techniques. Figure 3 describes the methodology proposed in this study.

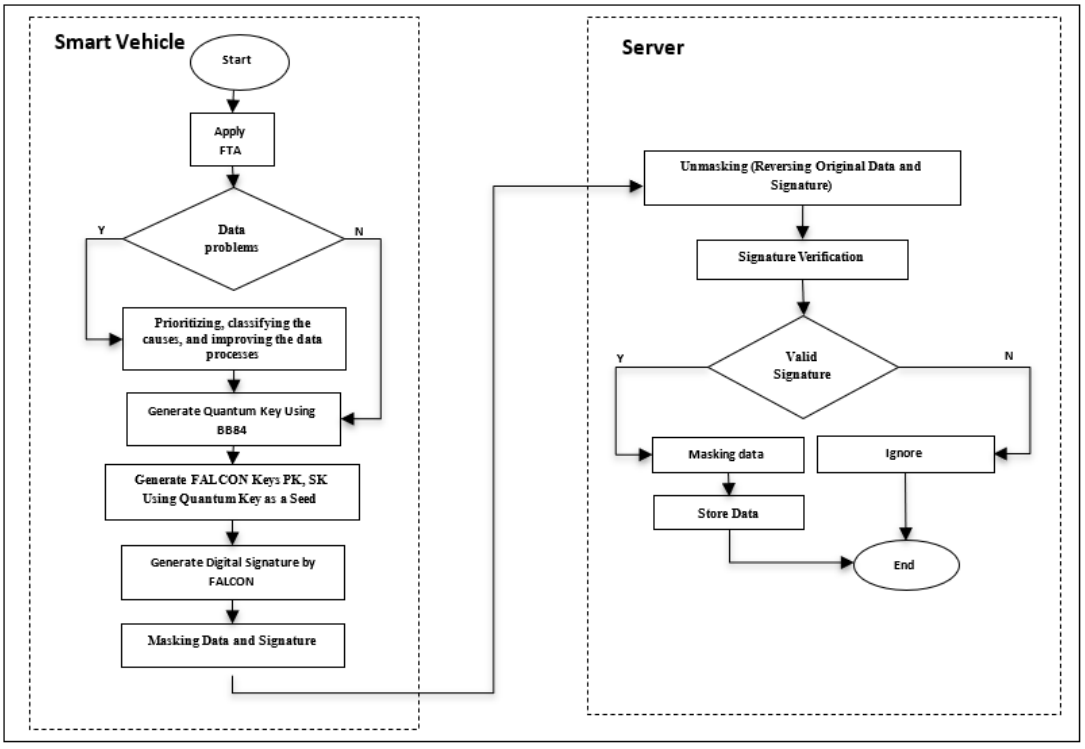

Fig. 3. General proposed methodology for the TSS system.

After data from smart cars and various modes of transportation in the city are collected, they are sent to the traffic department's server via wireless communication channels. To ensure data quality, FTA is used to detect and correct potential errors before further security steps are performed. Because the TTS system relies on the BB84 protocol for distributing a quantum key, it is used as a seed to generate the private key used to digitally sign data via Falcon. A quantum key is generated via BB84 between the smart car and the traffic department server. It is used as a seed to generate Falcon's private key. Smart vehicles then digitally sign traffic data via Falcon. Sensitive data are masked to ensure that the data cannot be traced back to actual users before being sent to the server, which in turn verifies the signature via the corresponding public key to ensure that the data have not been tampered with during transmission. The server also masks sensitive data and creates digital signatures before storing them in the database. This approach provides a strong verification mechanism, as any modification to the data will result in digital signature mismatch and inaccessibility of personal and sensitive data, ensuring the integrity of the data exchanged between the smart media and the traffic server.

4.1 Fault Tree Analysis

FTA is an effective tool that contributes to enhancing the reliability and security of the proposed TSS system. It is used in TSS to analyse data in a systematic way and explore the factors that may lead to system failure and affect data accuracy. The process begins by identifying the end event, such as data integrity loss, and then breaks the problem down into its root causes across multiple levels via logic gates such as AND and OR to illustrate the relationships between events. This technique helps in prioritizing and classifying the causes according to their probability of occurrence and impact on the system. This analysis enables us to predict potential risks and assess their impact on the entire system. In addition, it is used as a preventive tool that helps in developing proactive plans to reduce the probability of failure, whether by improving the concealment processes, enhancing the security of quantum keys, or improving digital signature procedures. The role of FTA is not limited to analysis; rather, it contributes to improving the understanding of the processes on which it depends. By analysing the causal relationships between data.

4.2 Initial Pseudonymization Using Masking

Pseudonymization is a disguise method used to hide sensitive data with nonsensitive codes so that the privacy of those data is maintained. It aims to mask identifiers that make it difficult to identify individuals directly without compromising the system's ability to analyse the data. When sensitive data are collected from smart electrical equipment, codes replace the key fields to protect the original data. Maintaining data privacy and enabling secure data analysis helps reduce the consequences of data breaches or their use, thus reducing risk. The method begins by identifying areas that need defense and identifying a mask, which is a mathematical matrix whose values are combined with the mask using (XOR, AND) gates and masked in the fields that contain sensitive data. This process maintains a secure database where the original data and the mask matrix are kept in a confidential database and can only be accessed by authorized persons. This database requires additional layers of protection and limited access.

4.3 Apply BB84 Protocol

The main goal of BB84 in the TSS system is to enable a secure method for exchanging secret keys applied in the digital signature of data. Using quantum entanglement and noncloning theory, the protocol generates and distributes quantum keys between communicating nodes and thus ensures improved security. The central computer and the deployed sensors collaborate to generate a quantum key, which is then used to verify the authenticity of the data, thus ensuring its confidentiality during transmission. By helping identify any eavesdropping or hacking efforts during key exchange, BB84 ensures a high degree of security. The FS then uses the private key generated by the digital signature of the data, thus proving its integrity and authenticity. This is a well-known and widely used protocol that represents binary values (0, 1) by polarized photons in discrete quantum states. Eavesdropping occurs when the state of the photon changes in line with the ideas of quantum physics, especially the challenge of measurement without changing the state. While the FS for digital signatures builds a strong security system that protects the transmitted data, it has been used for key exchange. In the face of improvements in quantum technology and cryptographic attacks, BB84 enhances the security of the TSS system. It combines digital signatures and provides an innovative way to protect large amounts of sensitive information stored in SCs.

4.4 Digital Signature Using Falcon

Our approach relies heavily on FS. Its key step in TSS is data verification and information protection. It is ideal for SC data security because it uses lattice-based encryption, which helps it resist quantum attacks. This technique generates a secret key to sign the data and a public key to authenticate the data via the BB84 secret key. These two keys ensure the authenticity of the source and the integrity of the data by verifying the transmitted data without revealing the secret key. Using the secret key and complex mathematical operations, FS analyses the sensitive data that have been masked via pseudonyms and plain data and then signs it to verify that the signature fairly represents the identity of the source and detects any changes in the data. The complex approach ensures that the data have not been altered and that any change will result in a mismatch in the signature. Public key verification verifies the validity of the digital signature. The obtained signature is verified via the public key, thus ensuring that the β^2 security criterion is met. The signature confirms that the data have not changed during

transmission. Mathematical networks provide deep security against both conventional and quantum attacks as well as integrity and reliability.

4.5 Final Pseudonymization Using Masking

The final stage of the TSS is to add an additional layer of data protection by masking sensitive information even after it has been digitally signed. This step ensures that the data remain secure and anonymous, reducing the risk of unauthorized identification or misuse. In this stage, masking techniques are applied to replace sensitive fields with masked values, which breaks any direct link to the original data. This complements previous anonymization efforts by addressing security vulnerabilities that may arise during transmission or storage. By making the data unidentifiable, it protects sensitive information from advanced threats, even if the dataset is intercepted. This stage enhances the privacy framework of the TSS, ensuring that the data remain secure while maintaining usability for legitimate analytical purposes.

Algorithm 6: Multilayer data security using FTA, Masking, Key Distribution, and Digital Signatures

Input: *Collected data*
Output: *Integrity data*
Steps:

```
Function main():
    SD ← getSensitiveData()
    DI ← getDeviceSpecificInfo()
    Function performFTA(SD, DI):
        identifiedIssues ← []
        For each issue in analyseFaultTree(SD, DI):
            identifiedIssues.append(issue)
        Resolve(identifiedIssues)
    performFTA(SD, DI)
    Function applyInitialMasking(SD):
        maskedData ← []
        For each field in SD:
            M ← applyMask(field)
            maskedData.append(M)
        Return maskedData
    maskedSD ← applyInitialMasking(SD)
    Function generateSecretKeyUsingBB84():
        SK ← performBB84()
        Return SK
    SK ← generateSecretKeyUsingBB84()
    Function signDataUsingFalcon(SK, maskedSD, DI):
        CD ← combineData(maskedSD, DI)
        S ← applyFalconSignature(SK, CD)
        Return S, CD
    S, CD ← signDataUsingFalcon(SK, maskedSD, DI)
    Function applyFinalMasking(CD):
        finalMaskedData ← []
        For each field in CD:
            M ← applyMask(field)
            finalMaskedData.append(M)
        Return finalMaskedData
    finalMaskedData ← applyFinalMasking(CD)
    StoreOrTransmit(finalMaskedData, S)
```

Algorithm 6 explains that performFTA() analyses the collected sensitive data (SD) and device-specific information (DI). The applyInitialMasking() replaces sensitive data fields with masked values. The generateSecretKeyUsingBB84() function creates a quantum-resistant secret key (SK) via the BB84 quantum key distribution protocol. The signDataUsingFalcon() combines the masked sensitive data (maskedSD) and the device-specific information (DI) into a complete dataset (CD). The applyFinalMasking() function applies an additional layer of masking to the combined and signed data (CD). The StoreOrTransmit() function securely stores or transmits the final masked data (finalMaskedData) along with its signature (S).

The proposed TSS security procedure sequence is shown in Figure 4.

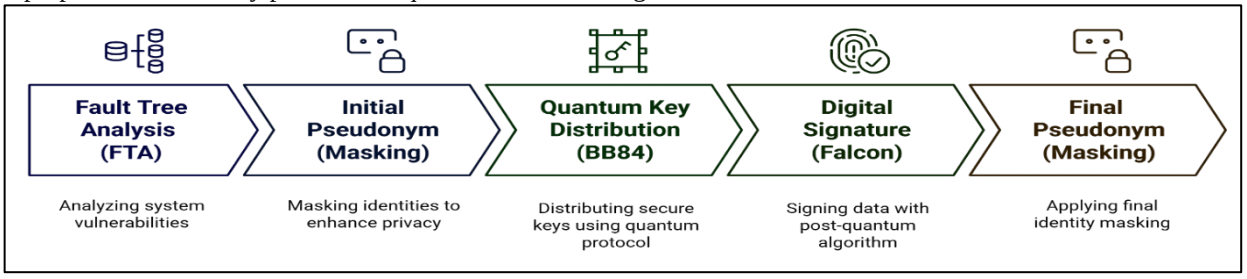

Fig. 4. Security process sequence of the proposed TSS.

5. SECURITY ANALYSIS

In this section, we demonstrate security analysis through attack analysis and testing of the Scyther verification tool.

5.1 Attack Analysis

1. Replay attacks: Replay attacks deceive legitimate participants into thinking that the protocol execution has been successfully finalized by replaying messages in a setting that is different from the original context. The TSS mitigates replay attacks by using digital signatures via the FS, which verifies data integrity and ensures that only new, unspooled messages are accepted.
2. Sybil attacks: Also called false-name attacks. Fake nodes are commonly considered among the most damaging attacks because they create a large number of pseudonymous identities to gain a disproportionately large influence. These fake nodes can disrupt communication or trust in systems. The TSS system combats this by adopting BB84 secure key distribution protocols to ensure the integrity of the connection, allowing only legitimate entities to participate in the network.
3. Blackhole attack: This type of attack is referred to as packet dropping attacks, which significantly deteriorate the network's performance. In this form of attack, the network may contain either a single legitimate node or multiple legitimate nodes. The TSS prevents this by FTA, which is used to detect malicious nodes that may behave abnormally or cause data loss. Data flow paths in the network are analysed to identify nodes that may become “black holes” and how they may affect the network.
4. Eavesdropping: This is a cyberattack where an unauthorized party, referred to as an eavesdropper, intercepts private data between two or more parties and captures sensitive information. Applying pseudonymization technology to mask sensitive data renders the intercepted information meaningless, reducing the amount of information that can be accessed.
5. Tampering attacks: This involves modifying data during transmission, compromising its integrity. The TSS combats tampering by using digital signatures from the FS, which detects any unauthorized modifications. Pseudonymization ensures that sensitive data fields are masked, reducing an attacker's ability to understand the data.
6. Ransomware attacks: The process of encrypting system data and demanding payments to restore access and compromise data availability. The TSS uses FS digital signatures to ensure that only authorized changes to the data are accepted. By masking sensitive data, it becomes more difficult for attackers to identify valuable targets.
7. APTs: Long-range targeted attacks are attacks in which adversaries infiltrate a system to steal data and are often continuous. The quantum key distribution provides a high level of security in data transmission, as any attempt to eavesdrop on quantum keys will result in a change in the quantum state, making the attack detectable. APTs often rely on eavesdropping for long periods of time to gather information, but BB84 makes this activity impossible owing to the nature of quantum physics.
8. Supply chain attacks: Targeting vulnerabilities in the system's built-in components, allowing attackers to introduce malicious elements. These attacks are identified via FTA, which detects any failure in the system components.

Table I provides a comparison between the proposed TSS and various previous systems in repelling attacks.

TABLE II. COMPARISON OF ATTACK PREVENTION BETWEEN THE TSS SYSTEM AND THE SIMILAR SYSTEMS

Attacks	**[34]**	**[35]**	**[36]**	**[37]**	**[38]**	**TSS**
Replay			✓	✓	✓	✓
Supply Chain						✓
Sybil		✓	✓	✓	✓	✓
Blackhole						✓
Eavesdropping	✓	✓	✓	✓	✓	✓
APTs						✓
Tampering	✓	✓	✓		✓	✓
Ransomware						✓

5.2 Scyther as an Analysis Tool

We utilize Scyther simulation as an effective tool for assessing cryptographic systems. This simulation is exceptional because of its sophisticated features, attack monitoring, and swift verification speed. It swiftly authenticates most systems and procedures throughout several sessions without depending on approximation methods, guaranteeing that all identified risks are legitimate and do not jeopardize the system [39]. Users (client-receiver (CR) and server-receiver (SR)) may choose for

unfettered verification or utilize Scyther for assault detection. Scyther is unique among scheme analysis tools because it combines the benefits of model-checking approaches, including attack detection and termination, with the functionalities of theorem proving or abstraction-based methods for unbounded verification. Furthermore, Scyther provides unique features such as attack detection and thorough characterization, which are absent in competing systems. It may be utilized through the graphical user interface, the command-line interface, or as a backend for analytical programs employing Python interface functions. Scyther employs the analysis of security protocols across many approaches to identify data breaches and ensure the confidentiality and integrity of information during transmission between a client and a server or among corporations and organizations. This tool uses security requirement attributes to verify certain authentication data, including Aliveness, Nisynch, Niagree, and Weakagree.

5.3 Scyther's Authentication Test Results

We illustrate the evaluation solution of the proposed TSS using the Scyther tool. The test outcomes of our procedure are predicated on the following events: Alive, Niagree, Nisynch, and Secret. The results indicate that the security parameters are sent between the network entities (the traffic officer administrator (TOA) and the traffic department server (TDS)) without any threats or assaults. Figure 5 illustrates the design of an attack-resistant system in the proposed TSS field. Furthermore, we finalized a summary of the role descriptions for the proposed TSS system, with the outcomes shown in Figures 5 and 6. The TOA is responsible for managing the smart power plant, collecting data, and generating security values such as keys and quantum codes to ensure that the information is protected before being sent to the central TDS. The TDS receives the data received from the TOA, verifies its integrity, analyses it, and manages the necessary security keys and directions. The coordination between the two sides is based on exchanging data in a way that ensures the security, synchronization, and privacy of information related to the power plants.

Scyther results : characterize

Claim				Status		Comments	Patterns
TSS	TOA	TSS,TOA2	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern
	TDS	TSS,TDS2	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern

Done.

Fig. 5. TSS system summary of the characterized roles.

Scyther results : verify

Claim				Status		Commer
TSS	TOA	TSS,4	Nisynch	Ok	Verified	No attacks.
		TSS,TOA2	Secret quantumkey	Ok	Verified	No attacks.
		TSS,TOA3	Secret pseudonym	Ok	Verified	No attacks.
		TSS,TOA4	Alive nonceTOA	Ok	Verified	No attacks.
		TSS,TOA5	Nisynch	Ok	Verified	No attacks.
		TSS,TOA6	Niagree	Ok	Verified	No attacks.
	TDS	TSS,5	Nisynch	Ok	Verified	No attacks.
		TSS,TDS2	Secret quantumkey	Ok	Verified	No attacks.
		TSS,TDS3	Secret pseudonym	Ok	Verified	No attacks.
		TSS,TDS4	Alive nonceTDS	Ok	Verified	No attacks.
		TSS,TDS5	Nisynch	Ok	Verified	No attacks.
		TSS,TDS6	Niagree	Ok	Verified	No attacks.

Done.

Fig. 6. Depiction of the Scyther results.

6. PERFORMANCE ANALYSIS

The performance evaluation of the proposed TSS is presented in this section.

6.1 Theoretical Performance Analysis

To guarantee the security of large amounts of data and operational efficacy in SC applications, particularly in the traffic circle, the TSS system is implemented. To guarantee the secure utilization of power plant data within the SC infrastructure, the system's efficiency is assessed via BB84, FS, FTA, pseudonymization, and processing. This is achieved through the implementation of security and analysis techniques that are both efficient and rapid while also being appropriate for the limited capacity of sensors and smart transportation. FTA technology was implemented to increase the accuracy of the collected data, ensure its consistency, and reduce the percentage of errors caused by misconduct or incorrect data input. This technology analyses the data and identifies errors prior to processing. To safeguard the confidentiality and security of sensitive data and prevent their exposure, pseudonymization technology was implemented. This technology converts sensitive data into fictitious identifiers, thereby reducing data exposure and safeguarding privacy. It is a less complex process than encryption, which frequently involves the use of large and intricate keys that impose a burden on the network. The system is engineered to be performance efficient, ensuring high security without significantly affecting the data transfer speed. This is achieved by implementing signature and signature verification processes that minimize latency and ensure data security, thereby making it suitable for sensitive operations and enhancing user confidence in incoming data. TSS is a cutting-edge approach to safeguarding traffic data in smart cities, as it seamlessly integrates operational efficiency with high security, rendering it appropriate for critical infrastructure. The system is anticipated to overcome performance obstacles as a result of enhancements in the technology and apparatus that support it. Table II presents the results of an evaluation of three digital signature algorithms using various criteria. Because of its lattice-based cryptographic design, FS provides superior quantum security; this makes it suitable for resource-constrained IoSCT and makes it more resistant to quantum attacks. The three rival algorithms, Rivest, Shamir, and DSA, are vulnerable to assaults from Shor's algorithm. Additionally, CZ-Rainbow tends to be less efficient because of the complexity of the keys and is not ideal for these environments. Table III juxtaposes the security, important dimensions, and applicability of the three protocols for applications in SCs. BB84 is the most efficient in terms of speed and has the best degree of protection against quantum assaults. Conversely, RSA and Diffie–Hellman exhibit diminished security and efficiency with intricate keys, making them the most appropriate for these applications.

TABLE III. A COMPARISON OF FS WITH OHER DIGITAL SIGNATURE ALGORITHMS

Criteria	**TSS**	**[40,41]**	**[41]**
	FALCON	**CZ-Rainbow**	**DSA**
Security	Post-quantum secure (NTRU)	Post-quantum secure (Multivariate)	Not quantum-secure
Public Key	897–1793 B	58.8–523.6 KB	1024–3072 bits
Secret Key	32 B	101.2–1375.7 KB	1024–3072 bits
Signature	666–1280 bytes	528–1696 bits	320 bits
Efficiency	Small keys/signatures, high speed	Large keys, small signatures, medium speed	Large keys, slower performance
Suitability for IoSCT	Suitable	Suitable for large storage resources	Not suitable for the future IoSCT needs

TABLE IV. A COMPARISON OF BB84 WITH OTHER KEY EXCHANGE PROTOCOLS

Criteria	**TSS**	**[42,43]**	
	BB84	**Diffie-Hellman**	**RSA**
Security	Quantum-resistant	Prone to quantum attacks	Prone to quantum attacks
Key size	Approximately 256 bits	Relies on large keys >2048 bits	Relies on large keys >2048 bits
Suitability for IoSCT	Suitable	Appropriate for substantial resources	Appropriate for substantial resources

6.2 Practical Performance Analysis

Java was used to implement the proposed TSS system algorithms in Ubuntu 18.04.6 LTS. The computer in question has an Intel(R) Core (TM) i5-1135G7 CPU, 9th generation, and 8.00 MB RAM. We executed all our algorithms 100 times in Java to evaluate them explicitly and extract the results accurately. The obtained numerical data were then analysed via Microsoft Excel tables in Ubuntu to generate performance figures and graphs, which will be briefly discussed later. Figure 7 shows the execution times of applying FTA to big data and the masking process for sensitive data. Figure 8 illustrates the implementation of quantum key generation via BB84 protocols, where the average time taken to generate keys was approximately 0.46 milliseconds. As Figure 9 depicts the FS sign and validation of the signatures of the proposed TSS system, the average signing time was approximately 0.002 milliseconds. In comparison, the average signature verification time was approximately 0.004 milliseconds. These numbers show that FALCON outperforms other digital signature

algorithms in terms of speed and resistance to quantum computing. The results showed that the average execution time of the TSS system was 0.54 when the system was executed from the first execution to the hundredth execution, which illustrates the performance speed, as shown in Figure 10.

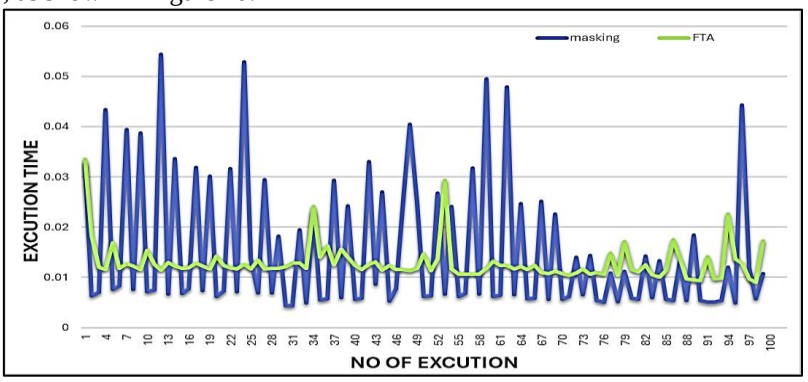

Fig. 7. Execution time of applying FTA data and masking.

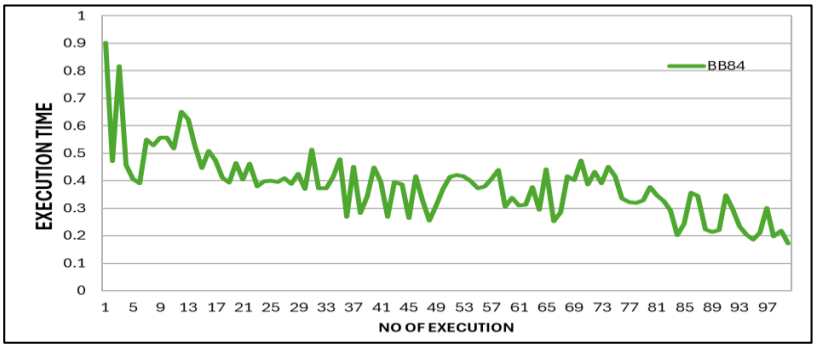

Fig. 8. Using QKD to generate quantum keys.

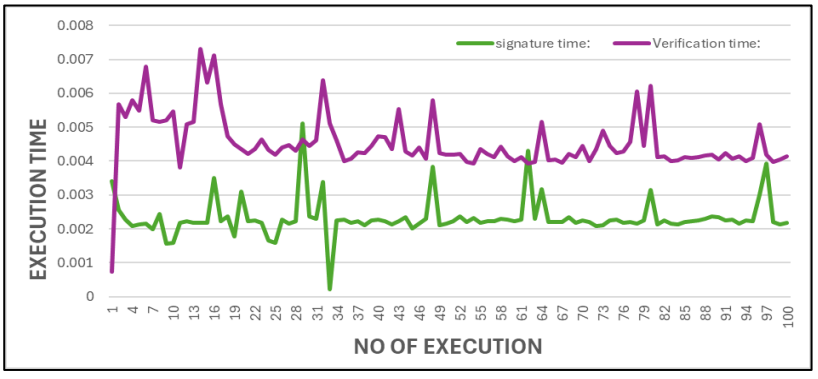

Fig. 9. FS operations for signature and verification.

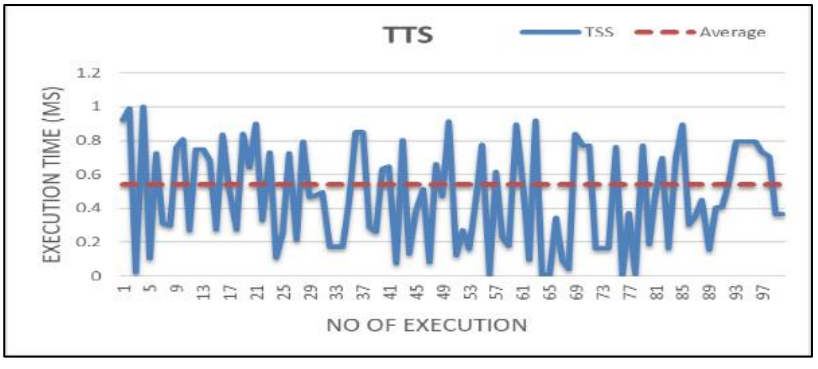

Fig. 10. Execution time in the proposed TSS system.

In the proposed TSS system, the following results are obtained after executing the code 100 times: The true positive (TP) is 88, the false positive (FP) is 6, the false negative (FN) is 2, and the true negative (TN) is 4 for data that are supposed to be protected. The following measures are used:

1. Precision: It is used to measure the accuracy of a system in identifying valid and securely verified transactions or data.

$$Precision = \frac{TP}{TP + FP} \times 100\% = \frac{88}{88 + 6} \times 100\% = 93.6\ \%$$

2. Recall: It plays a vital role in measuring the system's ability to identify all sensitive data that require privacy.

$$Recall = \frac{TP}{TP + FN} \times 100\% = \frac{88}{88 + 2} \times 100\% = 97.8\%$$

3. F1-Score: It is a metric used to evaluate the performance of a classification model, especially in tasks involving multiclass classification. The harmonic mean emphasizes the smaller value, making it suitable for scenarios where both precision and recall are crucial and where

$$F1_{Score} = 2 \times \frac{Precision \times Recall}{Precision + Recall} \times 100\% = 95.6\ \%$$

Table V provides a comparison between the proposed TSS system and various previous systems in terms of performance on the basis of the precision, recall, and F1 score metrics. Additionally, Figure 11 displays a comparison with other studies. Our proposed system has shown its superiority over other security systems in terms of precision, recall, and F1_Score between the proposed TSS and similar systems.

TABLE V. A COMPARISON OF EXECUTION TIMES, PRECISION, RECALL AND F1-SCORE

Parameters	**TSS**	**Previous Research**
Average Execution Time	0.54 ms	50.6 ms, [44]
Precision	93.6 %	92.3 %,[45] 91.8 %, [46]
Recall	97.8 %	91.8 %,[45] 90.7 %,[46]
F1_Score	95.6 %	92.0 %,[45] 91.2 %,[46]

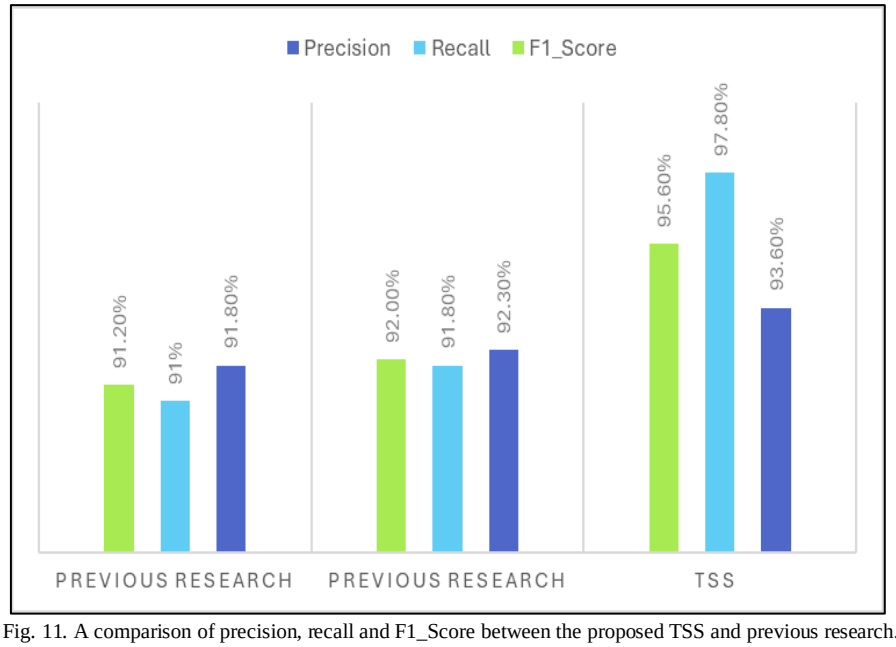

Fig. 11. A comparison of precision, recall and F1_Score between the proposed TSS and previous research.

7. CONCLUSION

In this work, we suggested a strong security architecture that combines FTA, BB84 quantum key distribution, masking methods, and Falcon signatures to protect traffic data in smart cities. To ensure the safe collection, transfer, and authentication of smart city data, the suggested technique addresses important security issues, such as data integrity,

privacy, and resistance to quantum-based assaults. Our study presents TSS, an innovative method to address the challenges of secure and high-quality data in IoSCT applications, particularly within traffic circles.

By use of FTA, early identification of possible traffic data collection faults is made possible, therefore improving the dataset's dependability before the application of security policies. Safely sharing cryptographic keys among smart city infrastructures depends critically on the BB84 quantum key distribution protocol, hence reducing authentication vulnerabilities. Furthermore, adding a layer of privacy protection is a masking methods, which stop sensitive data from being exposed even in the case of data interception. Our results show that the suggested method is a potential option for contemporary smart city infrastructures, as it considerably improves data security and privacy preservation. Investigating alternative quantum-resistant cryptographic techniques and extending the framework to other vital smart city uses, such as energy management, will be the main priorities of future studies.

Conflicts of interest

The authors declare that they have no conflicts of interest.

Funding

There is no funding from sponsors or institutions for this paper.

References

[1] M. Imran, A. B. Altamimi, W. Khan, S. Hussain, and M. Alsaffar, "Quantum cryptography for future networks security: A systematic review," IEEE Access, 2024. Available: https://doi.org/10.1109/ACCESS.2024.3504815.

[2] W. A. Jebbar, R. H. Razzaq, D. H. Tahayur, and M. Al-Zubaidie, "Blockchain and cryptography framework of e-apps with big data," Journal of Education for Pure Science-University of Thi-Qar, 14(3), 2024. Available: https://doi.org/10.32792/jeps.v14i3.545.

[3] K. Ahmad, M. Maabreh, M. Ghaly, K. Khan, J. Qadir, and A. Al-Fuqaha, "Developing future human-centered smart cities: Critical analysis of smart city security, data management, and ethical challenges," Computer Science Review, vol. 43, p. 100452, 2022. Available: https://doi.org/10.1016/j.cosrev.2021.100452.

[4] A. R. Javed, F. Shahzad, S. ur Rehman, Y. B. Zikria, I. Razzak, Z. Jalil, and G. Xu, "Future smart cities: Requirements, emerging technologies, applications, challenges, and future aspects," Cities, vol. 129, p. 103794, 2022. Available: https://doi.org/10.1016/j.cities.2022.103794.

[5] R. H. Razzaq, M. Al-Zubaidie, and R. G. Atiyah, "Intermediary decentralized computing and private blockchain mechanisms for privacy preservation in the Internet of medical things," Mesopotamian Journal of CyberSecurity, 4(3), 152-165, 2024. Available: https://doi.org/10.58496/MJCS/2024/020.

[6] R. Sánchez-Corcuera, A. Nuñez-Marcos, J. Sesma-Solance, A. Bilbao-Jayo, R. Mulero, U. Zulaika, G. Azkune, and A. Almeida, "Smart cities survey: Technologies, application domains and challenges for the cities of the future," International Journal of Distributed Sensor Networks, vol. 15, no. 6, 2019. Available: https://doi.org/10.1177/1550147719853984.

[7] S. Siddiqui, S. Hameed, S. A. Shah, A. K. Khan, and A. Aneiba, "Smart contract-based security architecture for collaborative services in municipal smart cities," Journal of Systems Architecture, vol. 135, 2023. Available: https://doi.org/10.1016/j.sysarc.2022.102802.

[8] D. H. Tahayur, and M. Al-Zubaidie, "Establishing an optimized searching approach with e-signatures based on blockchain for electronic agriculture applications," In AIP Conference Proceedings (Vol. 3264, No. 1). AIP Publishing, March 2025. Available: https://doi.org/10.1063/5.0258784.

[9] M. Al-Zubaidie, and W. A. Jebbar, "Providing security for flash loan system using cryptocurrency wallets supported by XSalsa20 in a blockchain environment," Applied Sciences, 14(14), 6361, 2024. Available: https://doi.org/10.3390/app14146361.

[10] D. Kales and G. Zaverucha, "An attack on some signature schemes constructed from five-pass identification schemes," in Lecture Notes in Computer Science, Cham: Springer International Publishing, 2020. Available: https://doi.org/10.1007/978-3-030-65411-5_1.

[11] R. Chen, Y. Li, Y. Yu, H. Li, X. Chen, and W. Susilo, "Blockchain-based dynamic provable data possession for smart cities," IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4143–4154, 2020. Available: https://doi.org/10.1109/JIOT.2019.2963789.

[12] E. Ismagilova, L. Hughes, and N. P. Rana, "Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework," Inf Syst Front, 24, 393–414, 2022. https://doi.org/10.1007/s10796-020-10044-1.

[13] K. Ahmad, M. Maabreh, M. Ghaly, K. Khan, J. Qadir, and A. Al-Fuqaha, "Developing future human-centered smart cities: Critical analysis of smart city security, data management, and ethical challenges," Computer Science Review, vol. 43, p. 100452, 2022. Available: https://doi.org/10.1016/j.cosrev.2021.100452

[14] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' IoT communications," Transactions on Emerging Telecommunications Technologies, vol. 33, no. 3, p. e3677, 2022. Available: https://doi.org/10.1002/ett.3677.

[15] F. S. Gharehchopogh, "Quantum-inspired metaheuristic algorithms: comprehensive survey and classification," Artif Intell Rev 56, 5479–5543, 2023. https://doi.org/10.1007/s10462-022-10280-8.

[16] N. J. Mohammed, "Quantum cryptography in convolution neural network approach in smart cities," Journal of Survey in Fisheries Sciences, vol. 10, no. 2S, pp. 2043–2056, 2023. Available: https://doi.org/10.17762/sfs.v10i2S.1105.
[17] G. R. Figlarz and F. P. Hessel, "Enhancement in LoraWAN's security with post-quantum key encapsulation method," 2024 IEEE 10th World Forum on Internet of Things (WF-IoT), Ottawa, ON, Canada, 2024, pp. 804-809, http://doi.org/10.1109/WF-IoT62078.2024.10811133.
[18] D. Das, P. Chaterjee, U. Ghosh, and B. Blakely, "Secure and privacy aware data sharing approach for smart electric vehicles," IEEE Consumer Electronics Magazine, 2025. Available: https://doi.org/10.1109/MCE.2025.3529398.
[19] H. Y. Peivandizadeh, B. Adarbah, A. Molavi, A. Mohajerzadeh, and A. H. Al-Badi, "A secure key exchange and authentication scheme for securing communications in the Internet of Things environment," Future Internet, vol. 16, no. 10, p. 357, 2024. Available: https://doi.org/10.3390/fi16100357.
[20] M. Yazdi, J. Mohammadpour, H. Li, H. Z. Huang, E. Zarei, R. G. Pirbalouti, and S. Adumene, "Fault tree analysis improvements: A bibliometric analysis and literature review," Quality and Reliability Engineering International, 39(5), 1639-1659, 2023.
[21] A. Abdulhamid, S. Kabir, I. Ghafir, and C. Lei, "Quantitative failure analysis for IoT systems: an integrated model-based framework," International Journal of System Assurance Engineering and Management, pp. 1–23, 2025. Available: https://doi.org/10.1007/s13198-024-02700-5.
[22] S. M. Nicoletti, E. M. Hahn, and M. Stoelinga, "BFL: A logic to reason about fault trees," in 2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 441–452, 2022. Available: https://doi.org/10.1109/DSN53405.2022.00051.
[23] J. Heaton, "'Pseudonyms are used throughout': A footnote, unpacked," Qualitative Inquiry, vol. 28, no. 1, pp. 123–132, 2022. Available: https://doi.org/10.1177/10778004211048379.
[24] R. Tandon and P. K. Gupta, "A novel pseudonym assignment and encryption scheme for preserving the privacy of military vehicles," Defence Science Journal, vol. 71, 2021. Available: https://doi.org/10.14429/dsj.71.15534.
[25] M. Mehic, L. Michalek, E. Dervisevic, P. Burdiak, M. Plakalovic, J. Rozhon, and M. Voznak, "Quantum cryptography in 5G networks: a comprehensive overview," IEEE Communications Surveys & Tutorials, 2023. Available: https://doi.org/10.1109/COMST.2023.3309051.
[26] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Reviews of Modern Physics, vol. 81, no. 3, pp. 1301–1350, 2009. Available: https://doi.org/10.1103/RevModPhys.81.1301.
[27] D. H. Tahayur, and M. Al-Zubaidie, "Enhancing electronic agriculture data security with a blockchain-based search method and e-signatures," Mesopotamian Journal of CyberSecurity, 4(3), 1-21, 2024. Available: https://doi.org/10.58496/MJCS/2024/012.
[28] E. Karabulut and A. Aysu, "A hardware-software co-design for the discrete Gaussian sampling of falcon digital signature," in 2024 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 90–100, 2024. Available: https://doi.org/10.1109/HOST55342.2024.10545399.
[29] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pp. 197–206, 2008. Available: https://doi.org/10.1145/1374376.1374407.
[30] Y. Kim, J. Song, and S. C. Seo, "Accelerating FALCON on ARMv8," IEEE Access, vol. 10, pp. 44446–44460, 2022. Available: https://doi.org/10.1109/ACCESS.2022.3169784.
[31] M. Vidaković and K. Miličević, "Performance and applicability of post-quantum digital signature algorithms in resource-constrained environments," Algorithms, vol. 16, no. 11, p. 518, 2023. Available: https://doi.org/10.3390/a16110518.
[32] P. A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, and Z. Zhang, "FALCON: Fast-Fourier lattice-based compact signatures over NTRU, Specification v1. 2," NIST Post-Quantum Cryptography Standardization Round, vol. 3, 2020.
[33] Y. Kim, J. Song, and S. C. Seo, "Accelerating FALCON on ARMv8," IEEE Access, vol. 10, pp. 44446–44460, 2022. Available: https://doi.org/10.1109/ACCESS.2022.3169784.
[34] M. Keerthika and D. Shanmugapriya, "Wireless sensor networks: Active and passive attacks-vulnerabilities and countermeasures," Global Transitions Proceedings, vol. 2, no. 2, pp. 362–367, 2021. Available: https://doi.org/10.1016/j.gltp.2021.08.045.
[35] M. Al-Zubaidie and W. Jebbar, "Transaction security and management of blockchain-based smart contracts in e-banking-employing microsegmentation and yellow saddle Goatfish," Mesopotamian Journal of CyberSecurity, vol. 4, no. 2, pp. 1–19, 2024. Available: https://doi.org/10.58496/MJCS/2024/005.
[36] B. Saha, M. M. Hasan, N. Anjum, S. Tahora, A. Siddika, and H. Shahriar, "Protecting the decentralized future: An exploration of common blockchain attacks and their countermeasures," arXiv preprint, 2023. Available: https://doi.org/10.48550/arXiv.2306.11884.

[37] M. Al-Zubaidie and R. A. Muhajjar, "Integrating trustworthy mechanisms to support data and information security in health sensors," Procedia Computer Science, vol. 237, pp. 43–52, 2024. Available: https://doi.org/10.1016/j.procs.2024.05.078.

[38] S. Mollajafari and K. Bechkoum, "Blockchain technology and related security risks: Towards a seven-layer perspective and taxonomy," Sustainability, vol. 15, no. 18, p. 13401, 2023. Available: https://doi.org/10.3390/su151813401.

[39] G. S. Shyaa, and M. Al-Zubaidie, "Securing transactions using hybrid cryptography in e-commerce apps," Journal of Education for Pure Science-University of Thi-Qar, 13(3), 2023. Available: https://doi.org/10.32792/jeps.v13i3.357.

[40] M. A. León Chávez, and F. Rodríguez Henríquez, "Post-quantum digital signature for the mexican digital invoices by Internet," Computación y Sistemas, 25(4), 729-737, 2021. Available: https://doi.org/10.13053/cys-25-4-4048.

[41] R. Flores-Carapia, V. M. Silva-García, and M. A. Cardona-López, "A chaotic digital signature algorithm based on a dynamic substitution box," Scientific Reports, 15(1), 2435, 2025. https://doi.org/10.1038/s41598-024-83943-x.

[42] A. Adu-Kyere, E. Nigussie, and J. Isoaho, "Quantum key distribution: Modeling and simulation through BB84 protocol using python3," Sensors, 22(16), 6284, 2022.

[43] M. Saračević, S. Adamović, M. Maček, M. Elhoseny, and S. Sarhan, "Cryptographic keys exchange model for smart city applications," IET Intelligent Transport Systems, vol. 14, no. 11, pp. 1456–1464, 2020. Available: https://doi.org/10.1049/iet-its.2019.0855.

[44] T. Sharma, M. R. Kumar, S. Kaushal, D. Chaudhary, and K. Saleem, "Privacy aware post quantum secure ant colony optimization ad hoc on-demand distance vector routing in intent based Internet of vehicles for 5G smart cities," IEEE Access, pp. 110391–110399, 2023. Available: https://doi.org/10.1109/ACCESS.2023.3311515.

[45] H. Shahid, H. Ashraf, H. Javed, M. Humayun, N. Z. Jhanjhi, and M. A. AlZain, "Energy optimised security against wormhole attack in IoT-based wireless sensor networks," Computational Materials Continuum, vol. 68, no. 2, pp. 1967–1981, 2021. Available: https://doi.org/10.32604/cmc.2021.015259.

[46] R. D. Prasad, and M. Srivenkatesh, "A hybrid model combining graph neural networks, reinforcement learning, and autoencoders for automated code refactoring and optimization," Journal of Theoretical and Applied Information Technology, 103(1), 2025.

[47] J. H. Namdar and J. F. Yonan , Trans., “Revolutionizing IoT Security in the 5G Era with the Rise of AI-Powered Cybersecurity Solutions”, *BJIoT*, vol. 2023, pp. 85–91, Nov. 2023, doi: 10.58496/BJIoT/2023/011.

[48] M.. Abotaleb, E.-S. M. El-kenawy, and K. . Dhoska, “Deep Learning-Based Time Series Forecasting: A Convolutional Neural Network Approach for Predicting Inflation Trends”, EDRAAK, vol. 2025, pp. 19–28, Jan. 2025, doi: 10.70470/EDRAAK/2025/004.