IET Smart Cities

WILEY

The Institution of Engineering and Technology

REVIEW OPEN ACCESS

Securing Smart City Ecosystems: A Taxonomy-Based Review of Emerging Technologies and Frameworks for Scalable Collaborative Services

Usama Antuley[1] | Sufian Hameed[1] | Shahbaz Siddiqui[1] | Syed Attique Shah[2]

[1]Fast School of Computing, National University of Computer and Emerging Sciences, Karachi, Pakistan | [2]Department of Computer Science, Birmingham City University, Birmingham, UK

Correspondence: Syed Attique Shah (syedattique.shah@bcu.ac.uk)

Received: 3 February 2025 | **Revised:** 1 May 2025 | **Accepted:** 1 July 2025

Handling Editor: Wu Yongdong

Funding: The authors received no specific funding for this work.

Keywords: artificial intelligence | blockchain | information security and privacy | intelligent control | quantum computing | smart cities | systematic literature review | trust

ABSTRACT

The smart city concept integrates various collaborative services to enhance urban living. However, these services introduce significant security concerns, especially in authentication, authorisation, and access control (AAA). To address these security challenges, researchers must design and implement frameworks that safeguard data exchange between smart services. This paper offers a taxonomy-based review of current solutions, focusing on how emerging technologies like Blockchain, artificial intelligence (AI), quantum computing, and hybrid approaches address AAA concerns. We evaluate these technologies based on key factors such as confidentiality, integrity, availability (CIA), trust, privacy, and scalability. Through a systematic review of literature from 2017 to 2024, we classify and assess methods that strengthen authentication, optimise access control, and refine authorisation processes to mitigate risks in data sharing. A major contribution of this paper is the integration of case studies, demonstrating real-world applications of these technologies in smart city contexts. Additionally, we explore the applicability of these solutions, highlighting their challenges and future potential. This research also outlines future directions for building secure, efficient, and scalable smart city ecosystems, ultimately facilitating the development of adaptable frameworks for smart city services.

1 | Introduction

Smart cities aim to transform urban life by integrating multiple smart services to enhance sustainability, efficiency and quality of life for their residents. Real-time data collection and analysis facilitate the integration of smart city ecosystems, improving services such as transportation, energy, healthcare, and public safety [1]. For example, Barcelona's intelligent street lighting system adjusts brightness according to pedestrian and vehicle movement, reducing energy consumption and costs [2]. Similarly, integrated waste management systems equipped with sensors monitor waste levels and optimise collection routes, promoting cleanliness and reducing resource consumption. The Amsterdam transport system addresses traffic congestion by encouraging cycling and using electric vehicles, thus supporting sustainable commuting practices [3]. For instance, V2X (Vehicle-to-Everything) smart services integrate with the intelligent transportation system to provide consumers with car data. Unauthorised access to these collaborative services can significantly jeopardise public safety through data breaches, traffic

interruptions, or system manipulations, including altering traffic signals. Figure 1 provides an overview of smart city applications. Although smart cities promise enhanced efficiency through smart collaborative services, they also face significant challenges related to authentication, authorisation and access control (AAA) during data exchanges between these services, particularly in terms of security, privacy, trust, and scalability [4]. Using collaborative smart services also increases the risk of unauthorised access to sensitive financial and personal data [5]. Furthermore, manipulation of vital systems, such as healthcare and transportation, could erode public confidence (trust) and compromise the general integrity of smart city infrastructure. Furthermore, the exponential growth of data and services in smart cities presents challenges in scalability [6].

Smart applications in urban ecosystems rely heavily on strong authentication mechanisms when smart services exchange their data to verify the user's and device's identities and greatly control the accessibility of sensitive data and critical services to authorised parties only [7]. In essence, effective authentication procedures embedded within the infrastructure of these advanced network devices act as the first line of defence against potential breaches [8]. However, such mechanisms can lead to severe vulnerabilities in the absence or inadequacy of these mechanisms. For example, if the authentication protocols are weak or insufficient, easy unauthorised access to these collaborative smart services becomes a risk of compromising the confidentiality and integrity of sensitive data with potential manipulation or theft. Moreover, authentication breaches are dangerous to individual services and threaten the cross-linked nature of a smart city ecosystem, with cascading failures possible in multiple domains, such as transportation, healthcare, or energy management. Robust authorisation mechanisms are needed to support smart applications in collaborative services in urban ecosystems, ensuring safe and effective access control. Authorisation defines and enforces the actions authenticated users or devices can perform, especially during collaborative activities involving interrelated smart services [9]. The systems protect the integrity of sensitive operations by ensuring that access to resources and functions is strictly limited to authorised entities. Implementing robust authorisation protocols is essential to ensure both the reliability and security of collaborative smart services [10]. Without strong and properly executed authorisation mechanisms, such services can be exploited. For example, in smart healthcare settings, unauthorised access to patient information or modification of diagnostic equipment can jeopardise privacy and safety [11]. Similarly, in intelligent transportation systems, weak authorisation controls may allow for unauthorised manipulation of traffic signals that may lead to significant disruptions or accidents. Effective solutions to such vulnerabilities require robust authorisation strategies. Role and attribute-based access control models are considered effective methods for enabling smart collaborative services through the assignment based on specific roles, responsibilities, or contextual elements such as location and task requirements [12]. Adaptive authorisation methods improve security by integrating real-time elements, guaranteeing that collaborative services remain secure and adaptable. ML has transformed the operations of urban systems by enabling real-time analytics, automation, and decision-making in smart city environments. Although there is a tremendous potential for such applications, their implementation faces massive barriers related to AAA, primarily towards securing and guaranteeing the reliability of collaborative services. In the case of Intelligent Transportation Systems (ITS), Machine Learning (ML) techniques process information from IoT sensors installed on roads and vehicles to improve traffic flow management. If unauthorised access occurs, it may inject malicious data that will introduce traffic flow prediction errors that could trigger congestion and accidents [13].

To address these critical challenges, smart city infrastructures are adopting three disruptive technologies. Blockchain establishes a tamper-proof, decentralised ledger system that enables verifiable peer-to-peer transactions through cryptographic hashing and distributed consensus protocols, removing reliance on central authorities [14]. Artificial Intelligence (AI) develops cognitive systems capable of autonomous reasoning, pattern recognition, and predictive analytics to optimise urban operations and service delivery [15]. Quantum computing leverages quantum superposition and entanglement phenomena to solve complex urban optimisation and cryptographic problems exponentially faster than classical systems.

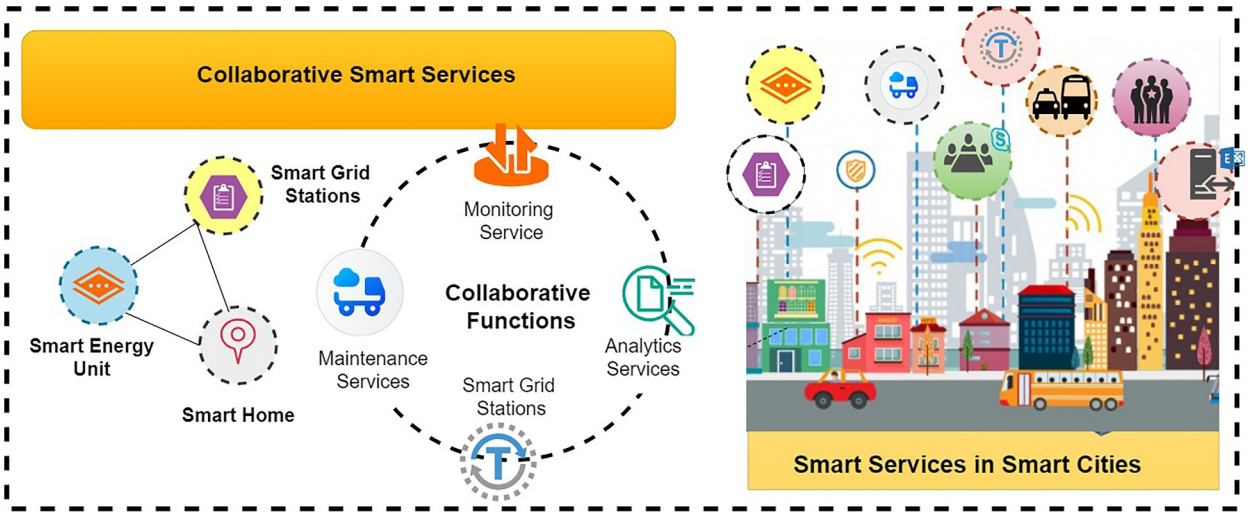

FIGURE 1 | An illustration of collaborative smart city applications.

As described above, emerging technologies like Blockchain, AI, and quantum computing are enhancing the possibilities for smart city applications by tackling AAA challenges in these domains. These technologies offer innovative features that improve security, integrity, and scalability in collaborative services [16]. Specifically, they provide a decentralised and unchangeable framework to facilitate AAA protocols. This design not only eliminates the need for an authentication server but also guarantees secure verification of users and devices using sophisticated cryptographic techniques. In addition, smart contracts running on Blockchain automatically enforce controls, with predetermined rules about how data should be accessed and used for control reasons, so direct user input is not required [17]. The immutable characteristic of Blockchain ensures the integrity of the data by making any unauthorised alteration immediately detectable, making it crucial for fields such as healthcare and transport. Furthermore, ML contributes to AAA security through adaptive real-time threat responses. ML algorithms make inferences for behavioural patterns and contextual information, such as login habits or device usage, to implement advanced authentication mechanisms. For example, an ML-based system would send additional verification steps when it finds suspicious activities such as login attempts from unknown devices. In addition, ML self-provides dynamic updates to authentication policies based on variable time values such as the user's location or their behaviour patterns [18]. ML-based solutions can detect abnormalities in the usual pattern, and then unauthorised access and data breaches are detected early before it becomes a huge problem, thus protecting collaborative smart services. The ultimate computational capability to solve AAA problems with scalability and cutting-edge cryptography solutions is provided by quantum computing. Lattice-based cryptography is one of the quantum-resistant encryption techniques; it is a safe authentication technique impervious to adversaries with quantum-capable computers [19]. In smart city ecosystems, quantum algorithms also effectively manage complex permissions, streamline access control procedures, and scale to handle the growing number of users and devices. This keeps the authorisation responsive and strong as the system grows.

Blockchain, AI, and quantum computing each address distinct facets of AAA mechanisms in smart cities. Blockchain's decentralised architecture ensures tamper-proof authorisation and access control through immutable ledgers and smart contracts, eliminating reliance on centralised authorities [20–22]. AI enables dynamic authentication by analysing behavioural patterns (e.g., login habits, device usage) and adapting security policies in real time, thereby mitigating unauthorised access [23]. Quantum computing addresses future-proof scalability in AAA through quantum-resistant cryptographic techniques (e.g., lattice-based cryptography), safeguarding authentication and authorisation processes against quantum-enabled threats [19]. Together, these technologies synergise to address the CIA triad: Blockchain ensures data integrity, AI enhances availability via adaptive monitoring, and quantum computing fortifies confidentiality, while balancing trust and scalability in collaborative smart ecosystems.

In the following subsections, we present the motivation behind this study, the related surveys published in the existing literature, and this survey's main contributions.

1.1 | Motivation of the Survey

Smart cities aim to improve the efficiency of urban services and promote sustainability through the integration of advanced technologies such as Artificial Intelligence (AI), Blockchain, and Quantum Computing. These technologies are essential for optimising resources and automating services across critical domains such as smart healthcare, smart homes, and transportation. However, the interconnectedness of these systems introduces significant security challenges. Ensuring robust Authentication, Authorisation, and Access Control (AAA) mechanisms, alongside maintaining the Confidentiality, Integrity and Availability (CIA) of data, is critical to protecting sensitive information and maintaining trust in smart city infrastructures.

In this survey, our objective is to present existing solutions that address security concerns related to authentication, authorisation, and access control during collaborative tasks in smart city applications. We investigate technological solutions that protect the infrastructure of smart cities and provide a comparative analysis of these technologies across key domains such as smart homes, smart healthcare, and Intelligent Transportation Systems (ITS). Through this analysis, we evaluate how Blockchain, AI and Quantum Computing enhance AAA mechanisms and their overall impact on security, privacy, trust, and scalability in each domain. Furthermore, we integrate case studies to strengthen the findings, showcasing real-world applications of these technologies and illustrating the practical challenges and benefits of their implementation in smart city environments.

Additionally, this survey highlights the significance of Hybrid Approaches, which combine the strengths of Blockchain, AI and Quantum Computing to overcome the limitations of individual technologies. Hybrid solutions offer a more comprehensive and scalable approach to address the complex security needs of smart cities, providing synergies that enhance data integrity, real-time monitoring, and privacy protection. These approaches are crucial for overcoming scalability and interoperability challenges, thus ensuring the security and resilience of smart city ecosystems. This survey provides a roadmap for building secure, scalable, and trustworthy smart city infrastructures that promote long-term sustainability and growth by synthesising theoretical insights with real-world case studies and practical applications.

1.2 | Existing Surveys

In recent years, surveys have individually addressed AAA security concerns (Authentication, Authorisation, and Access Control) for various applications [24, 25]. These surveys generally examine various technological solutions and approaches designed to address the complex security challenges associated with the scope and complexity of smart cities. However, our survey presents a comprehensive review of AAA security concerns by collectively considering factors such as trust, privacy, and scalability in the context of smart city services. This is done in light of diverse technologies, including

Blockchain, machine learning, quantum computing, and hybrid approaches. Furthermore, we provide a detailed technological taxonomy to categorise existing solutions across three primary domains of smart city applications: smart homes, smart healthcare, and intelligent transportation. We provide a comprehensive technological taxonomy to organise existing solutions in three primary domains of smart city applications: transportation, healthcare, and smart homes. Figure 2 gives a more detailed view of the taxonomy adopted in this study, showing how these technologies can be applied to solve AAA challenges in smart cities efficiently. Our taxonomy allows for the classification and analysis of various technological solutions used to improve security in such areas, specifically focusing on improving AAA security procedures. Table 1 presents a comparative analysis of existing research surveys, emphasising how the core characteristics Confidentiality, Integrity, Availability (CIA), trust, privacy, and scalability contribute to achieving comprehensive AAA security solutions across distinct domains, particularly in smart home, smart healthcare and ITS. This comparison highlights the strengths and limitations of current methodologies, offering a deeper insight into each sector's challenges within the evolving landscape of smart city environments. Furthermore, the subsequent section elaborates on how these critical factors, CIA, trust, privacy, and scalability, are interconnected and foundational to the design of robust AAA mechanisms. By mapping these relationships, our study clarifies how integrated security solutions can be effectively implemented in smart cities. Importantly, the novelty of our survey lies in its integrated focus on AAA security within the context of four core technological adaptation domains in smart city applications: smart healthcare, intelligent transportation systems (ITS) and smart homes. The literature reveals that no existing survey offers a cross-domain perspective while aligning AAA with CIA, trust, privacy and scalability across these critical sectors. Below is the detail of these factors.

CIA triad: The CIA triad encapsulates the essence of information security, which involves keeping data confidential (i.e., not accessible to unauthorised parties), ensuring its integrity (i.e., it is not altered), and maintaining its availability (i.e., accessible to authorised users when they need it) [36]. These three information security attributes are necessary to form an efficient AAA security solution. Smart city platforms heavily rely on secure AAA mechanisms to keep private data safe, particularly in healthcare systems. OAuth 2.0 and Multi-Factor Authentication (MFA) are crucial authentication methods since they guarantee that only authorised healthcare professionals can view private patient information. Additional processes, such as role-based access control (RBAC), ensure the safe maintenance of patient data; only authorised medical professionals can alter treatment regimens [37]. These systems guard all degrees of access to vital medical records. When combined, they provide a powerful AAA response.

Trust factor: In smart city applications, where data is shared among multiple stakeholders, including citizens, enterprises, and government agencies, any AAA security system must be predicated on trust. Individuals who have confidence in a

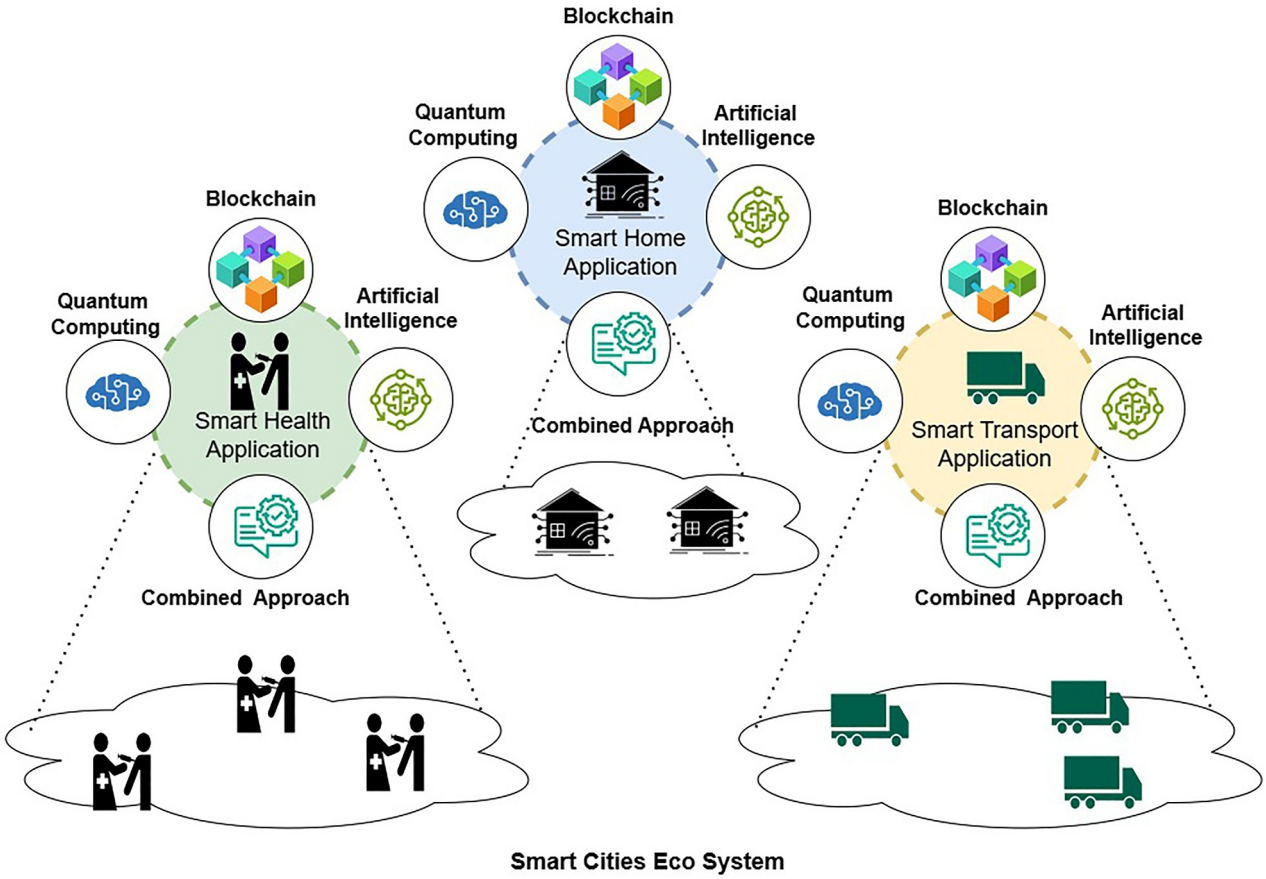

FIGURE 2 | Proposed interaction of technologies for smart city applications.

TABLE 1 | A comparison of existing surveys.

Existing survey	Year	CIA triads	Privacy	Trust	Scalability	Domains	Technological adaptations
Gharaibeh et al. [26]	2017	✓	✗	✓	✓	Smart home, ITS	AI, blockchain
Hwang et al. [27]	2017	✓	✗	✓	✓	ITS, smart home	Quantum computing
Samaila et al. [28]	2018	✓	✓	✓	✗	Smart home, smart healthcare, ITS	Blockchain
Talal et al. [29]	2019	✓	✓	✗	✗	Smart home, smart healthcare	AI
Algarni et al. [30]	2020	✓	✓	✗	✗	Smart healthcare	Blockchain
Rahman et al. [31]	2021	✓	✓	✓	✗	Smart healthcare	AI, blockchain
Alamri et al. [32]	2022	✓	✓	✗	✗	Smart healthcare	Blockchain
Alhaj et al. [33]	2022	✓	✓	✗	✗	Smart healthcare, IoMT	Blockchain
Kamalov et al. [24]	2023	✓	✓	✗	✗	Smart healthcare	Blockchain
Bashirpour et al. [25]	2023	✓	✗	✓	✗	ITS	AI, blockchain, quantum computing
Rajkumar et al. [34]	2024	✓	✗	✗	✓	Smart home, ITS	Quantum computing, AI
Alzu et al. [35]	2024	✓	✓	✓	✗	Smart healthcare	AI
Our survey	2025	✓	✓	✓	✓	Smart home, smart healthcare, ITS	Blockchain, AI, quantum computing

system know that its security mechanisms will safeguard private data and maintain its integrity. Urban smart environments, such as those in healthcare and intelligent transport systems, foster trust by utilising secure authentication methods, open authorisation frameworks, and standardised access control measures [38]. By limiting service access solely to authorised users, authentication protocols like OAuth 2.0, combined with digital certificates, reinforce confidence and ensure the continuous operation of systems. In addition, trusted computing solutions such as Trusted Platform Modules (TPM) offer secure execution by validating hardware and software integrity.

Privacy factor: Privacy in smart city applications is crucial because personal and organisationally sensitive data is shared among various systems. To maintain privacy in AAA security solutions, the authentication and authorisation process must be carried out very carefully so that only those with proper justification to view or modify the data are granted access. For instance, differential privacy algorithms can be applied to anonymise individual data within a large dataset so that accessing the data doesn't compromise the privacy of individuals. Similarly, through privacy-enhancing technologies (PETs) like secure multiparty computation (SMC), one will have the ability to process data in a way that would not expose raw data and hence protect privacy during computation [39]. Moreover, robust authentication protocols such as OpenID Connect empower individuals to manage who can access their data. In contrast, role-based access control (RBAC) guarantees users are restricted to information pertinent to their specific roles [37, 40]. These techniques and mechanisms are integrated into the AAA framework to safeguard user privacy by regulating data access, processing, and storage within the smart city environment.

Scalability factor: Smart city infrastructures involve numerous users and devices across diverse fields such as transportation, healthcare, and public services, posing a significant challenge in implementing AAA security measures that are suitable for every form of application. AAA solution must be capable of expanding without compromising security or efficiency to integrate tools, clients, and transactions. SAML (Security Assertion Markup Language) and OAuth 2.0 are scalable protocols that facilitate the dispersion of authentication and permission management in distributed systems, meeting the growing user base and system demand. Load balancing techniques are advantageous for large-scale systems, ensuring that authentication requests are distributed equitably among all sites [41]. This avoids congestion and guarantees uninterrupted operations. Due to their adaptable infrastructure and rigorous access limits, cloud-based identity management technologies, including Microsoft Azure Active Directory and AWS Cognito, can simultaneously administer millions of logon requests.

1.3 | Scope of This Survey and Contributions

This survey paper systematically reviewed the different security frameworks proposed for smart city ecosystems. We commented on their ability to address the challenges of authentication, authorisation, and access control. Our work aims to create a taxonomy that categorises existing solutions based on their application of advanced technologies such as Blockchain,

artificial intelligence, and quantum computing in the smart cities domain. We included studies published after 2017 and evaluated these frameworks in terms of their capability to enhance security, scalability, and operational efficiency in domains such as smart homes, smart healthcare and ITS. To this end, we performed an SLR based on Kitchenham's widely recognised methodological framework [42]. SLR is a method based on evidence in which the process defines, evaluates and analyzes all relevant evidence repetitively in an unbiased manner on focused topics or research questions. The SLR method follows a predetermined protocol, ensuring rigorous selection and elimination procedures to synthesise the study's specific findings clearly and systematically to answer the research questions. The main contributions of this survey are as follows:

1. An SLR is conducted that provides a comprehensive review of advanced technologies that address security challenges in smart city ecosystems.
2. A tailored taxonomy categorises these solutions across three major domains: smart homes, smart healthcare, and intelligent transport systems (ITS).
3. A set of critical research gaps is identified, highlighting immediate needs for improving security frameworks in smart city ecosystems.
4. Emerging challenges and opportunities are outlined, offering a roadmap for future research to enhance these systems' scalability, cost-efficiency, and security.

In this research, a bibliometric and conceptual study of the literature published in peer-reviewed journals was conducted on smart cities, focusing on security challenges and innovative solutions. The selection of relevant journals and articles was guided by Kitchenham's theory, which emphasises systematic evaluation of sources based on their relevance, reliability, and contribution to the research domain [42]. The study aims to understand the development of academic thought and practical approaches related to authentication, authorisation, and access control in the context of smart city ecosystems. The remainder of this paper is structured as follows: Section 2 outlines the research methodology, including the systematic literature review (SLR) process, the formulation of research questions, and paper selection techniques like snowballing. It also details the data analysis methods and presents a mathematical framework for evaluating the adaptation levels of emerging technologies Blockchain, Artificial Intelligence (AI), Quantum Computing, and hybrid approach within the context of smart city security. These technologies are categorised into four adaptation levels; Low, Medium, High and High (Future); based on factors such as scalability, trust, privacy, and alignment with the CIA triad. This framework provides a structured approach for assessing the maturity and practical applicability of these technologies in real-world smart city environments. Section 3 provides a comprehensive domain-specific analysis of AAA security solutions in three key smart city domains: smart homes, smart healthcare, and intelligent transportation systems (ITS). It evaluates the impact of technological adaptations including Blockchain's immutable authorisation mechanisms, AI-driven identity verification, quantum-resistant cryptography, and hybrid approaches on enhancing AAA mechanisms. Section 4 presents a cross-domain comparative analysis and examines the practical applicability of the reviewed technologies. Using the Technology Adaptation Levels framework from Section 2, this section evaluates Blockchain, AI, Quantum Computing and hybrid models across the three domains. The adaptation scores, presented in Table 2, assess each technology's alignment with the CIA triad and AAA protocols. Based on a thorough literature review, these scores provide an in-depth evaluation of the benefits, limitations, and future directions of these technologies, offering practical insights into securing smart city ecosystems and facilitating their effective deployment. Section 5 presents three representative case studies that demonstrate the application of these emerging technologies in smart city settings, as well as future research directions. These case studies include:

- Blockchain-based framework for healthcare data management, focusing on patient-centric control and secure data sharing.
- A hybrid Quantum-Blockchain-6G (QBG) model for intelligent urban infrastructure, combining the processing power of quantum computing with the data integrity of Blockchain.
- An AI-enhanced dynamic authentication mechanism for the Internet of medical things (IoMT), capable of real-time adaptation based on health data sensitivity.

These case studies showcase the potential for integrating these technologies, highlight future research opportunities, and discuss challenges such as limitations in edge devices, quantum threats to existing encryption standards, and regulatory hurdles in diverse smart city environments. Section 6 concludes the paper by synthesising key insights and emphasising the need for comprehensive, multi-technology AAA frameworks that combine Blockchain's decentralised trust models, AI's adaptive intelligence, and Quantum Computing's cryptographic resilience. This convergence is essential for meeting the growing demands of secure, scalable, and intelligent urban systems.

2 | Systematic Literature Review

A systematic review of the literature (SLR) is a thorough search of the present literature that helps to compile what is now known, identify knowledge gaps and provide a basis for future research endeavours. A systematic literature review must evaluate sources based on their relevance, reliability, and impact in the research field. Kitchenham's framework provides a systematic selection method for identifying relevant and reliable articles for reviews [42].

Using SLR, this research highlighted major academic work, conference contributions, and peer-reviewed journal articles concerning the possibility of utilising new emerging technologies such as Blockchain, artificial intelligence, and quantum computing to enhance the security of smart cities. This framework guided the literature review to resources that examine the technological aspects of smart city ecosystems, which can be valuable recommendations to improve access control, authorisation, and authentication systems. Consequently, the SLR

TABLE 2 | Consolidated technology adaptation scores across domains (CIA, AAA, trust, privacy, scalability).

Technology	Smart home	Smart healthcare	ITS	Overall adaptation
Blockchain	*High* Nasonov et al. [43] Lin et al. [21] Qashlan et al. [22] Awan et al. [38] Tchagna et al. [44]	*Medium* Tripathi et al. [45] Rahman et al. [46] Mallick et al. [47] Rouzbahani et al. [48] Rani et al. [49]	*High* Wazid et al. [50] Qureshi et al. [51] Alkhalifa et al. [52] Hao et al. [53] Badshah et al. [54]	*High*
AI	*Medium* Al-Mtawa et al. [55] Majumder et al. [56] Shahjalal et al. [57]	*High* Li et al. [58] Liu et al. [59] Wang et al. [60] Kulurkar et al. [61] Habbal et al. [62]	*High* Kaushik et al. [63] Alam et al. [64] Xu et al. [65]	*High*
Quantum computing	*Low* Chaudhary et al. [19] Shahid et al. [66] Alomari et al. [67]	*Medium* Janani et al. [68] Ju et al. [69] Kalaivani et al. [70]	*Medium* Mohanty et al. [71] Jagirdar et al. [72] Sutradhar et al. [73] Qu et al. [74]	*Medium*
Hybrid approaches	*High (future)* Khan et al. [75] Farooq et al. [76] Raza et al. [77] Shahbazi et al. [78]	*High (future)* Tagade et al. [79] Shuaib et al. [80] Marridi et al. [81] Patel et al. [82]	*High (future)* Saleem et al. [83] Gupta et al. [84] Vaidyan et al. [85] Liu et al. [86] Nguyen et al. [87]	*High (future)*

comprehensively covers the entire range and complexity of academic discussions on this critical topic.

2.1 | Systematic Review Methodology

The initial phase of the methodology included developing specific research questions to guide the review process. This investigation concentrated particularly on authentication, authorisation, and access control, intending to explore the application of modern developments in smart city technologies to address security issues. Subsequently, the search terms were determined to gather the pertinent literature.

We used the following equation to form search strings and find related articles and surveys that answered the research questions.

$$B_{ij} = \{\alpha \| \beta \| \gamma \| \Gamma\} \tag{1}$$

$$i = \{\text{Blockchain},\ \text{Artificial Intelligence},\ \text{Quantum Computing}\}$$

$$j = \{\text{Smart Home},\ \text{Smart Healthcare},\ \text{Smart Transport}\}$$

In this equation, the terms α, β, γ, and Γ represent critical attributes related to the AAA framework, which are essential in ensuring secure and efficient smart city operations:

α: This represents the Confidentiality, Integrity, and Availability (CIA) triad, which forms the foundation of security in any information system. The CIA triad ensures that the data remains confidential (only accessible to authorised users), intact (not tampered with), and available (accessible when needed). These principles are fundamental in implementing AAA mechanisms for smart city systems, safeguarding critical data such as personal information, health records, or transportation data.

β: This represents Scalability, which refers to the ability of a system to handle an increasing number of users, devices, or data without compromising performance. Scalability is critical in smart city environments, where systems must accommodate many connected devices and users while maintaining optimal performance. In the context of AAA, scalability ensures that authentication, authorisation, and access control mechanisms remain effective as the smart city expands.

γ: This symbolises Privacy, a critical issue within smart cities, particularly about personal data management. Privacy within AAA frameworks guarantees that sensitive details, including medical records or personal transit data, are accessible solely to authorised parties, thereby maintaining individuals' confidentiality and privacy. Technologies that improve privacy, such as encryption or anonymisation, play a vital role in protecting personal data in a highly interconnected environment.

Γ: This signifies Trust, a crucial factor for effective deployment of any smart city solution. Establishing trust involves ensuring that systems remain secure, reliable, and transparent, along with providing users with explicit means to verify the integrity of the service. In the context of AAA, trust is facilitated by secure authentication and authorisation processes, which

ensure that users can rely on the system to protect their data and maintain system integrity. This also involves using trusted technologies, such as Blockchain, which can offer decentralised trust mechanisms in smart city applications.

This equation allows us to systematically generate combinations of these critical attributes (α, β, γ, and Γ) with relevant technological solutions (Blockchain, AI, Quantum Computing) and application domains (Smart Home, Smart Transport, Healthcare) to identify pertinent literature that addresses these intersections. After the search strings were formed, the literature was retrieved from various academic databases, including IEEE Xplore, Springer, and Elsevier. The relevance of each article was then evaluated based on several criteria, including the quality of the research, the methods used, and its contributions to addressing the security challenges in smart cities. Articles that met the inclusion criteria were subjected to further analysis to extract key findings, trends, and gaps in the research.

2.2 | Reserach Questions

We have developed a series of focused research questions to methodically investigate the effects on AAA (authentication, authorisation, and access control) security mechanisms in smart cities using modern technologies, including Blockchain, artificial intelligence (AI), and quantum computing. Different questions seek to enable the analysis of how various technologies address the security concerns of the AAA process in smart city applications, particularly by considering CIA, trust, privacy, and scalability features within AAA solutions.

Below is a list of research questions developed to explore the application and impact of modern technologies on smart cities' AAA (Authentication, Authorisation, and Access Control) security mechanisms. Each question is accompanied by an explanation of its intention and expected outcomes:

2.2.1 | R1-What Are the Current Technological Solutions Employed for Enhancing AAA Security Mechanisms in Smart Cities?

This question seeks to classify several technologies, such as Blockchain, Artificial Intelligence, and Quantum Computing, now used to handle AAA security concerns in smart city systems. It aims to find how smart homes, transportation, and healthcare, among other fields, use these technologies to enhance authentication, authorisation, and access control systems.

2.2.2 | R2-How Do Advanced Technologies Such as Blockchain, AI, and Quantum Computing Impact the CIA Triad, Trust, Privacy, and Scalability in AAA Security Solutions?

This question investigates the contributions of modern technologies to the core attributes of AAA security, such as Confidentiality, Integrity and Availability (CIA), as well as trust, privacy, and scalability. It focuses on how these technologies address traditional security challenges while enhancing AAA mechanisms in smart city ecosystems.

2.2.3 | R3-What Are the Challenges and Limitations Associated With Implementing AAA Security Solutions in the Context of Smart City Applications?

This question aims to identify the obstacles and limitations faced during the deployment of AAA mechanisms in smart city environments. The question considers issues such as system complexity, resource constraints, operational costs, latency, and integration difficulties with existing infrastructure.

2.3 | Procedure for Selection of Studies

This section describes the inclusion and exclusion criteria used to assess the validity of the primary selected articles. The selected article should be in English and published between 2017 and 2024 in a reputable ISI-indexed scientific journal or a top-notch conference proceeding. The primary study should pass the following three-phase selection and evaluation process.

1. *Phase-1*: An article will only be evaluated for the next step if it addresses AAA security concerns, as defined by analysing factors such as the CIA triad, Trust, Privacy, and Scalability, and falls within the Smart Cities area. Smart cities should also include smart homes, smart healthcare, and intelligent transportation.
2. *Phase-2*: In this phase, from the articles selected in Phase 1, further investigation is carried out to look for explanations of AAA solutions concerning Scalability, Trust, Privacy and the CIA triad (Confidentiality, Integrity, Availability).
3. *Phase-3*: Selected paper screening is finalised, and an article is removed unless it follows the following content requirements.

2.4 | Systematic Review Execution

The systematic literature review for this study started on August 15, 2024, with the search for high-quality research articles published between 2017 and 2024. 255 research papers were initially retrieved from various digital libraries such as IEEE, Science Direct, ACM, Springer, and Scopus, using specific search strings based on the above mentioned methodology. The review then went through a rigorous multiphase selection process as follows:

2.4.1 | Phase 1: Inclusion/Exclusion Criteria

In the first screening phase, all retrieved articles were selected according to their abstracts, conclusions, and relevance to the predefined research questions. In this phase, all studies that address AAA security concerns of authentication, authorisation, and access control in smart city ecosystems are sought. In this first round, 96 papers were rejected, and 159 papers were allowed to progress to the next stage.

2.4.2 | Phase 2: Screening of Title and Keywords

In the second stage, the titles and keywords of the remaining articles were carefully analysed to select those that focused on explicit advanced technological solutions such as Blockchain, artificial intelligence, and quantum computing in smart homes, smart healthcare, and ITS. This process excluded an additional 60 papers, leaving 99 papers for the next round.

2.4.3 | Phase 3: Abstract Analysis

Abstracts for selected articles were exhaustively reviewed in the third stage to evaluate their contribution to solving AAA-related security challenges in terms of CIA, scalability, privacy, and trust. As a result of this evaluation, 34 more papers were excluded from the pool in this round, making the pool 65 papers strong.

2.4.4 | Final Phase: Full-Text Screening and Snowballing

In the final phase, a comprehensive review of the full texts of selected papers was performed. Articles that did not meet the quality requirements or provide sufficient evidence regarding the research questions raised were excluded. Furthermore, using the forward and backward snowballing techniques yielded another 18 articles for this sample. Therefore, 83 articles were selected to form the basis of this research study.

Table 3 summarises the detailed paper selection process. The complete procedure from initial selection to full text selection is outlined in Figure 3. The systematic approach ensured a rigorous literature evaluation based on research questions. Metadata forms have been prepared to categorise the gathered studies and accumulate relevant information, including their publication year, keywords, authors, name of the journal/conference, type of research, and application of technologies in AAA frameworks. Most of the resulting articles were published between 2017 and 2024, indicating a growing interest in protecting smart city ecosystems with advanced technologies, as shown in Figure 4. This process formed the basis for the taxonomy-based classification of solutions and research gaps presented in the following sections.

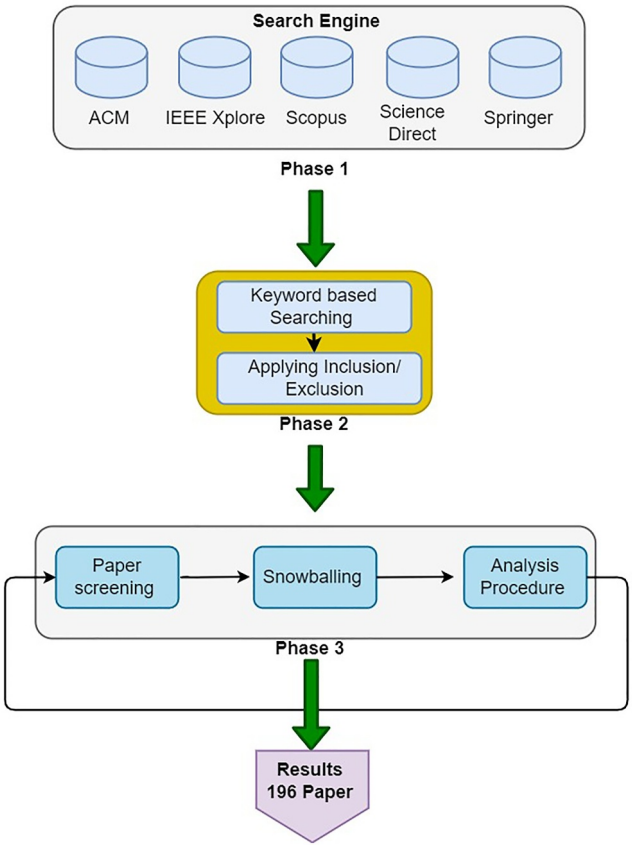

FIGURE 3 | Search and selection process.

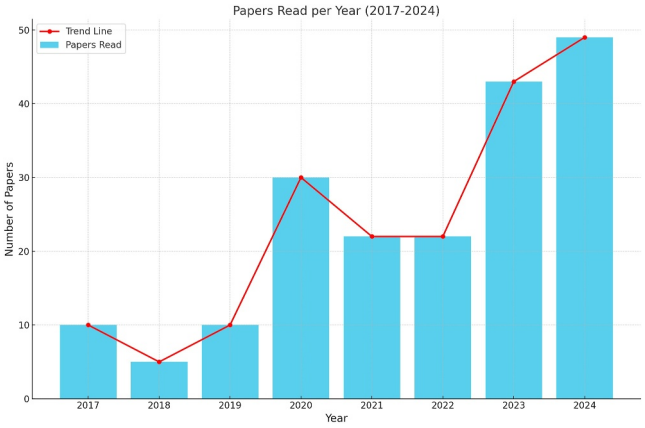

FIGURE 4 | Year-wise distribution of selected papers.

TABLE 3 | Paper selection process during different phases.

Digital library	Initial selection	Inclusion/exclusion criteria	Title and keywords	Abstract	Forward and backward snowballing	Full-text selection
IEEE	50	−15	−10	−05	+03	23
Science direct	45	−17	−15	−05	+07	15
ACM	30	−15	−06	−03	+02	08
Springer	60	−19	−18	−07	+03	19
Scopus	70	−30	−11	−14	+03	18
Total	255	−96	−60	−34	+18	= 83

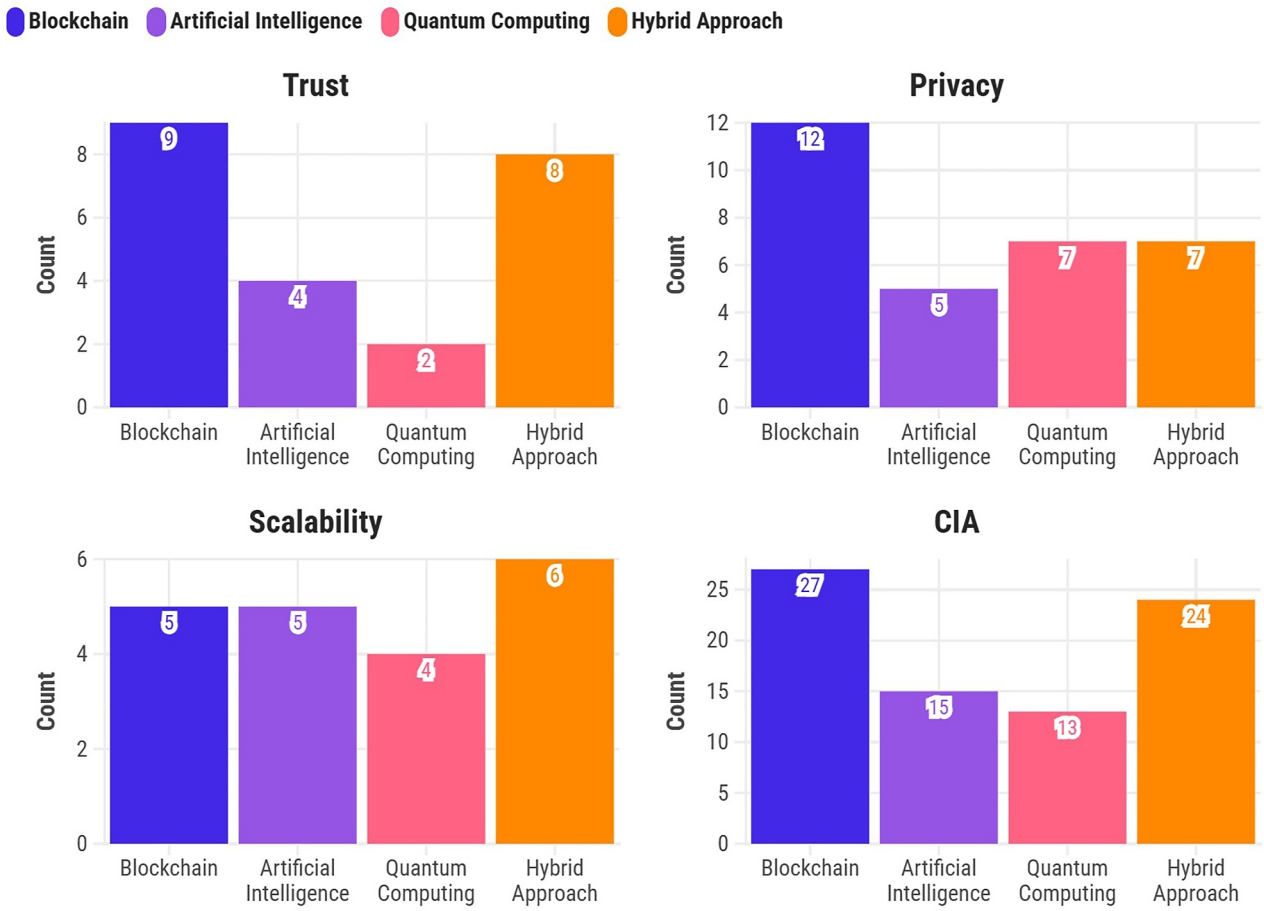

FIGURE 5 | Distribution of articles across technologies addressing AAA challenges in smart cities. Technologies include blockchain, AI, quantum computing, and hybrid approaches focusing on trust, privacy, scalability, and the CIA triad.

This survey emphasises the solutions developed to address the AAA issue of smart cities, including scalability, privacy, security, and trust. Smart cities are substantially dependent on networked technologies, essential domains for providing optimal services to citizens, preserving system integrity, and protecting private information. Our research investigates existing solutions in three fundamental domains of smart cities, such as healthcare, smart homes, and ITS. To address the AAA challenges in smart cities, the bar chart presented in Figure 5 provides a clear comparison of how various technologies such as Blockchain, AI, quantum computing, and hybrid approaches contribute to solving issues related to Trust, Privacy, Scalability, and the CIA triad (Confidentiality, Integrity and Availability). Based on a comprehensive review of current literature, this analysis highlights the number of publications associated with each technology within these key security domains. The chart effectively visualises the significance of each technology in tackling the AAA challenges, illustrating the distribution of research across these technologies and their respective areas of impact.

2.5 | Technology Adaptation Levels and Applicability in Smart City Security Solutions

In this survey, we propose a mathematical framework to evaluate the technology adaptation levels within the context of smart city security solutions, specifically focusing on AAA mechanisms. Through a systematic analysis of existing literature, we categorise the applicability of technologies such as Blockchain, artificial intelligence (AI), quantum computing and hybrid approaches into four levels: low, medium, high, and high (future). These categories reflect the extent to which each technology addresses the security challenges in smart cities, specifically in the AAA domain:

Low: Technologies labelled as 'low' exhibit significant limitations or inefficiencies in addressing the required security and scalability criteria in smart city systems. These technologies may have minimal applicability or face severe constraints in current implementations, hindering their adoption in real-world environments.

Medium: A 'medium' rating indicates that the technology partially addresses the security and scalability criteria but requires significant improvements to achieve widespread adoption. These technologies show promise but are still evolving, often lacking robustness or scalability for large-scale deployment in smart cities.

High: 'High' adaptation refers to technologies that effectively and robustly address the security and scalability requirements in current applications. These technologies are widely applicable and have demonstrated strong performance in solving AAA-

related issues, making them highly relevant for deployment in smart city ecosystems.

High (Future): Technologies categorised as 'high (future)' are in early stages of development or are theoretical but have strong future potential to address emerging security challenges. These technologies promise to overcome current limitations but are not yet fully deployable or mature for large-scale use in smart cities.

To quantify the technology adaptation level for each selected article, we define a technology adaptation score T_i as follows:

$$T_i = \begin{cases} 0, & \text{if low adaptation} \\ 1, & \text{if medium adaptation} \\ 2, & \text{if high adaptation} \\ 3, & \text{if high (future) adaptation} \end{cases}$$

where i represents the article index. The total technology adaptation score S for all articles is calculated as:

$$S = \sum_{i=1}^{n} T_i$$

This formulation provides a systematic approach to categorise and quantify the applicability of various technologies in addressing the AAA challenges within smart cities. By classifying the literature in this way, we aim to identify current trends, gaps, and future research opportunities in smart city security.

In the next section, we will address contemporary solutions within the context of smart cities using the previously mentioned taxonomy. This will primarily focus on smart home, intelligent transportation, and smart healthcare. Each domain will be thoroughly studied to demonstrate how cutting-edge technologies such as Blockchain, artificial intelligence, quantum computing, and hybrid approaches are being used to address critical concerns such as trust, privacy, scalability, and the CIA triad. Using the taxonomy, we will thoroughly analyse how these technologies transform security for AAA processes in smart city applications.

3 | Domain-Specific Analysis of Emerging Technologies in Smart Cities

This section comprehensively analyzes the different trust frameworks and mechanisms used in smart cities. This discussion highlights the advantages and shortcomings of these frameworks, identifying deficiencies that future studies must address to develop more resilient, secure, scalable, and adaptable trust management systems.

3.1 | Smart Home

Integrating intelligent and automated systems improves living standards in a smart home ecosystem. Smart devices such as thermostats, environmentally friendly appliances and state-of-the-art security systems enhance comfort and safety. However, these technological advances present considerable security challenges. It is crucial to secure the communication between these devices and the broader urban network to prevent unauthorised access and data breaches that might erode trust in these technologies.

3.1.1 | Blockchain-Enabled Smart Home

Blockchain Technology (BT) plays a pivotal role in enhancing smart homes' security, privacy, and reliability and is a key component within the broad smart city infrastructure. Its robust, decentralised and temper-resistant architecture enables scalable methods for safely exchanging data and communications between interconnected devices. Such systems are essential for creating long-lasting, reliable smart homes in complex urban environments.

Recent studies stress that Blockchain should be integrated into the smart home system to ensure higher security, privacy, trust, and scalability. According to Xue et al. [88], Blockchain facilitates trust through transparent data exchange and powerful access control features. Xue demonstrates this by using examples of Blockchain to ensure increased efficiency while maintaining privacy and integrity in a smart home context. Xue introduces a permissioned Blockchain framework for access management, thus locking out unauthorised access and preserving users' privacy. All these findings underscore Blockchain's role in developing trust and security in smart homes.

Building upon these ideas, the zero trust access control framework, drawing from the attribute-based strategy outlined in Ref. [38], integrates Blockchain with adaptive policies and behaviour monitoring. This approach upholds the CIA triad by persistently tracking user and device actions, reinforcing authentication, authorisation, and access control (AAA). The Interplanetary File System (IPFS) further improves data privacy and scalability by utilising decentralised storage, thus fostering secure and efficient data management in smart homes.

The encryption methods presented by She et al. [39] enable computations directly on encrypted information, preserving its confidentiality without decrypting it and enhancing privacy. These designs, focused on Blockchain technology, support secure operations and efficient access control, thereby reducing the risk of privacy violations.

The works by Arif et al. [20] examine the potential of Blockchain to bolster security and trust. Arif suggests a consortium Blockchain designed for smart homes to create a secure, tamper-resistant system that ensures data integrity. Similarly, authentication and access control solutions are focused on developing in smart home contexts in [21, 22]. Lin et al. [21] develop the HomeChain framework that incorporates Blockchain technology, group signatures, and message authentication codes to provide mutual authentication securely. Similarly, Qashlan et al. [22] leverages edge computing and Ethereum smart contracts to secure user-device systems by using differential privacy techniques to enhance system scalability.

Tchagna et al. [44] and Nasonov et al. [43] apply Blockchain to protect IoT data in smart homes. Tchagna uses the EOS Blockchain to secure data exchanges in large-scale smart home systems. On the other hand, Nasonov et al. introduces a distributed big data platform to create a digital data marketplace. Their Integrity Manager module ensures data accuracy, consistency, and privacy, facilitating reliable data transactions. All of these works explain how Blockchain technology, with its sophisticated cryptographic approach, can be used to support the CIA triad mechanisms and AAA in the smart home ecosystem. With Blockchain combined with advanced encryption techniques and privacy-preserving frameworks, all of these works underscore the fact that it is a fundamental technology that will provide the strength for security, privacy, trust, and scalability in smart cities.

3.1.2 | Smart Home With AI

Artificial Intelligence (AI) is increasingly integral to smart homes, improving comfort and addressing key security, privacy, trust, and scalability challenges. AI supports the CIA triad, Confidentiality, Integrity, and Availability, by enabling real-time monitoring, adaptive behaviour, and secure resource management. In addition, it improves authentication, authorisation, and access control (AAA) by employing machine learning and deep learning techniques, thereby ensuring robust user verification and access management. This advancement contributes to the increased security, scalability, and adaptability of smart homes in the context of smart city applications.

The development of AI is significantly increasing the system's adaptability and strengthening the security protocols. Majumder et al. [56] integrate AI with motion and facial recognition technologies to notify the users promptly, thus augmenting confidentiality and integrity and strengthening AAA frameworks. Research by Taiwo et al. [89] and Shahjalal et al. [57] explores complex applications of AI within the smart home security context. Taiwo uses Convolutional Neural Networks (CNNs) for movement analysis to detect intrusions, markedly improving access control and safeguarding data confidentiality and integrity. In contrast, Shahjalal combines LoRa technology with AI to enhance communicative capabilities, thereby increasing system availability, operational efficiency, and cybersecurity while upholding privacy and trust.

The significance of AI-driven methods for privacy protection is highlighted by Rahim et al. [90]. Rahim introduces a CNN model enhanced with Logit-Boost to improve anomaly detection and facilitate real-time facial recognition, tackling the issues of scalability and resource requirements. Furthermore, Furtado et al. [91] explore the effects of Generative AI (GAI) on smart home systems, demonstrating its role in creating adaptable, secure, and scalable urban solutions. Al Mtawa et al. [55] stress using machine learning techniques to detect DDoS attacks to increase the security resilience of smart home networks.

These studies underscore artificial intelligence's potential to enhance intelligent residential systems' security, privacy, reliability, and scalability. The methods assessed support the CIA triad and the AAA protocols vital for access control, employing AI algorithms and machine learning techniques within smart home environments.

3.1.3 | Smart Home With Quantum Computing

Quantum computing holds great promise for revolutionising smart home systems, dealing with key security, privacy, trust, and scalability issues. QC increases the efficacy of encryption, strengthens privacy protocols, and enhances communication security. Thus, QC offers the robust protection required against emerging cyber threats. Inclusion of quantum algorithms in cryptographic frameworks optimises data processing and protects user privacy. This integration further enhances the CIA and extends the AAA framework to deliver adaptive and scalable security solutions in response to emerging threats.

The research conducted by Shahid et al. [66] investigates a 'post-quantum distributed ledger for the Internet of things', implementing the DL-OTS mechanism, which is known for its robustness against quantum threats. This strategy effectively decreases the size of signatures and reduces computational expenses in one-time signatures, thus being particularly adept for IoT resources in smart home settings. The system enhances transaction validation by ensuring data integrity and availability, following the CIA triad, thereby increasing the efficiency of IoT applications. Moreover, the pruning method considerably improves ledger scalability, vital for sustaining secure and adaptable smart home environments. Simultaneously, Rajat et al. [19] evaluate the lattice-based public-key cryptosystems (LB-PKC) against the ransomware and man-in-the-middle attacks in smart homes. Their findings stress the need for effective cryptographic mechanisms to secure data communication and devices in smart home settings. LB-PKC is used to implement robust AAA functionalities while addressing challenges associated with privacy, trust, and scalability, and hence enhancing the CIA framework.

Alomari et al. [67] investigate the security challenges that quantum computing introduces to IoT systems, focusing on smart home environments. They underscore vulnerabilities such as weak encryption and embedded passwords, which quantum attacks could exploit to undermine data security. This research promotes quantum-resilient cryptographic solutions, postulates the use of quantum machine learning for detection and prediction of quantum security threats, enhances smart home security measures and privacy, thus building confidence in smart home technologies, and initiates large-scale research projects into understanding how quantum computing can add strength and resilience to smart homes. This will address present-day vulnerabilities and implement progressive cryptographic and security solutions. These strategies support the CIA triad and integrate AAA models, especially Authentication, Authorisation, and Access Control. This approach is helpful in scaling, ensuring privacy, and building trust, thus creating secure environments for smart homes against the challenges of quantum computing.

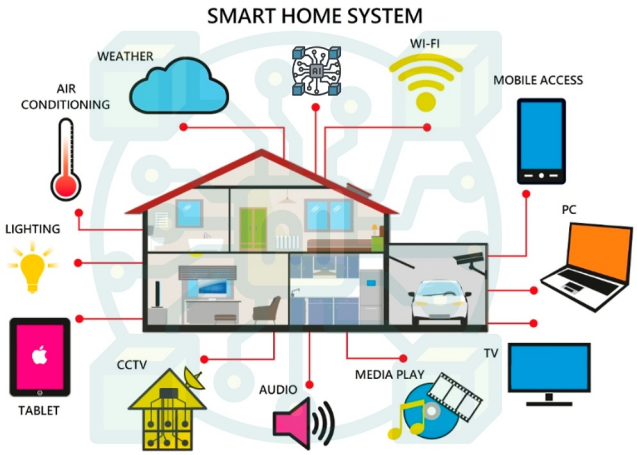

FIGURE 6 | Smart Home enabled by blockchain and AI.

3.1.4 | Smart Home With Hybrid Approach

Integrating Blockchain technology, artificial intelligence and quantum computing into smart home systems transforms all key aspects such as security, privacy, trust, and scalability, while highlighting their inevitable role in developing smart city designs. This broad approach increases the collaborative progress in security frameworks on the core issues within the smart home environment. Figure 6 illustrates a brief overview of a smart home ecosystem.

Considering the integration of technologies, the studies conducted by Khan et al. [75] and Shahbazi et al. [78] highlight the critical benefits derived from the integration of Blockchain technology with AI to improve the security of the smart home. Khan suggests a sophisticated Blockchain approach integrated with machine learning to secure data transmission, ensuring compliance with confidentiality, integrity, and availability (CIA) standards. Shahbazi combines Blockchain with deep reinforcement learning to identify fraudulent activities through AI-driven processing of IoT sensor data, thus enhancing user confidence.

Comprehensive analyses by Raza et al. [77] and Farooq et al. [76] explore the confluence of artificial intelligence and Blockchain technology. Raza presented a specialised private Blockchain platform incorporating AI to identify anomalies, improving secure monitoring of user activities and device management, eventually optimising authentication processes and scalability. Simultaneously, Farooq designed a private Blockchain framework that includes machine learning for intrusion detection, ensuring the authenticity of communication while maintaining CIA, along with AAA protocols.

These research studies demonstrate the valuable potential of combining Blockchain, AI, and quantum technologies to solve the complex security, privacy, trust, and scalability issues of the smart home. Table 4 provide a summary of the literature on technologies related to smart homes and an overview of Blockchain, AI, quantum computing and hybrid approaches in smart home security respectively. Their results focus on an integrated approach that aligns with robust, scalable, and future-ready home environments using CIA and AAA principles. Likewise, Figure 7 presents the number of papers addressing the challenges in Smart Home with respect to security, privacy, scalability, and trust, grouped by emerging technologies like Blockchain, AI, Quantum Computing, and Hybrid approach.

3.2 | Smart Healthcare

Smart healthcare is a critical component of smart cities, and it combines the power of IoT, AI, Blockchain, and quantum computing to bring efficiency, personalisation, and security to the healthcare services offered. These technologies enable real-time data sharing, remote monitoring, and preventive care, which meet the growing needs for healthcare in urban areas. Innovation in telemedicine and wearable health devices contributes to this transformation by allowing remote consultations, continuous tracking, and predictive analysis. These developments ease the burden on conventional healthcare systems and improve patient outcomes by offering more accessible and proactive healthcare options.

Integration of these technologies has brought up security, privacy, and trust-related issues. There is a need to protect the patients' data, the communication between the devices must be secured, and AAA mechanisms must be implemented with great strength. All these necessities fall under the CIA triad. This section elaborates on how wearables, sensors, telemedicine, and real-time data analytics support smart healthcare and how robust security protocols are required to prevent data breaches and unauthorised access. Figure 8 depicts the integrated smart healthcare ecosystem, emphasising the importance of these innovations.

3.2.1 | Blockchain-Based Smart Healthcare

Blockchain technology is recognised as a transformative methodology for making smart healthcare systems more secure, focusing on privacy, trust, and scalability issues. The decentralised design and tamper-resistance of Blockchain make it a good candidate to manage sensitive health data securely and enable secure interaction among patients, healthcare providers, and devices. This section covers several Blockchain models proposed for the healthcare domain, including aspects like the CIA triad for security, privacy, scalability, and trust frameworks, while stressing the factors that AAA would strengthen the system's reliability and functionality. Proper electronic medical records (EMRs) and IoMT data management are necessary for building smart healthcare systems.

Recent studies underscore the importance of cryptographic techniques in protecting patient data within Blockchain architectures. Tripathi et al. [45] introduced the S2HS framework, which utilises cryptographic methodologies to secure electronic medical records (EMRs) and data from mobile sources, ensuring confidentiality and access management. Rahman et al. [46] introduced the Proof of Trust and Expertise (PoTE) consensus mechanism to improve the authentication and authorisation processes, focusing on the assessment of the credibility and competence of the nodes. These strategies advance trust,

TABLE 4 | Consolidated analysis of smart home technologies: Security, privacy, trust, scalability, and summary.

Technology	References	Security	Privacy	Trust	Scalability	Summary
Blockchain	Awan et al. [38]	✓	✓	✓	✗	Zero-trust framework with adaptive policies and IPFS for decentralised storage. *AAA perspective*: Robust AAA but struggles with scalability due to on-chain storage costs
Blockchain	Lin et al. [21]	✓	✓	✗	✗	HomeChain uses group signatures for mutual authentication. *AAA perspective*: Strong authentication but lacks trust mechanisms for multi-user behaviour
Blockchain	Qashlan et al. [22]	✓	✓	✗	✗	Ethereum smart contracts with differential privacy. *AAA perspective*: Effective authentication but high computational complexity limits scalability
Blockchain	Tchagna et al. [44]	✓	✗	✗	✗	EOS blockchain for IoT data integrity. *AAA perspective*: Focuses on security but lacks privacy and access control features
Blockchain	Nasonov et al. [43]	✓	✓	✓	✗	Maintain data accuracy and privacy. *AAA perspective*: Secure transactions but scalability challenges in large-scale systems
AI	Al-Mtawa et al. [55]	✓	✗	✗	✗	ML-based DDoS attack detection. *AAA perspective*: Strong security but no privacy and trust mechanisms
AI	Majumder et al. [56]	✓	✗	✗	✗	Facial recognition for authorisation. *AAA perspective*: Raises privacy concerns due to surveillance
AI	Shahjalal et al. [57]	✓	✗	✗	✓	LoRa and AI for communication efficiency. *AAA perspective*: Improves availability but lacks privacy safeguards and trust
Quantum computing	Shahid et al. [66]	✓	✗	✓	✓	Post-quantum DLT with pruning for IoT. *AAA perspective*: Quantum-resistant but energy-intensive for large deployments
Quantum computing	Chaudhary et al. [19]	✓	✗	✗	✗	Lattice-based PKC for ransomware defense. *AAA perspective*: Strong encryption but lacks privacy mechanisms
Quantum computing	Alomari et al. [67]	✓	✗	✗	✗	Quantum ML for threat detection. *AAA perspective*: Addresses quantum vulnerabilities but no privacy focus
Hybrid approach	Khan et al. [75]	✓	✗	✗	✗	Blockchain integrated with ML for data integrity. *AAA perspective*: Secure transmission but ignores scalability
Hybrid approach	Farooq et al. [76]	✓	✗	✓	✗	ML-based intrusion detection (95.28% accuracy). *AAA perspective*: Strong trust but lacks scalability strategies
Hybrid approach	Raza et al. [77]	✓	✓	✗	✗	Private blockchain integrated with AI for anomaly detection. *AAA perspective*: Limited to small-scale environments
Hybrid approach	Shahbazi et al. [78]	✓	✗	✓	✗	Blockchain integrated with deep RL for fraud detection. *AAA perspective*: Robust security but scalability challenges

maintain data integrity, and provide robust access management within healthcare systems.

The rising volume of data significantly influences scalability within the healthcare sector. Mallick et al. [47] proposed a Blockchain based fog computing system and the InterPlanetary File System to reduce latency and address some of the critical scalability issues in healthcare. Additionally, Rouzbahani et al. [48] proposed 'SCoTMan', a scalable smart contract framework that employs social IoT to enhance trust management, tackle privacy issues, and optimise Blockchain infrastructure for extensive IoT networks. Concurrently, Rani et al. [49] combined Blockchain with IPFS and AES encryption to establish secure and scalable IoT-enabled healthcare systems, thus allowing patients to manage their data.

When viewed collectively, these studies emphasise the transformative capabilities of Blockchain technology within smart healthcare. This includes data protection, privacy maintenance, trust building, and scalability. Furthermore, Blockchain provides

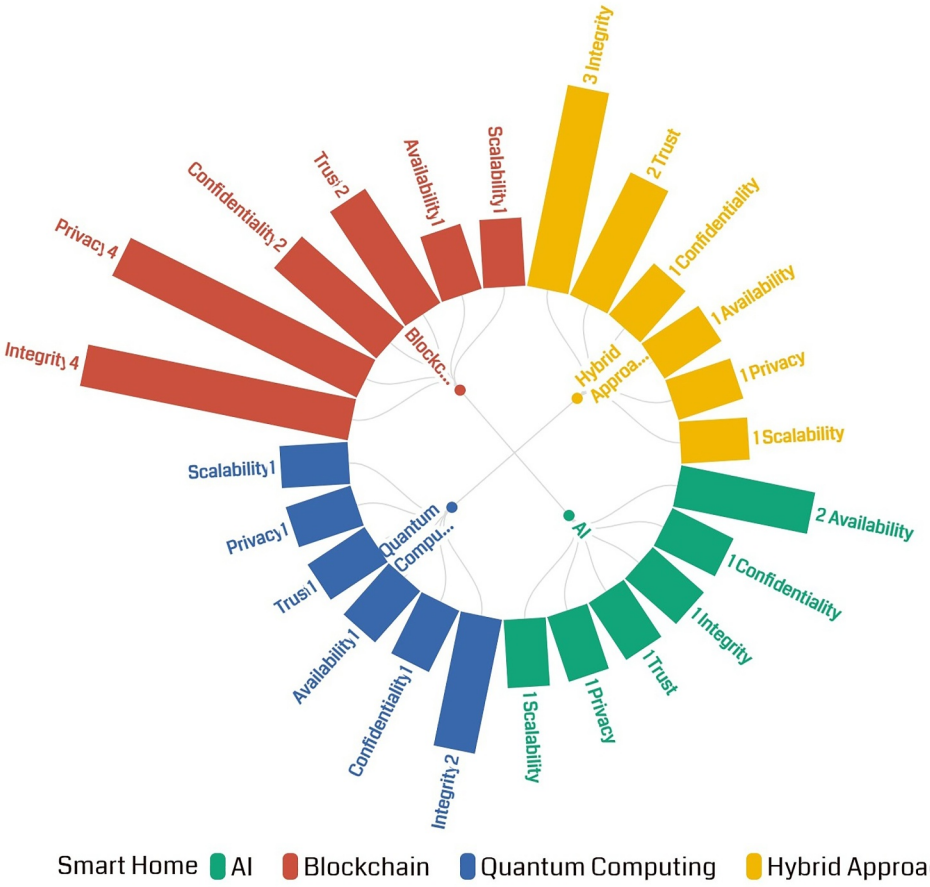

FIGURE 7 | Number of papers addressing challenges in smart home systems (security, privacy, scalability, and trust), categorised by emerging technologies (blockchain, AI, and quantum computing).

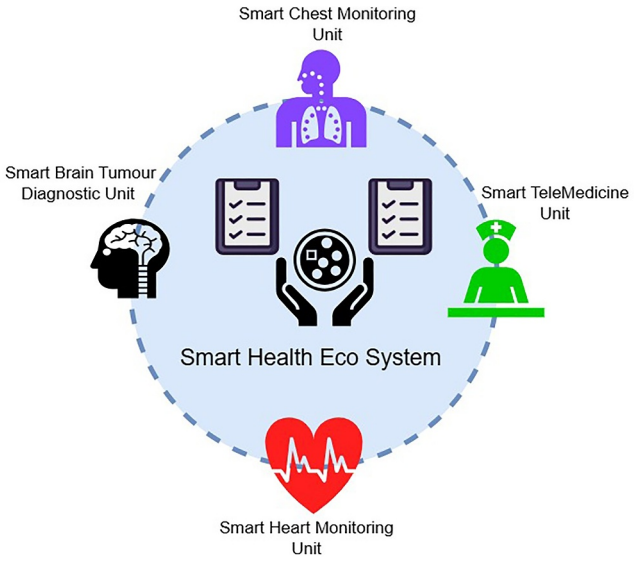

FIGURE 8 | Smart health ecosystem.

solutions to various challenges through diverse cryptographic and decentralised methods and acts as an essential platform for progressing IoMT applications.

3.2.2 | Smart Healthcare With AI

AI technologies have been instrumental in improving the efficiency, accessibility, and quality of health care services. These technologies transform healthcare systems through advanced data analytics, predictive modelling, and automated reasoning processes. This chapter focuses on AI in intelligent healthcare on security, privacy, trust, and scalability of smart city infrastructure.

Focusing on the protection of privacy in AI, Wang et al. [60] proposed the FRESH framework. This methodology improves privacy by merging federated learning with ring signatures and ensures scalability within healthcare networks, thereby enhancing user trust through data protection. Extending the Technology Acceptance Model, Liu et al. [59] incorporated the aspects of privacy and trust in AI healthcare applications, highlighting their essential role in building user confidence and customising experiences. Concurrently, Habbal et al. [62] developed the AI TRiSM framework, emphasising trust, risk, and security management. This model utilises privacy-by-design principles to enhance trust, transparency, and accountability in AI, highlighting their importance within scalable healthcare systems. According to Li et al. [58], the ETECTOR system is proposed as a novel approach for the early detection of Alzheimer's disease, utilising federated learning and differential

privacy to ensure safe data transmission, which is crucial for promoting trust in healthcare services. Kulurkar et al. [61] opted LSTM for data analysis and prediction along with cloud computing for data processing and scalability.

These studies demonstrate the transformative impact of AI and IoT technologies on the logic of smart healthcare systems, making them scalable, efficient, and user-trusted. However, they fail to address the fundamental need for integrating standards from the CIA and AAA frameworks, essential for establishing secure, reliable, and adaptable smart healthcare environments within smart cities.

3.2.3 | Smart Healthcare With Quantum Computing

The potential of quantum computing to transform security, privacy, and efficiency within intelligent healthcare systems is substantial, particularly in managing and exchanging sensitive health data. This section presents how quantum computing can bolster the CIA triad (Confidentiality, Integrity, and Availability) and AAA models, such as Authentication, Authorisation, and Access Control, in healthcare settings. The focus is on its applications in medical imaging, data sharing, and patient monitoring.

In smart healthcare, a major issue is the secure transfer of sensitive medical information, especially in telehealth and remote monitoring. To address this challenge, Janani et al. [68] introduced a quantum cryptographic method for the secure transmission of medical images, which uses a two-layer encryption strategy to protect diagnostic details, such as tumour data. Building on this foundation, Kalaivani et al. [70] improved the BB84 quantum cryptography protocol employing the quantum key distribution (QKD) to protect the confidentiality of the keys exchanged in wireless body sensor networks. This advancement guarantees data security and minimises the threat of eavesdropping. Research emphasises how quantum cryptography fortifies the CIA triad while increasing security measures concerning data transfer with AAA protocols.

Quantum computing delivers significant advancements in healthcare. According to Ju et al. [69], quantum-enhanced machine learning could provide more accurate and efficient analysis in healthcare and sports; however, obstacles like resource constraints and institutional challenges persist. Future research needs to focus on the advancement of quantum technologies and the cultivation of trust in these innovations to ensure their successful incorporation into modern healthcare systems.

3.2.4 | Smart Healthcare With Hybrid Approach

Blockchain, AI, and Quantum Computing collectively transform the healthcare sector by significantly advancing security, privacy, trust, and scalability. This comprehensive approach leverages decentralisation, rapid data analysis, and advanced security protocols to adhere to the principles of the CIA triad and the AAA frameworks, thus promoting a more robust and secure healthcare infrastructure.

Tagde et al. [79] introduced a new paradigm by integrating Blockchain with AI for more reliable and effective management of health data systems. Blockchain provides secure, decentralised storage, and AI improves data analysis and decision-making, using role-based access control (RBAC) to safeguard patient privacy. In enhancing Blockchain-based EHR systems with quantum computing, Shuaib et al. [80] highlighted the need for quantum-resistant cryptographic algorithms to secure sensitive medical information. Additionally, Marridi et al. [81] introduced the IP-HealthChain framework, emphasising Blockchain's essential function in improving the efficiency, security, and dependability of medical data transactions, especially during emergencies such as pandemics.

Ali et al. [92] integrated Blockchain with deep learning techniques to improve scalability and security, employing federated learning and homomorphic encryption to protect sensitive data. Additionally, Patel et al. [82] recommended a robust communication system that utilises fuzzy logic, artificial intelligence, and Blockchain to guarantee the secure storage and verification of healthcare information, addressing scalability challenges through IPFS.

Integrating Blockchain, AI, and quantum computing transforms the healthcare sector by improving patient treatment, safeguarding security, and maintaining privacy. Table 5 provide a summary of the literature on technologies related to smart healthcare and a summary of Blockchain, AI, quantum computing, and hybrid approaches in smart healthcare respectively. These technologies address significant healthcare challenges such as scalability, data protection, and operational efficiency. Blockchain provides secure data storage, AI enhances decision-making, and quantum computing delivers sophisticated encryption for sensitive health information, overcoming obstacles encountered by intelligent healthcare systems. Similarly, Figure 9 shows the number of papers dealing with challenges in Smart Healthcare with regard to security, privacy, scalability, and trust, grouped by emerging technologies like Blockchain, AI, Quantum Computing, and Hybrid approach.

3.3 | Intelligent Transportation System

Intelligent Transportation Systems (ITS) integrate advanced technologies with transportation infrastructure to optimise urban mobility, improving efficiency, safety, and sustainability. As shown in Figure 10, ITS encompasses various components, including vehicles, public transit, pedestrian paths, bicycles, and associated sensors, wireless communications, and GPS systems, all working in coordination to improve traffic management. These systems enable real-time data exchange between vehicles, infrastructure and users, thereby optimising traffic flow, reducing congestion, ensuring public safety, and promoting environmentally sustainable transportation solutions.

In alignment with smart city goals, ITS must adhere to core principles such as the CIA triad (Confidentiality, Integrity and Availability) and AAA mechanisms (Authentication,

TABLE 5 | Consolidated analysis of smart healthcare technologies: Security, privacy, trust, scalability, and summary.

Technology	References	Security	Privacy	Trust	Scalability	Summary
Blockchain	Tripathi et al. [45]	✓	✓	✓	✗	S2HS framework secures EMRs via cryptographic methods. *AAA perspective*: Strong access management but lacks regulatory compliance details
Blockchain	Rahman et al. [46]	✓	✓	✓	✗	PoTE consensus enhances node authentication. *AAA perspective*: Robust AAA but scalability in large networks needs validation
Blockchain	Mallick et al. [47]	✓	✓	✓	✓	Blockchain integrated with fog computing reduces latency. *AAA perspective*: Efficient data management but lacks energy optimisation
Blockchain	Rouzbahani et al. [48]	✓	✗	✓	✓	SCoTMan optimises trust via social IoT. *AAA perspective*: Privacy mechanisms need stronger focus for interoperability
Blockchain	Rani et al. [49]	✓	✓	✓	✗	IPFS along with AES encryption for patient-centric control. *AAA perspective*: Secure but scalability untested in large systems
AI	Wang et al. [60]	✓	✓	✗	✓	FRESH framework merges federated learning with ring signatures. *AAA perspective*: Strong privacy but lacks cross-system integration
AI	Liu et al. [59]	✗	✓	✓	✗	Focuses on trust and privacy in user adoption. *AAA perspective*: Weak security foundations limit AAA robustness
AI	Habbal et al. [62]	✓	✓	✓	✗	AI TRiSM ensures trust and risk management. *AAA perspective*: Theoretical framework; real-world testing needed
AI	Li et al. [58]	✓	✓	✓	✗	Federated learning for Alzheimer's detection. *AAA perspective*: Privacy-preserving but scalability challenges
AI	Kulurkar et al. [61]	✗	✗	✗	✓	LSTM along with cloud computing for data analysis. *AAA perspective*: Prioritises scalability over security, privacy and trust
Quantum computing	Janani et al. [68]	✓	✓	✓	✗	Quantum encryption for medical imaging. *AAA perspective*: Tamper-proof but limited scalability
Quantum computing	Kalaivani et al. [70]	✓	✓	✓	✗	Enhanced BB84 protocol for WBSNs. *AAA perspective*: Secure key exchange; scalability unexplored
Quantum computing	Ju et al. [69]	✗	✗	✗	✓	Quantum ML for healthcare analytics. *AAA perspective*: Focuses on efficiency, not security/trust
Hybrid approach	Tagde et al. [79]	✓	✓	✓	✓	Blockchain integrated with AI and RBAC for data management. *AAA perspective*: Balances security and scalability but lacks real-world trials
Hybrid approach	Shuaib et al. [80]	✓	✓	✓	✗	Quantum-resistant blockchain for EHRs. *AAA perspective*: Strong encryption; scalability needs testing
Hybrid approach	Marridi et al. [81]	✓	✓	✓	✗	IP-HealthChain for emergency data efficiency. *AAA perspective*: Secure but integration with legacy systems unclear
Hybrid approach	Patel et al. [82]	✓	✓	✗	✗	Integration of AI, fuzzy logic and blockchain for secure storage. *AAA perspective*: Strong AAA but untested in dynamic environments

Authorisation and Access Control). Ensuring data security and robust AAA protocols is essential for building trust and scalability within the transportation ecosystem, thereby fostering secure and resilient urban environments.

3.3.1 | ITS With Blockchain

The integration of Blockchain in Intelligent Transportation Systems (ITS) addresses key concerns of security, privacy, trust,

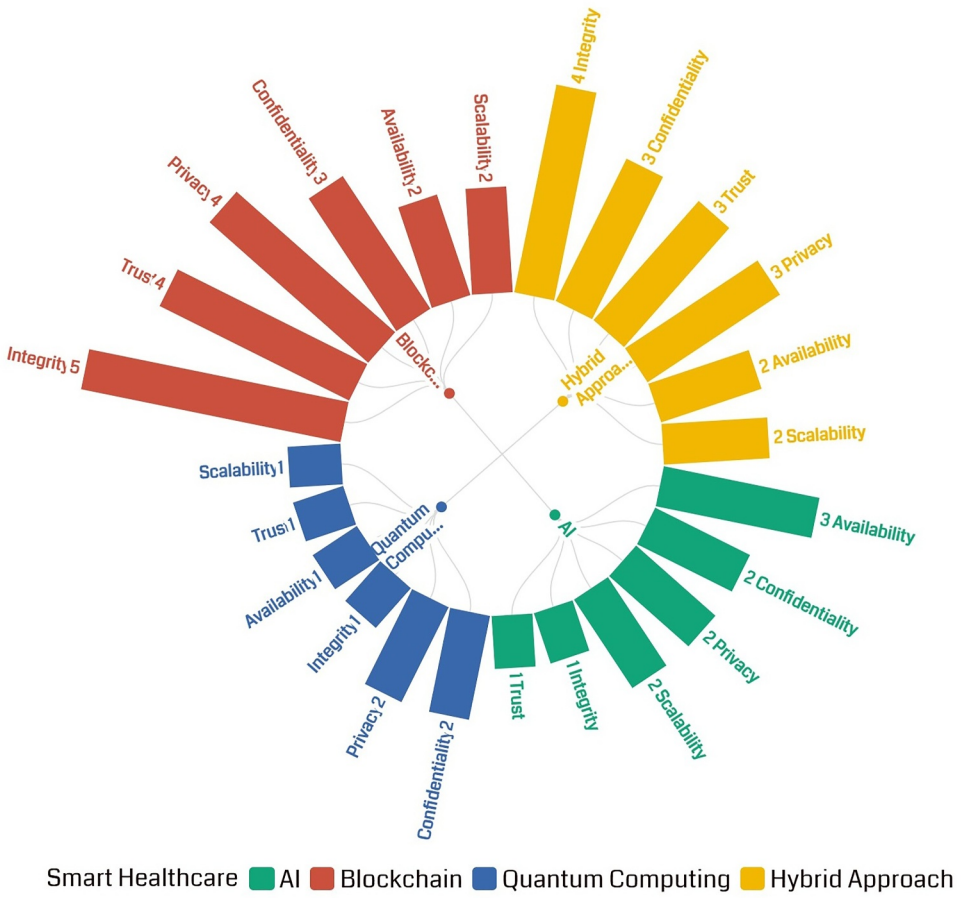

FIGURE 9 | Number of papers addressing challenges in smart healthcare (security, privacy, scalability, and trust), categorised by emerging technologies (blockchain, AI, and quantum computing).

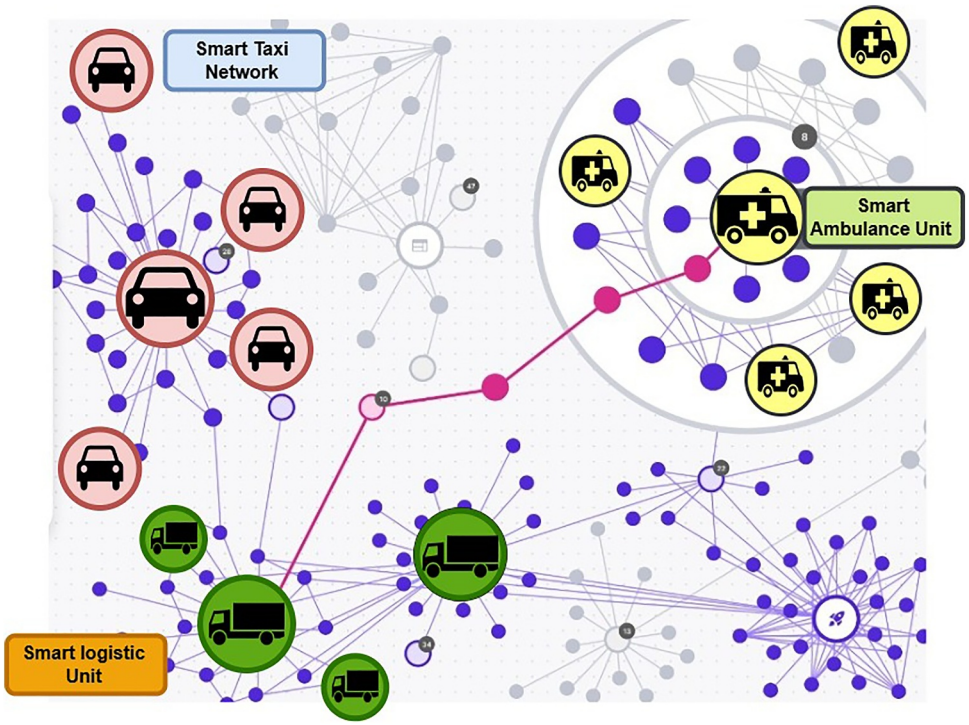

FIGURE 10 | ITS ecosystem.

and scalability by aligning with the CIA triad and implementing AAA mechanisms. Various studies have proposed Blockchain-based frameworks to improve ITS security and efficiency by ensuring secure data exchanges, protecting user privacy, and mitigating cyber threats.

Wazid et al. [50] introduced a Public Blockchain-Envisioned Secure Communication Framework (PBSCF-ITS) that protects communication channels between vehicles, roadside units (RSU) and cloud servers through strong access control and key management, protecting against attacks such as Man-in-the-Middle (MiTM). Qureshi et al. [51] advanced the role of Blockchain in privacy-preserving authentication within ITS, using decentralised authentication and dynamic identity management to increase user privacy and prevent unauthorised vehicle monitoring, which aligns well with the CIA triad. Alkhalifa et al. [52] proposed a Bayesian DAG-based Blockchain for vehicle networks, improving data privacy and real-time processing capabilities while ensuring robust security against rogue nodes.

The latest technological advancement has integrated Blockchain with zero trust frameworks to secure critical infrastructures. Hao et al. [53] designed a two-layer consortium Blockchain within a zero trust paradigm, concentrating on optimising interactions between vehicles and RSUs (Roadside Units) via automatic identity verification and secure transaction execution. Badshah et al. [54] introduced a Blockchain-based authentication security framework (BASF-ITS) that integrates Elliptic Curve Cryptography (ECC) with Physical Unclonable Functions (PUF) to enhance authentication and bolster privacy, while guarding against identity theft and Man-in-the-Middle (MiTM) attacks. Meanwhile, Din et al. [93] explored trust management in Intelligent Cyber-Physical Transportation Systems (ICPTS) through the use of a Context-Aware Cognitive Memory Trust Management system, which integrates game theory and Blockchain to ensure secure, transparent decision-making and scalability.

These studies highlight Blockchain's importance in enhancing CIA and AAA mechanisms within ITS, proposing scalable, secure, and privacy-preserving solutions. The integration of Blockchain into the ITS framework can be seen as a way to pave the way for smart urban mobility in the face of current issues, which will eventually allow for advanced transportation systems.

3.3.2 | ITS With AI

The advent of AI has transformed ITS by enhancing security, privacy, trust, and scalability. These improvements provide highly effective solutions to contemporary transportation issues. In this section, we look at how AI resolves some of the critical challenges for ITS, from the perspective of the CIA triad and AAA protocols.

Kaushik et al. [63] underscore the significant role of AI in the evolution of Intelligent Transportation Systems (ITS), especially through cognitive computing, the Internet of things (IoT), and machine learning integration. They propose utilising Blockchain technology to secure data integrity and privacy in Vehicle-to-Everything (V2X) communications, adhering to the principles of confidentiality, integrity, and availability (CIA). Their findings suggest that scalability can be enhanced with machine learning and deep learning techniques, but also stress the necessity for ongoing improvements to ensure strong security and dependability in traffic management systems.

Alam et al. [64] examine the privacy and security challenges associated with Autonomous Connected Vehicles (ACVs) within the context of smart cities. They introduce a decentralised BFRL architecture aimed at securing communication, emphasising the need for security solutions that are both scalable and adaptable. This framework is consistent with the principles of CIA and AAA, advocating for security in the dynamic environment of Intelligent Transportation Systems (ITS).

Xu et al. [65] integrate generative AI with digital twin technologies to facilitate autonomous vehicle training in virtual reality settings. The framework they propose enhances transparency, thereby building user confidence. While security and privacy issues remain partially unresolved, the model's scalability is apparent, ensuring effective data exchanges in ITS. Future studies could focus on strengthening security protocols to comply with CIA and AAA standards.

In summary, AI offers substantial potential to improve the security, privacy, trust, and scalability of ITS. The reviewed studies demonstrate AI's ability to manage traffic, enable autonomous navigation, and address incidents in real time. However, to fully realise its potential, future research should focus on refining AI technologies to improve safety, user trust, and integration of robust security mechanisms aligned with CIA and AAA models, ensuring secure, flexible, and efficient ITS solutions.

3.3.3 | ITS With Quantum Computing

Quantum computing has the transformative ability to tackle key security, privacy, and scalability challenges within Intelligent Transportation Systems (ITS). This section explores incorporating quantum technologies, emphasising quantum cryptography, optimisation, and post-quantum security frameworks in alignment with the principles of CIA (Confidentiality, Integrity, Availability) and AAA (Authentication, Authorisation, Access Control).

The study by Mohanty et al. [71] presents the Quantum Secure Threshold Private Set Intersection (QuTPSI) protocol, leveraging quantum cryptography to bolster privacy measures within IoT-facilitated ride-sharing applications. This protocol provides a secure method for identifying intersection points within private datasets, thus protecting user privacy, ensuring data confidentiality, and upholding a dependable trust infrastructure in ride-sharing systems. The QuTPSI framework's ability to withstand classical and quantum security threats guarantees its compliance with CIA and AAA standards.

Jagirdar et al. [72] emphasise the pivotal importance of quantum cryptography in securing transport-related data, particularly in

fleet monitoring and traffic light synchronisation. The research focuses on developing stronger encryption methods to mitigate the quantum attack to ensure safety and scalability while solving the two significant issues of privacy and trust in an urban transportation infrastructure. Sutradhar et al. [73] introduce the Secure Vehicle Quantum Communication Protocol (SVQCP), which uses quantum cryptography to achieve confidential, authenticated, and secure interactions amongst vehicles. It applies multiple cryptographic methods on this point to ensure no unauthorised access threat crosses the path of reliability and scalability of dynamic vehicular networks and guarantees efficient and secure communication within the systems.

The work in Qu et al. [74] addresses the security and privacy issues for the 6G Quantum Internet of Vehicles by employing the Quantum Efficient Privacy Protection Protocol QEPP. The protocol utilises quantum mechanics principles in improving data protection as well as optimising cloud resource usage for secure and scalable communication in IoV. The integration of quantum computing is going to add significantly to the security, privacy, and scalability of Intelligent Transportation Systems (ITS). The analysis points out that the combination of quantum cryptography with post-quantum security schemes gives a comprehensive solution to the current system problems; hence, it supports the maturation of an advanced, efficient, and dependable transportation network as the quantum technology develops.

3.3.4 | ITS With Hybrid Approach

The integration of quantum computing, Blockchain, and AI plays a vital role in developing ITS. The combination of these technologies addresses the complex issues related to urban transportation while adhering to CIA and AAA security, privacy, and trust frameworks. The following section explains some of the key developments based on these innovations to improve the security, reliability, and scalability of ITS.

The research by Ghosh et al. [94] presents a novel hybrid Blockchain framework that leverages quantum properties, including superposition and entanglement, to overcome the conventional Blockchain scalability and transaction efficiency problems in an urban context. The solution incorporates quantum-resistant cryptography for urban sensitive data for both confidentiality and integrity. This technique adds further transparency and enhances stakeholder trust, thus leading to scalable and safe smart urban environments. Similarly, Saleem et al. [83] propose a traffic management system with the integration of MapReduce, private Blockchain, and explainable artificial intelligence (XAI) that can efficiently control urban traffic congestion for reliable and secure operations.

Gupta et al. [84] explore a technique called quantum-secured Blockchain-supported data authentication (QBCPDA). This method employs lattice-based cryptography and Blockchain technology to safeguard the Internet of vehicles (IoV) from potential quantum threats. It also ensures conditional anonymity and unlinkability during message verification and allows for batch validation of vehicle data, thereby enhancing network scalability as the vehicle count rises. On the other hand, the research by Vaidyan et al. [85] looks at the issue of cybersecurity related to Traffic Signal Control (TSC) systems in interconnected vehicular settings. Their work applies hybrid quantum AI methods to detect malware and adversarial threats, specifically to minimise risks associated with data tampering in the TSC system. This further improves the security, privacy, and dependability of TSC systems as they align with the core principles of CIA and AAA in ITS frameworks.

Liu et al. [86] develop a quantum Blockchain framework (QBIoV) for the Internet of vehicles, which emphasises quantum threat mitigation, using Quantum Hash Functions (QHF) and Quantum Public Key Signatures, for secure data transmission. Although scalability is not considered, the Quantum Proof of Authority consensus model minimises communication overhead and supports expansion of the IoV network.

Nguyen et al. [87] integrate generative AI and Blockchain to enhance security, privacy, and scalability. Their Generative Diffusion Model (GDM) enhances the efficiency and latency of Blockchain by generating synthetic data that simulates user behaviour, keeping users anonymous. This improves confidentiality, reliability, and scalability for large-scale ITS deployment.

Integrating quantum computing, artificial intelligence, Blockchain, and combined approaches shows significant promise in addressing security, privacy, and scalability issues within intelligent transportation systems. Table 6 provide a comprehensive summary of the pertinent literature related to ITS technologies, including a detailed examination of Blockchain, AI, quantum computing, and hybrid strategies, highlighting their characteristics and limitations. Together, these technologies improve transport networks' efficiency, safety, and reliability, fostering the creation of smart cities with cutting-edge mobility solutions. Likewise, Figure 11 illustrates the number of papers dealing with challenges in Intelligent Transportation Systems (ITS) with regard to security, privacy, scalability, and trust, grouped by emerging technologies like Blockchain, AI, Quantum Computing, and Hybrid approach.

4 | Cross-Domain Comparative Analysis and Practical Applicability

According to the Technology Adaptation Levels framework introduced in Section 2.5, this section provides a detailed evaluation of Blockchain, artificial intelligence (AI), quantum computing, and hybrid approaches across three pivotal smart city domains: smart homes, healthcare, and intelligent transportation systems (ITS). The adaptation scores, as depicted in Table 2, act as a method of measuring the degree of compliance each technology holds towards the CIA triad and the AAA protocols. Based on a thorough literature review for each domain, these scores offer an in-depth basis for the assessment of the advantages, drawbacks, and future directions of these technologies. Our goal is to provide practical observations in terms of the opportunities and challenges in securing smart city ecosystems and, through that, advance the knowledge of their effective deployment.

TABLE 6 | Consolidated analysis of ITS technologies: Security, privacy, trust, scalability, and summary.

Technology	References	Security	Privacy	Trust	Scalability	Summary
Blockchain	Wazid et al. [50]	✓	✓	✓	✗	Public blockchain-Envisioned secure communication framework secures V2X communication via access control and key management. *AAA perspective*: Strong security and privacy but scalability untested in high-traffic scenarios
Blockchain	Qureshi et al. [51]	✓	✓	✓	✗	Decentralised authentication with dynamic identity management. *AAA perspective*: Robust AAA but scalability challenges in large networks
Blockchain	Alkhalifa et al. [52]	✓	✓	✗	✓	Bayesian DAG-Blockchain enhances real-time processing and privacy. *AAA perspective*: Scalable but trust mechanisms need validation in complex ITS
Blockchain	Hao et al. [53]	✓	✓	✓	✗	Zero-trust consortium blockchain for secure vehicle-RSU interactions. *AAA perspective*: Strong AAA but scalability limited by transaction throughput
Blockchain	Badshah et al. [54]	✓	✓	✓	✗	ECC-PUF framework for authentication and anti-tampering. *AAA perspective*: Privacy-focused but scalability requires real-world testing
AI	Kaushik et al. [63]	✓	✓	✗	✓	Privacy-preserving V2X security and traffic management. *AAA perspective*: Comprehensive but needs empirical validation
AI	Alam et al. [64]	✓	✓	✓	✗	BFRL architecture for ACV security. *AAA perspective*: Strong privacy and trust but scalability unproven
AI	Xu et al. [65]	✗	✗	✓	✓	Generative AI for autonomous vehicle training. *AAA perspective*: Trust and scalability prioritised; security and privacy gaps remain
Quantum computing	Mohanty et al. [71]	✓	✓	✓	✗	QuTPSI protocol for IoT ride-sharing privacy. *AAA perspective*: Quantum-secure but scalability limited
Quantum computing	Jagirdar et al. [72]	✓	✓	✗	✓	Quantum cryptography for fleet monitoring and traffic control. *AAA perspective*: Scalable encryption but lacks dynamic trust models
Quantum computing	Sutradhar et al. [73]	✓	✓	✗	✓	SVQCP for authenticated vehicular communication. *AAA perspective*: Secure but trust mechanisms need refinement
Quantum computing	Qu et al. [74]	✓	✓	✓	✗	QEPP for 6G IoV data protection. *AAA perspective*: Quantum-efficient but scalability un-addressed
Hybrid approach	Saleem et al. [83]	✓	✓	✓	✓	MapReduce integrated with private blockchain for traffic management. *AAA perspective*: Efficient but dynamic network challenges unaddressed
Hybrid approach	Gupta et al. [84]	✓	✓	✓	✗	QBCPDA with lattice cryptography for IoV. *AAA perspective*: Quantum-resistant but computationally intensive
Hybrid approach	Vaidyan et al. [85]	✓	✗	✓	✗	Quantum integrated AI in traffic signal control (TSC) for malware detection. *AAA perspective*: Security-focused; privacy and scalability gaps
Hybrid approach	Liu et al. [86]	✓	✓	✓	✗	QBIoV framework with quantum consensus. *AAA perspective*: Secure but scalability needs testing
Hybrid approach	Nguyen et al. [87]	✓	✓	✗	✓	GAI + blockchain for synthetic data anonymity. *AAA perspective*: Balances privacy and scalability; trust needs validation

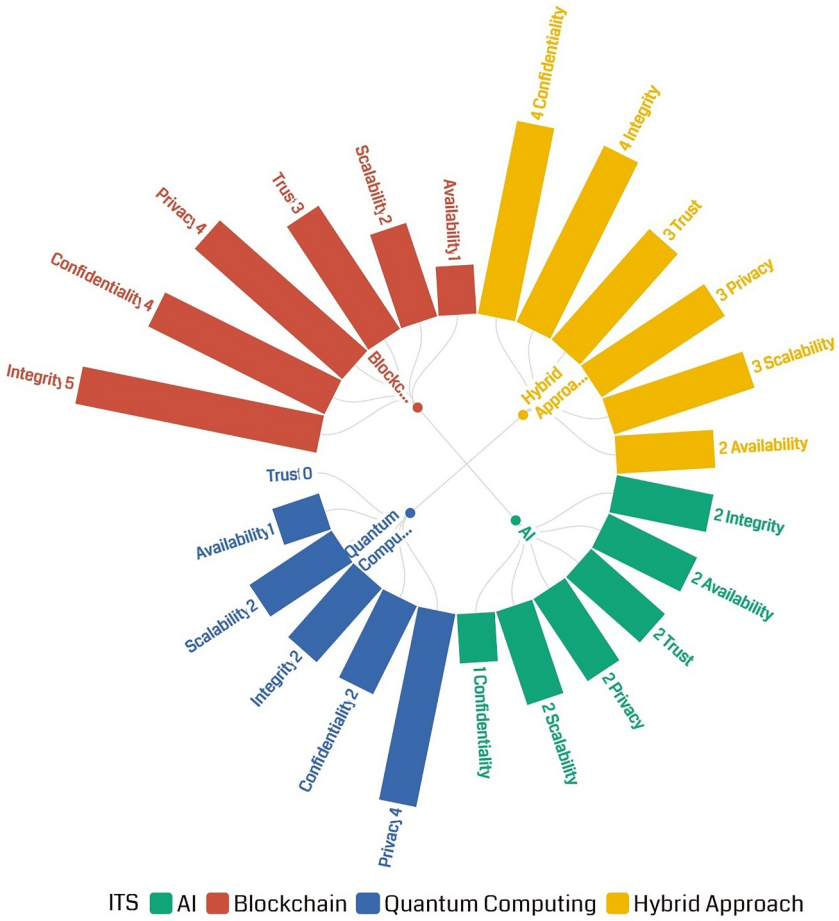

FIGURE 11 | Number of papers addressing challenges in intelligent transportation system (security, privacy, scalability, and trust), categorised by emerging technologies (blockchain, AI, and quantum computing).

4.1 | Cross-Domain Comparative Analysis

This sub-section presents a balanced comparison of Blockchain, AI, quantum computing, and hybrid solutions in smart homes, healthcare, and ITS on the basis of their adherence to the CIA triad and AAA protocols based on a rich repository of domain-specific literature to highlight their respective strengths and inherent challenges.

Blockchain is recognised as a robust solution across multiple domains due to its decentralised structure and cryptographic foundations, which provide enhanced security and trust. In the context of smart homes, research by Xue et al. [88] and Awan et al. [38] highlights Blockchain's ability to safeguard data integrity and enforce stringent access controls. However, scalability issues arise in expansive IoT ecosystems, as noted by Lin et al. [21] and Qashlan et al. [22]. Within the healthcare sector, Blockchain plays a pivotal role in securing electronic medical records (EMRs), as demonstrated by Tripathi et al. [45] and Rahman et al. [46], though scalability concerns persist amidst increasing data volumes [47, 49]. In intelligent transportation systems (ITS), Blockchain enhances vehicle-to-everything (V2X) communication, as shown by Wazid et al. [50] and Qureshi et al. [51], yet scalability remains a challenge in dynamic vehicular networks [52, 53]. While Blockchain excels in security and trust, its scalability limitations necessitate innovative solutions.

Artificial Intelligence (AI) stands out due to its remarkable scalability and real-time adaptability, making it well-suited for environments requiring rapid responsiveness. In smart homes, AI improves monitoring and intrusion detection, as shown by Shahjalal et al. [57] and Taiwo et al. [89], although privacy concerns arise from centralised data processing [56]. In healthcare, AI drives scalable analytics for telemedicine, with federated learning approaches by Li et al. [58] and Wang et al. [60] enhancing privacy. However, the opacity of AI models undermines trust, as highlighted by Habbal et al. [62] and Kulurkar et al. [61]. In ITS, AI optimises traffic management and autonomous navigation, according to Kaushik et al. [63] and Alam et al. [64], though privacy and trust issues persist in decentralised settings [65, 73]. While AI excels in scalability, advancements in transparency and privacy preservation are essential to fully unlock its potential.

Quantum Computing holds transformative potential for cryptography, though its practical deployment is hindered by current hardware limitations. In smart homes, quantum-resistant frameworks proposed by Shahid et al. [66] and Chaudhary et al. [19] signal future security enhancements, though infrastructure immaturity remains a challenge [67]. In healthcare, quantum cryptography secures medical data transmission, as explored by Janani et al. [68] and Kalaivani et al. [70], but scalability remains an unresolved issue [69, 74]. In ITS, quantum technologies bolster privacy in ride-sharing and vehicle communication,

according to Mohanty et al. [71] and Jagirdar et al. [72], yet hardware constraints limit immediate applicability [73, 74]. While quantum computing offers unparallelled security potential, its scalability and trustworthiness remain developmental.

Hybrid Approaches combine Blockchain, AI, and quantum computing to harmonise security, scalability, and trust. In smart homes, Khan et al. [75] and Shahbazi et al. [78] integrate Blockchain's security with AI's adaptability, though integration complexity hinders widespread adoption [76, 77]. In healthcare, hybrid frameworks like those by Tagde et al. [79] and Shuaib et al. [80] fuse Blockchain's trust mechanisms with AI's analytical capabilities, yet computational overhead remains a concern [82, 92]. In ITS, Gupta et al. [84] and Liu et al. [86] utilise quantum-Blockchain integration for enhanced security, though scalability and complexity issues persist [83, 87]. Hybrid approaches promise a balanced solution but their complexity emphasises the need for streamlined, modular designs.

4.2 | Practical Insights and Applicability

The practical deployment of Blockchain, AI, quantum computing, and hybrid approaches varies across smart homes, healthcare, and ITS, with each domain offering unique opportunities and challenges. Table 2 shows applicability and Table 7 consolidates how these technologies address key research questions (RQs) related to security, privacy, trust, and scalability, providing a holistic view of their real-world applications. The adaptation ratings in Table 2 point to significant trends: Blockchain has high compliance in smart homes and ITS but merely medium in healthcare due to scalability issues in medical data environments. AI, by contrast, exhibits high adaptability in healthcare and ITS, powered by federated learning and real-time analytics, while quantum computing is behind with low/medium ratings across domains, reflecting its nascent stage. Hybrid solutions, though flagged as high (future), point to transformational potential by addressing gaps in privacy and scalability, reflecting the demand for interdisciplinary innovation to make them viable.

In *Smart Homes*, Blockchain secures high-stakes IoT applications, as evidenced by Xue et al. [88] and Awan et al. [38], ensuring robust data exchange and access control (RQ1). Blockchain's decentralised architecture strengthens the CIA triad through tamper-proof data integrity and confidentiality, while AI enhances availability via real-time anomaly detection (RQ2). AI facilitates scalable, real-time monitoring, as shown by Shahjalal et al. [57] and Taiwo et al. [89], though privacy concerns remain (RQ3). Hybrid approaches, such as those of Khan et al. [75], offer a balance between security and scalability, though their complexity necessitates lightweight protocols and privacy-by-design strategies for broader adoption.

In *Smart Healthcare*, Blockchain offers a secure foundation for managing EMRs, as demonstrated by Tripathi et al. [45] and Rahman et al. [46] (RQ1). Blockchain ensures trust and data integrity via decentralised consensus, while federated learning in AI preserves privacy during telemedicine analytics (RQ2). AI powers scalable telemedicine analytics, with federated learning enhancing privacy, as seen in Li et al. [58], though trust in AI requires explainable models (RQ3). Hybrid solutions, such as those proposed by Tagde et al. [79], deliver comprehensive security but face challenges due to their complexity, necessitating modular architectures for effective implementation.

In *ITS*, Blockchain secures V2X communication, as shown by Wazid et al. [50] and Qureshi et al. [51] (RQ1). Blockchain's immutability guarantees data integrity, while AI enhances trust through real-time traffic incident management and adaptive decision-making (RQ2). AI optimises traffic flow, as demonstrated by Kaushik et al. [63], but privacy concerns persist (RQ3). Hybrid approaches, like those of Gupta et al. [84], elevate security through quantum-Blockchain synergy, though scalability challenges demand hierarchical designs and explainable AI to realise their full potential.

Across these domains, hybrid approaches offer a promising strategy to balance security, trust, and scalability. However, their practical deployment requires standardised protocols and modular frameworks to reduce complexity, paving the way for seamless integration into smart city ecosystems.

5 | Case Studies With Future Directions

This section presents a detailed exploration of four case studies focused on the technological adaptation of Blockchain, Artificial Intelligence (AI), Quantum Computing, and their hybrid integration within various domains of smart cities. These case studies have been selected to illustrate how advanced technologies are being leveraged to address AAA (Authentication, Authorisation, and Accounting) security challenges, with a particular emphasis on security, privacy, trust, and scalability. Each case study is structured to highlight the following elements:

1. Motivation: The pressing need or domain-specific challenge led to technological intervention.
2. Technological solution: The proposed or implemented solution involving a specific emerging technology or a combination thereof.
3. Future directions: A critical analysis of the limitations, open challenges, and potential enhancements through the integration of other emerging technologies.

By synthesising insights from existing literature and real-world deployments, this section aims to provide a cross-domain perspective on how smart cities can evolve through secure and privacy-preserving architectures. Moreover, it outlines future research pathways where the convergence of Blockchain, AI, and Quantum Computing can significantly enhance the resilience and intelligence of urban services.

5.1 | Case Study 1: Blockchain for Healthcare Data Management [37]

5.1.1 | Motivation

The growing reliance on digital health services in smart cities necessitates a secure, transparent, and patient-centric approach

TABLE 7 | Consolidated answers to research questions across domains.

Research question	Smart homes	Healthcare	ITS
RQ1: What are the current technological solutions employed for enhancing AAA security mechanisms in smart cities?	Blockchain enables secure data exchanges and decentralised access control (Lin et al. and Qashlan et al.) [21, 22]. AI improves authentication through machine learning techniques like CNNs [89] and LoRa technology (Taiwo et al. and Shahjalal et al.) [57]. Quantum computing explores lattice-based cryptosystems for securing data against quantum threats (Shahid et al.) [66]	Blockchain secures electronic medical records (EMRs) and enables patient-centric access control (Tripathi et al. and Rahman et al.) [45, 46]. AI enhances real-time monitoring and decision-making through federated learning (Li et al. and Wang et al.) [58, 60]. Quantum computing provides advanced encryption for medical data (Janani et al. and Kalaivani et al.) [68, 70]	Blockchain enables secure data exchanges, decentralised authentication, and access control (Wazid et al. and Qureshi et al.) [50, 51]. AI plays a critical role in improving trust and scalability for incident detection and autonomous decision-making (Kaushik et al. and Alam et al.) [63, 64]. Quantum computing contributes to privacy and data protection through quantum encryption (Mohanty et al.) [71]
RQ2: How do advanced technologies such as blockchain, AI, and quantum computing impact the CIA triad, trust, privacy, and scalability in AAA security solutions?	Blockchain strengthens confidentiality and integrity through its decentralised structure (Awan et al. and Nasonov et al.) [38, 43]. AI enhances availability through real-time monitoring (Majymder et al. and Shahjalal et al.) [56, 57]. Quantum computing offers future-proof security with quantum-resistant cryptography (Chaudhary et al. and Shahid et al.) [19, 66]	Blockchain ensures data integrity and trust through decentralised storage and consensus mechanisms (Mallick et al. and Rahman et al.) [46, 47]. AI enhances scalability and availability via real-time analytics (Kulurkar et al. and Habbal et al.) [61, 62]. Quantum computing strengthens confidentiality with advanced encryption (Kalaivani et al. and Janani et al.) [68, 70]	Blockchain strengthens the CIA triad by ensuring data integrity (via immutability) and availability (decentralised networks), while enhancing privacy with cryptographic techniques [50, 51]. AI enhances trust through real-time data processing and incident management, facilitating scalability (Kaushik et al. and Alam et al.) [63, 64]. Quantum computing improves privacy and confidentiality with quantum cryptography (Sutradhar et al. and Dharminder et al.) [73, 95]
RQ3: What are the challenges and limitations associated with implementing AAA security solutions in the context of smart city applications?	Blockchain faces scalability challenges in large IoT environments (Lin et al. and Qashlan et al.) [21, 22]. AI struggles with privacy and trust in centralised systems (Majumder et al.) [56]. Quantum computing is limited by infrastructure immaturity and energy inefficiency (Alomari et al. and Shahid et al.) [66, 67]	Blockchain encounters scalability issues due to growing medical data volumes (Rani et al. and Mallick et al.) [47, 49]. AI faces trust and privacy challenges in multi-user systems (Habbal et al. and Liu et al.) [59, 62]. Quantum computing is constrained by hardware limitations and deployment barriers (Ju et al. and Kalaivani et al.) [69, 70]	Blockchain faces scalability challenges, especially in integrating with existing ITS infrastructures and ensuring real-time data processing (Wazid et al. and Qureshi et al.) [50, 51]. AI faces privacy concerns in autonomous systems and the need for real-time adaptability (Kaushik et al. and Alam et al.) [63, 64]. Quantum computing is still in the early stages of development, with hardware limitations and challenges in creating quantum-resistant cryptography (Mohanty et al.) [71]

to managing electronic health records (EHR). Traditional centralised health information systems are often vulnerable to data breaches, unauthorised access, and inefficiencies in data sharing across institutions. These issues pose significant risks to patient privacy and hinder seamless healthcare delivery.

5.1.2 | Technological Adaptation

The authors discussed the proposed a decentralised healthcare architecture that leverages Blockchain technology to enhance the management of EHRs. In this framework, patient data is

encrypted and securely stored on a Blockchain ledger, and smart contracts are deployed to regulate access control policies. This allows patients to maintain sovereignty over their data by selectively granting access to healthcare providers, thereby improving both confidentiality and trust in the healthcare data lifecycle.

5.1.3 | Future Direction

While Blockchain offers a strong foundation for secure and decentralised healthcare data management, the complexities of smart city healthcare ecosystems demand more than isolated technological interventions. The integration of Blockchain with Artificial Intelligence (AI) and Quantum Computing presents a futuristic, hybrid approach capable of addressing trust, privacy, scalability, and processing bottlenecks in a unified manner. However, this convergence also introduces novel challenges that remain open for exploration. Below are three critical and futuristic research directions based on this technological triad.

1. *Blockchain enabled AI adaptive trust frameworks across heterogeneous healthcare services:* In smart cities, healthcare services are delivered through a diverse and dynamic mix of entities ranging from public hospitals to mobile clinics and wearable IoT platforms. These entities often lack a unified trust and verification layer. A promising direction is the development of an AI-driven adaptive trust framework, built on top of Blockchain-based identity and access control systems, to evaluate service providers based on context-aware metrics (e.g., reputation scores, anomaly detection in service delivery, or historical integrity of shared data). AI can provide dynamic trust scoring, while Blockchain ensures transparent and auditable policy enforcement across stakeholders.
2. *Secure and interoperable data governance through quantum-resistant ledgers:* As quantum computing matures, it threatens to break traditional cryptographic algorithms underpinning Blockchain-based health records. A key research problem is designing quantum-resistant Blockchain architectures (e.g., based on lattice cryptography or post-quantum hash functions) to safeguard patient records for long-term confidentiality. Moreover, future systems should enable interoperability between quantum and classical systems, ensuring that data can move securely across legacy healthcare platforms and quantum-secure environments without risk of compromise.

5.2 | Case Study 2: Hybrid Integration of Quantum Computing and Blockchain in 6G-Enabled Smart City Infrastructure [96]

5.2.1 | Motivation

The rapid evolution of smart cities demands unprecedented levels of data processing, connectivity, and security. With the emergence of 6G technologies, characterised by ultra-reliable low-latency communication (URLLC), massive device connectivity, and real-time responsiveness, traditional computing and network paradigms face limitations. Urban management systems require scalable architectures capable of handling large volumes of heterogeneous data securely and efficiently.

5.2.2 | Technological Adaptation

The authors propose an innovative Quantum-Blockchain-6G (QBG) framework that synergistically combines quantum computing and Blockchain technology to meet these emerging demands. In this architecture, Quantum computing is utilised for its computational superiority, enabling rapid processing of complex urban data such as traffic patterns, energy distribution, and public safety metrics. Blockchain ensures data integrity, auditability, and secure communication among interconnected city services. 6G communication capabilities further strengthen the system through ultra-high bandwidth and low latency, supporting time-sensitive applications such as intelligent transportation, emergency response, and real-time environmental monitoring. Together, this hybrid approach empowers intelligent infrastructure management with enhanced computational speed and tamper-proof data exchange across the city ecosystem.

5.2.3 | Future Direction

Despite its potential, the QBG framework faces several key challenges and research opportunities:

1. *Scalability and integration complexity:* Quantum computing infrastructure is still in its early stages, costly, hardware-dependent, and requiring specialised expertise. Integrating it seamlessly with Blockchain and 6G demands modular, scalable architectures that can operate across hybrid classical-quantum environments.
2. *Quantum threats to blockchain security:* While quantum computing offers enhanced encryption capabilities, it also poses risks to traditional cryptographic techniques used in Blockchain. Developing quantum-resistant consensus algorithms and post-quantum cryptographic standards is essential to secure future Blockchain implementations against quantum attacks.
3. *Regulatory and standardisation gaps:* A lack of regulatory frameworks, interoperability standards, and ethical considerations limits the deployment of QBG frameworks in real-world urban environments. Future research must explore cross-border data policies, quantum-safe transaction standards, and AI-governed Blockchain governance frameworks within 6G smart cities.

5.3 | Case Study 3: AI-Empowered Dynamic Authentication in IoMT [97]

5.3.1 | Motivation

With the rise of Internet of Medical Things (IoMT) in smart healthcare systems, vast amounts of sensitive medical data are

continuously generated by wearable sensors, remote monitoring devices, and connected diagnostics platforms. Ensuring secure context-aware authentication for such critical health data while maintaining system performance and real-time responsiveness remains a key challenge. Traditional static authentication methods lack the adaptability to dynamically assess the sensitivity and urgency of healthcare information.

5.3.2 | Technological Adaptation

Authors propose a hybrid framework integrating Artificial Intelligence (AI) with Blockchain through a novel consensus mechanism called Proof of AI-driven Authentication (PoAh 2.0), specifically designed for IoMT environments. The author used AI models to classify data sensitivity levels in real time, dynamically adjusting the security requirements for each data block. Blockchain ensures immutability and secure transmission, while the consensus layer is enhanced to be context-aware, assigning stronger validation processes to high-risk medical data (e.g., heart condition signals). Machine learning algorithms are also embedded to predict health anomalies, such as potential heart attacks, enabling proactive responses in critical care scenarios. This adaptive approach balances privacy preservation, data integrity, and responsive authentication in smart healthcare ecosystems.

5.3.3 | Future Directions

While PoAh 2.0 presents a promising shift towards intelligent and secure IoMT data handling, several challenges must be addressed to enable large-scale deployment:

1. *Resource efficiency in edge environments:* The use of AI and real-time classification in IoMT requires substantial computational resources, which are often limited in edge devices. Future research must focus on lightweight AI models and energy-aware Blockchain protocols to maintain efficiency without compromising security.
2. *Interoperability with legacy healthcare infrastructure:* Many existing hospital systems lack compatibility with AI-enhanced Blockchain frameworks. Solutions such as interoperable middleware, standardised data schemas, and API-level integrations need to be explored to bridge this technological gap.
3. *Scalable trust and federated learning for distributed medical systems:* In a broader smart city context, a federated and scalable AI architecture is essential to support cross-institutional data trust, allowing secure sharing and collaboration among multiple healthcare entities without centralising data, especially relevant for pandemics and emergency response scenarios.

6 | Conclusion

This study comprehensively evaluates emerging technologies like Blockchain, AI, quantum computing, and hybrid approaches for securing AAA mechanisms in smart city ecosystems. We identified key trends and challenges across smart homes, healthcare, and ITS through a systematic review and taxonomy-based analysis. Blockchain ensures decentralised trust and immutable data integrity, while AI enhances dynamic authentication and anomaly detection. Quantum computing, though nascent, offers transformative potential through quantum-resistant encryption. Hybrid models, combining Blockchain's transparency with AI's adaptability and quantum cryptography's robustness, emerge as the most balanced solution for scalability and cross-domain security.

Case studies in healthcare data management, 6G-enabled infrastructure, and IoMT authentication illustrate real-world applications, emphasising the need for context-aware frameworks. However, challenges persist, including Blockchain's scalability trade-offs, AI's 'black-box' opacity, and quantum computing's infrastructural immaturity. Future research must prioritise hybrid architectures, lightweight consensus mechanisms, and quantum-safe standards to address these limitations. Additionally, regulatory frameworks and interoperability protocols are critical for seamless integration across heterogeneous urban systems. By bridging technological gaps and fostering collaborative innovation, this work paves the way for resilient, privacy-preserving smart cities capable of adapting to evolving security threats and scalability demands.

Author Contributions

Usama Antuley: conceptualization, formal analysis, investigation, methodology, writing – original draft. **Sufian Hameed:** conceptualization, supervision, writing – review and editing. **Shahbaz Siddiqui:** conceptualization, methodology, supervision, writing – original draft. **Syed Attique Shah:** conceptualization, investigation, supervision, writing – review and editing.

Acknowledgements

The authors would like to express their sincere gratitude to all those who contributed to the completion of this study, as well as to the research and administrative staff for their valuable assistance. We also gratefully acknowledge the support provided by the Birmingham City University and National University of Computer and Emerging Sciences, which made this work possible.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

1. H. Samih, "Smart Cities and Internet of Things," *Journal of Information Technology Case and Application Research* 21, no. 1 (2019): 3–12, https://doi.org/10.1080/15228053.2019.1587572.

2. L. A. Sánchez-Balvás, J. J. de Felipe, J. M. Quintero, and A. de la Fuente, "An Energy Efficiency-Based Classification Approach for Street Lighting by Considering Operational Factors: A Case Study of Barcelona," *Energy Efficiency* 14, no. 1 (2021): 15, https://doi.org/10.1007/s12053-020-09915-y.

3. N. Pourmohammad-Zia and M. van Koningsveld, "Sustainable Urban Logistics: A Case Study of Waterway Integration in Amsterdam," *Sustainable Cities and Society* 105 (2024): 105334, https://doi.org/10.1016/j.scs.2024.105334.

4. S. Siddiqui, S. Hameed, S. A. Shah, J. Arshad, Y. Ahmed, and D. Draheim, "A Smart-Contract-Based Adaptive Security Governance Architecture for Smart City Service Interoperations," *Sustainable Cities and Society* 113 (2024): 105717, https://doi.org/10.1016/j.scs.2024.105717.

5. A. S. George, T. Baskar, and P. B. Srikaanth, "Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors," *Partners Universal International Innovation Journal* 2, no. 1 (2024): 51–75.

6. P. M. Rao and B. D. Deebak, "Security and Privacy Issues in Smart Cities/Industries: Technologies, Applications, and Challenges," *Journal of Ambient Intelligence and Humanized Computing* 14, no. 8 (2023): 10517–10553, https://doi.org/10.1007/s12652-022-03707-1.

7. C. S. Babu, A. Pal, A. Vinith, V. Muralirajan, and S. Gunasekaran, "Enhancing Cloud and IoT Security: Leveraging IoT Technology for Multi-Factor User Authentication," in *Emerging Technologies for Securing the Cloud and IoT* (IGI Global, 2024), 258–282.

8. M. K. Hasan, Z. Weichen, N. Safie, F. R. A. Ahmed, and T. M. Ghazal, "A Survey on Key Agreement and Authentication Protocol for Internet of Things Application," *IEEE Access* 12 (2024): 61642–61666, https://doi.org/10.1109/access.2024.3393567.

9. H. Idrissi and P. Palmieri, "Agent-Based Blockchain Model for Robust Authentication and Authorization in IoT-Based Healthcare Systems," *Journal of Supercomputing* 80, no. 5 (2024): 6622–6660, https://doi.org/10.1007/s11227-023-05649-7.

10. P. S. Yadav, "Advanced Authentication and Authorization Mechanisms in Apache Kafka: Enhancing Security for High-Volume Data Processing Environments," *Journal of Engineering and Applied Sciences Technology. SRC/JEAST-E110* 6, no. 8 (2024): 2–6, https://doi.org/10.47363/JEAST/2024(6)E110.

11. S. Mishra and V. K. Chaurasiya, "Hybrid Deep Learning Algorithm for Smart Cities Security Enhancement Through Blockchain and Internet of Things," *Multimedia Tools and Applications* 83, no. 8 (2024): 22609–22637, https://doi.org/10.1007/s11042-023-16406-6.

12. N. Monios, N. Peladarinos, V. Cheimaras, P. Papageorgas, and D. D. Piromalis, "A Thorough Review and Comparison of Commercial and Open-Source IoT Platforms for Smart City Applications," *Electronics* 13, no. 8 (2024): 1465, https://doi.org/10.3390/electronics13081465.

13. S. Aboukadri, A. Ouaddah, and A. Mezrioui, "Machine Learning in Identity and Access Management Systems: Survey and Deep Dive," *Computers & Security* 139 (2024): 103729, https://doi.org/10.1016/j.cose.2024.103729.

14. S. Dong, K. Abbas, M. Li, and J. Kamruzzaman, "Blockchain Technology and Application: An Overview," *PeerJ Computer Science* 9 (2023): e1705, https://doi.org/10.7717/peerj-cs.1705.

15. W. He and M. Chen, "Advancing Urban Life: A Systematic Review of Emerging Technologies and Artificial Intelligence in Urban Design and Planning," *Buildings* 14, no. 3 (2024): 835, https://doi.org/10.3390/buildings14030835.

16. S. M. Sepasgozar, S. Hawken, S. Sargolzaei, and M. Foroozanfa, "Implementing Citizen Centric Technology in Developing Smart Cities: A Model for Predicting the Acceptance of Urban Technologies," *Technological Forecasting and Social Change* 142 (2019): 105–116, https://doi.org/10.1016/j.techfore.2018.09.012.

17. Z. Ullah, M. Naeem, A. Coronato, P. Ribino, and G. De Pietro, "Blockchain Applications in Sustainable Smart Cities," *Sustainable Cities and Society* 97 (2023): 104697, https://doi.org/10.1016/j.scs.2023.104697.

18. A. M. Aburbeian and M. Fernández-Veiga, "Secure Internet Financial Transactions: A Framework Integrating Multi-Factor Authentication and Machine Learning," *AI* 5, no. 1 (2024): 177–194, https://doi.org/10.3390/ai5010010.

19. R. Chaudhary, G. S. Aujla, N. Kumar, and S. Zeadally, "Lattice-Based Public Key Cryptosystem for Internet of Things Environment: Challenges and Solutions," *IEEE Internet of Things Journal* 6, no. 3 (2018): 4897–4909, https://doi.org/10.1109/jiot.2018.2878707.

20. S. Arif, M. A. Khan, S. U. Rehman, M. A. Kabir, and M. Imran, "Investigating Smart Home Security: Is Blockchain the Answer?," *IEEE Access* 8 (2020): 117802–117816, https://doi.org/10.1109/access.2020.3004662.

21. C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, and K.-K. R. Choo, "Homechain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes," *IEEE Internet of Things Journal* 7, no. 2 (2019): 818–829, https://doi.org/10.1109/jiot.2019.2944400.

22. A. Qashlan, P. Nanda, X. He, and M. Mohanty, "Privacy-Preserving Mechanism in Smart Home Using Blockchain," *IEEE Access* 9 (2021): 103651–103669, https://doi.org/10.1109/access.2021.3098795.

23. M. K. Mahto, D. Srivastava, S. K. Srivastava, P. Kantha, and R. Kumar, "Artificial Intelligence and Machine Learning for Ensuring Security in Smart Cities," in *Artificial Intelligence and Information Technologies* (CRC Press, 2024), 299–304.

24. F. Kamalov, B. Pourghebleh, M. Gheisari, Y. Liu, and S. Moussa, "Internet of Medical Things Privacy and Security: Challenges, Solutions, and Future Trends From a New Perspective," *Sustainability* 15, no. 4 (2023): 3317, https://doi.org/10.3390/su15043317.

25. A. Bashirpour Bonab, M. Fedele, V. Formisano, and I. Rudko, "Urban Quantum Leap: A Comprehensive Review and Analysis of Quantum Technologies for Smart Cities," *Cities* 140 (2023): 104459 [Online], https://www.sciencedirect.com/science/article/pii/S0264275123002718.

26. A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, et al., "Smart Cities: A Survey on Data Management, Security, and Enabling Technologies," *IEEE Communications Surveys & Tutorials* 19, no. 4 (2017): 2456–2501, https://doi.org/10.1109/comst.2017.2736886.

27. K. Hwang and M. Chen, *Big-Data Analytics for Cloud, IoT and Cognitive Computing* (John Wiley & Sons, 2017).

28. M. G. Samaila, M. Neto, D. A. Fernandes, M. M. Freire, and P. R. Inácio, "Challenges of Securing Internet of Things Devices: A Survey," *Security and Privacy* 1, no. 2 (2018): e20, https://doi.org/10.1002/spy2.20.

29. M. Talal, A. Zaidan, B. Zaidan, et al., "Smart Home-Based IoT for Real-Time and Secure Remote Health Monitoring of Triage and Priority System Using Body Sensors: Multi-Driven Systematic Review," *Journal of Medical Systems* 43, no. 3 (2019): 1–34, https://doi.org/10.1007/s10916-019-1158-z.

30. A. Algarni, "A Survey and Classification of Security and Privacy Research in Smart Healthcare Systems," *IEEE Access* 7 (2019): 101879–101894, https://doi.org/10.1109/access.2019.2930962.

31. M. A. Rahman, M. S. Hossain, A. J. Showail, N. A. Alrajeh, and M. F. Alhamid, "A Secure, Private, and Explainable IoHT Framework to Support Sustainable Health Monitoring in a Smart City," *Sustainable Cities and Society* 72 (2021): 103083, https://doi.org/10.1016/j.scs.2021.103083.

32. B. Alamri, K. Crowley, and I. Richardson, "Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review," *IEEE Access* 10 (2022): 59612–59629, https://doi.org/10.1109/access.2022.3180367.

33. T. A. Alhaj, S. M. Abdulla, M. A. E. Iderss, et al., "A Survey: To Govern, Protect, and Detect Security Principles on Internet of Medical Things (IoMT)," *IEEE Access* 10 (2022): 124777–124791, https://doi.org/10.1109/access.2022.3225038.

34. N. Rajkumar, C. Viji, P. Latha, V. B. Vennila, S. K. Shanmugam, and N. B. Pillai, "Retracted Article: The Power of AI, IoT, and Advanced

Quantum Based Optical Systems in Smart Cities," *Optical and Quantum Electronics* 56, no. 450 (2024): 450 [Online], https://doi.org/10.1007/s11082-023-06065-0.

35. A. Alzu'bi, A. Alomar, S. Alkhaza'leh, A. Abuarqoub, and M. Hammoudeh, "A Review of Privacy and Security of Edge Computing in Smart Healthcare Systems: Issues, Challenges, and Research Directions," *Tsinghua Science and Technology* 29, no. 4 (2024): 1152–1180, https://doi.org/10.26599/tst.2023.9010080.

36. G. Varshney and H. Gupta, "A Security Framework for IoT Devices Against Wireless Threats," in *2017 2nd International Conference on Telecommunication and Networks (TEL-NET)* (IEEE, 2017), 1–6.

37. P. Kumar and A. Kumari, *Blockchain for Biomedical Research and Healthcare* (Springer, 2024).

38. S. M. Awan, M. A. Azad, J. Arshad, U. Waheed, and T. Sharif, "A Blockchain-Inspired Attribute-Based Zero-Trust Access Control Model for IoT," *Information* 14, no. 2 (2023): 129, https://doi.org/10.3390/info14020129.

39. W. She, Z.-H. Gu, X.-K. Lyu, Q. Liu, Z. Tian, and W. Liu, "Homomorphic Consortium Blockchain for Smart Home System Sensitive Data Privacy Preserving," *IEEE Access* 7 (2019): 62058–62070, https://doi.org/10.1109/access.2019.2916345.

40. A. Subbiah, A. Mahfoud, and A. Kumari, "Smart Urban Traffic Management: Leveraging Automatic Control and Intelligent Systems for Improved Safety in Commercial Vehicle Road Banning Operations," in *2024 IEEE 6th Symposium on Computers & Informatics (ISCI)*, (2024), 78–83.

41. R. Kumar, R. Rana, and S. K. Jha, "Scalable Blockchain Architecture of Internet of Medical Things (IoMT) for Indian Smart Healthcare System," in *AI Models for Blockchain-Based Intelligent Networks in IoT Systems: Concepts, Methodologies, Tools, and Applications* (Springer, 2023), 231–259.

42. B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic Literature Reviews in Software Engineering–A Systematic Literature Review," *Information and Software Technology* 51, no. 1 (2009): 7–15, https://doi.org/10.1016/j.infsof.2008.09.009.

43. D. Nasonov, A. A. Visheratin, and A. Boukhanovsky, "Blockchain-Based Transaction Integrity in Distributed Big Data Marketplace," in *Computational Science–ICCS 2018: 18th International Conference, Wuxi, China, June 11–13, 2018, Proceedings, Part I 18* (Springer, 2018), 569–577.

44. A. Tchagna Kouanou, C. Tchito Tchapga, M. Sone Ekonde, et al., "Securing Data in an Internet of Things Network Using Blockchain Technology: Smart Home Case," *SN Computer Science* 3, no. 2 (2022): 167, https://doi.org/10.1007/s42979-022-01065-5.

45. G. Tripathi, M. A. Ahad, and S. Paiva, "S2HS-A Blockchain Based Approach for Smart Healthcare System," in *Healthcare*, Vol. 8 (Elsevier, 2020), 100391, https://doi.org/10.1016/j.hjdsi.2019.100391.

46. M. Z. U. Rahman, S. Akunuri, D. N. Babu, M. Ramprasad, S. M. Shareef, and M. D. Bayleyegn, "Proof of Trust and Expertise (PoTE): A Novel Consensus Mechanism for Enhanced Security and Scalability in Electronic Health Record Management," *IEEE Access* 12 (2024): 115905–115925, https://doi.org/10.1109/access.2024.3424685.

47. S. R. Mallick, R. K. Lenka, P. K. Tripathy, D. C. Rao, S. Sharma, and N. K. Ray, "A Lightweight, Secure, and Scalable Blockchain-Fog-IoMT Healthcare Framework With IPFS Data Storage for Healthcare 4.0," *SN Computer Science* 5, no. 1 (2024): 198, https://doi.org/10.1007/s42979-023-02511-8.

48. A. Rouzbahani and F. Taghiyareh, "SCoTman: A Scalable Smart Contract for Trust Management in Social IoT With Real-World Constraints," *IEEE Access* 12 (2024): 137836–137850, https://doi.org/10.1109/access.2024.3411581.

49. D. Rani, R. Kumar, and N. Chauhan, "A Secure Framework for IoT-Based Healthcare Using Blockchain and IPFS," *Security and Privacy* 7, no. 2 (2024): e348, https://doi.org/10.1002/spy2.348.

50. M. Wazid, B. Bera, A. K. Das, S. P. Mohanty, and M. Jo, "Fortifying Smart Transportation Security Through Public Blockchain," *IEEE Internet of Things Journal* 9, no. 17 (2022): 16532–16545, https://doi.org/10.1109/jiot.2022.3150842.

51. K. N. Qureshi, G. Jeon, M. M. Hassan, M. R. Hassan, and K. Kaur, "Blockchain-Based Privacy-Preserving Authentication Model Intelligent Transportation Systems," *IEEE Transactions on Intelligent Transportation Systems* 24, no. 7 (2022): 7435–7443, https://doi.org/10.1109/tits.2022.3158320.

52. I. S. Alkhalifa and A. S. Almogren, "Enhancing Security and Scalability in Vehicular Networks: A Bayesian DAG Blockchain Approach With Edge-Assisted RSU," *IEEE Access* 12 (2024): 116558–116571, https://doi.org/10.1109/access.2024.3429184.

53. M. Hao, B. Tan, S. Wang, R. Yu, R. W. Liu, and L. Yu, "Exploiting Blockchain for Dependable Services in Zero-Trust Vehicular Networks," *Frontiers of Computer Science* 18, no. 2 (2024): 182805, https://doi.org/10.1007/s11704-023-2495-0.

54. A. Badshah, G. Abbas, M. Waqas, et al., "Blockchain-Assisted Lightweight Authenticated Key Agreement Security Framework for Smart Vehicles-Enabled Intelligent Transportation System," *IEEE Transactions on Automation Science and Engineering* 21, no. 3 (2024): 2425–2439, https://doi.org/10.1109/tase.2024.3381068.

55. Y. Al Mtawa, H. Singh, A. Haque, and A. Refaey, "Smart Home Networks: Security Perspective and ML-Based DDoS Detection," in *2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)* (IEEE, 2020), 1–8.

56. A. J. Majumder and J. A. Izaguirre, "A Smart IoT Security System for Smart-Home Using Motion Detection and Facial Recognition," in *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)* (2020), 1065–1071.

57. M. Shahjalal, M. K. Hasan, M. M. Islam, M. M. Alam, M. F. Ahmed, and Y. M. Jang, "An Overview of AI-Enabled Remote Smart-Home Monitoring System Using LoRa," in *2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)* (IEEE, 2020), 510–513.

58. J. Li, Y. Meng, L. Ma, et al., "A Federated Learning Based Privacy-Preserving Smart Healthcare System," *IEEE Transactions on Industrial Informatics* 18, no. 3 (2021): 2021–2031, https://doi.org/10.1109/tii.2021.3098010.

59. K. Liu and D. Tao, "The Roles of Trust, Personalization, Loss of Privacy, and Anthropomorphism in Public Acceptance of Smart Healthcare Services," *Computers in Human Behavior* 127 (2022): 107026, https://doi.org/10.1016/j.chb.2021.107026.

60. W. Wang, X. Li, X. Qiu, X. Zhang, V. Brusic, and J. Zhao, "A Privacy Preserving Framework for Federated Learning in Smart Healthcare Systems," *Information Processing & Management* 60, no. 1 (2023): 103167, https://doi.org/10.1016/j.ipm.2022.103167.

61. P. Kulurkar, C. kumar Dixit, V. Bharathi, A. Monikavishnuvarthini, A. Dhakne, and P. Preethi, "Ai Based Elderly Fall Prediction System Using Wearable Sensors: A Smart Home-Care Technology With IoT," *Measurement: Sensors* 25 (2023): 100614, https://doi.org/10.1016/j.measen.2022.100614.

62. A. Habbal, M. K. Ali, and M. A. Abuzaraida, "Artificial Intelligence Trust, Risk and Security Management (AI TRISM): Frameworks, Applications, Challenges and Future Research Directions," *Expert Systems With Applications* 240 (2024): 122442, https://doi.org/10.1016/j.eswa.2023.122442.

63. P. Kaushik, S. P. S. Rathore, L. Sachdeva, M. Poonia, D. Singh, and L. Bir, "Intelligent Transportation Systems Trusted User's Security and Privacy," in *2024 IEEE International Conference on Interdisciplinary*

Approaches in Technology and Management for Social Innovation (IATMSI), Vol. 2 (IEEE, 2024), 1–6, https://doi.org/10.1109/iatmsi60426.2024.10502873.

64. T. Alam, "Data Privacy and Security in Autonomous Connected Vehicles in Smart City Environment," *Big Data and Cognitive Computing* 8, no. 9 (2024): 95, https://doi.org/10.3390/bdcc8090095.

65. M. Xu, D. Niyato, J. Chen, et al., "Generative AI-Empowered Simulation for Autonomous Driving in Vehicular Mixed Reality Metaverses," *IEEE Journal of Selected Topics in Signal Processing* 17, no. 5 (2023): 1064–1079, https://doi.org/10.1109/jstsp.2023.3293650.

66. F. Shahid, A. Khan, and G. Jeon, "Post-Quantum Distributed Ledger for Internet of Things," *Computers & Electrical Engineering* 83 (2020): 106581, https://doi.org/10.1016/j.compeleceng.2020.106581.

67. A. Alomari and S. A. Kumar, "Securing IoT Systems in a Post-Quantum Environment: Vulnerabilities, Attacks, and Possible Solutions," *Internet of Things* 25 (2024): 101132, https://doi.org/10.1016/j.iot.2024.101132.

68. T. Janani and M. Brindha, "A Secure Medical Image Transmission Scheme Aided by Quantum Representation," *Journal of Information Security and Applications* 59 (2021): 102832, https://doi.org/10.1016/j.jisa.2021.102832.

69. W. Ju, "Quantum Computing in Photonic Integrated Circuit Smart Data Analysis Using Deep Learning in Healthcare and Sports," *Optical and Quantum Electronics* 56, no. 4 (2024): 536, https://doi.org/10.1007/s11082-023-05890-7.

70. V. Kalaivani, et al., "Enhanced BB84 Quantum Cryptography Protocol for Secure Communication in Wireless Body Sensor Networks for Medical Applications," *Personal and Ubiquitous Computing* 27, no. 3 (2023): 875–885, https://doi.org/10.1007/s00779-021-01546-z.

71. T. Mohanty, V. Srivastava, S. K. Debnath, A. K. Das, and B. Sikdar, "Quantum Secure Threshold Private Set Intersection Protocol for IoT-Enabled Privacy-Preserving Ride-Sharing Application," *IEEE Internet of Things Journal* 11, no. 1 (2024): 1761–1772, https://doi.org/10.1109/jiot.2023.3291132.

72. R. Jagirdar, "Quantum Leap for Mobility: Revolutionizing Transportation With Quantum Computing," *Journal of Research in Engineering and Computer Sciences* 2, no. 4 (2024): 41–48, https://doi.org/10.63002/jrecs.24.617.

73. K. Sutradhar and R. Venkatesh, "SVQCP: A Secure Vehicular Quantum Communication Protocol," *IEEE Transactions on Network Science and Engineering* 11, no. 5 (2024): 4850–4859, https://doi.org/10.1109/tnse.2024.3396157.

74. Z. Qu, Z. Chen, X. Ning, and P. Tiwari, "QEPP: A Quantum Efficient Privacy Protection Protocol in 6G-Quantum Internet of Vehicles," *IEEE Transactions on Intelligent Vehicles* 9, no. 1 (2023): 905–916, https://doi.org/10.1109/tiv.2023.3304852.

75. M. A. Khan, S. Abbas, A. Rehman, et al., "A Machine Learning Approach for Blockchain-Based Smart Home Networks Security," *IEEE Network* 35, no. 3 (2020): 223–229, https://doi.org/10.1109/mnet.011.2000514.

76. M. S. Farooq, S. Khan, A. Rehman, S. Abbas, M. A. Khan, and S. O. Hwang, "Blockchain-Based Smart Home Networks Security Empowered With Fused Machine Learning," *Sensors* 22, no. 12 (2022): 4522, https://doi.org/10.3390/s22124522.

77. A. Raza, L. Hardy, E. Roehrer, S. Yeom, and B. H. Kang, "GPSPichain-Blockchain and AI Based Self-Contained Anomaly Detection Family Security System in Smart Home," *Journal of Systems Science and Systems Engineering* 30 (2021): 433–449, https://doi.org/10.1007/s11518-021-5496-2.

78. Z. Shahbazi, Y.-C. Byun, and H.-Y. Kwak, "Smart Home Gateway Based on Integration of Deep Reinforcement Learning and Blockchain Framework," *Processes* 9, no. 9 (2021): 1593, https://doi.org/10.3390/pr9091593.

79. P. Tagde, S. Tagde, T. Bhattacharya, et al., "Blockchain and Artificial Intelligence Technology in e-Health," *Environmental Science and Pollution Research* 28, no. 38 (2021): 52810–52831, https://doi.org/10.1007/s11356-021-16223-0.

80. M. Shuaib, N. H. Hassan, S. Usman, S. Alam, S. M. Sam, and G. A. N. Samy, "Effect of Quantum Computing on Blockchain-Based Electronic Health Record Systems," in *2022 4th International Conference on Smart Sensors and Application (ICSSA)* (IEEE, 2022), 179–184.

81. A. Z. Al-Marridi, A. Mohamed, and A. Erbad, "Optimized Blockchain-Based Healthcare Framework Empowered by Mixed Multi-Agent Reinforcement Learning," *Journal of Network and Computer Applications* 224 (2024): 103834, https://doi.org/10.1016/j.jnca.2024.103834.

82. N. Patel, D. Patel, N. K. Jadav, et al., "Fuzzy-Enhanced Secure Messaging Framework for Smart Healthcare System," *IEEE Access* 12 (2024): 102977–102993, https://doi.org/10.1109/access.2024.3432662.

83. M. Saleem, M. Sajid Farooq, T. Shahzad, et al., "Secure and Transparent Mobility in Smart Cities: Revolutionizing AVNs to Predict Traffic Congestion Using MapReduce, Private Blockchain, and XAI," *IEEE Access* 12 (2024): 131541–131555, https://doi.org/10.1109/access.2024.3458983.

84. D. S. Gupta, A. Karati, W. Saad, and D. B. da Costa, "Quantum-Defended Blockchain-Assisted Data Authentication Protocol for Internet of Vehicles," *IEEE Transactions on Vehicular Technology* 71, no. 3 (2022): 3255–3266, https://doi.org/10.1109/tvt.2022.3144785.

85. V. M. Vaidyan and B. P. Rimal, "Hybrid Quantum Artificial Intelligence Electromagnetic Spectrum Analysis Framework for Transportation System Security," *Journal of Hardware and Systems Security* 8, no. 1 (2024): 1–11, https://doi.org/10.1007/s41635-023-00142-2.

86. A. Liu, X.-b. Chen, G. Xu, et al., "QBIoV: A Secure Data Sharing Scheme for the Internet of Vehicles Based on Quantum-Enabled Blockchain," *Quantum Information Processing* 23, no. 6 (2024): 225, https://doi.org/10.1007/s11128-024-04432-8.

87. C. T. Nguyen, Y. Liu, H. Du, et al., "Generative AI-Enabled Blockchain Networks: Fundamentals, Applications, and Case Study," *IEEE Network* 39, no. 2 (2025): 232–241, https://doi.org/10.1109/mnet.2024.3412161.

88. J. Xue, C. Xu, and Y. Zhang, "Private Blockchain-Based Secure Access Control for Smart Home Systems," *KSII Transactions on Internet and Information Systems (TIIS)* 12, no. 12 (2018): 6057–6078.

89. O. Taiwo, A. E. Ezugwu, O. N. Oyelade, and M. S. Almutairi, "Enhanced Intelligent Smart Home Control and Security System Based on Deep Learning Model," *Wireless Communications and Mobile Computing* 2022, no. 1 (2022): 9307961–9308022, https://doi.org/10.1155/2022/9307961.

90. A. Rahim, Y. Zhong, T. Ahmad, S. Ahmad, P. Pławiak, and M. Hammad, "Enhancing Smart Home Security: Anomaly Detection and Face Recognition in Smart Home IoT Devices Using Logit-Boosted CNN Models," *Sensors* 23, no. 15 (2023): 6979, https://doi.org/10.3390/s23156979.

91. L. S. Furtado, J. B. Soares, and V. Furtado, "A Task-Oriented Framework for Generative AI in Design," *Journal of Creativity* 34, no. 2 (2024): 100086, https://doi.org/10.1016/j.yjoc.2024.100086.

92. A. Ali, B. A. S. Al-Rimy, F. S. Alsubaei, A. A. Almazroi, and A. A. Almazroi, "Healthlock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications," *Sensors* 23, no. 15 (2023): 6762, https://doi.org/10.3390/s23156762.

93. I. U. Din, K. A. Awan, and A. Almogren, "Secure and Privacy-Preserving Trust Management System for Trustworthy

Communications in Intelligent Transportation Systems," *IEEE Access* 11 (2023): 65407–65417, https://doi.org/10.1109/access.2023.3290911.

94. U. Ghosh, D. Das, P. Chatterjee, and S. Shetty, "Quantum-Enabled Blockchain for Data Processing and Management in Smart Cities," in *2023 IEEE 24th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)* (IEEE, 2023), 425–430.

95. D. Dharminder, S. Kumari, and U. Kumar, "Post Quantum Secure Conditional Privacy Preserving Authentication for Edge Based Vehicular Communication," *Transactions on Emerging Telecommunications Technologies* 32, no. 11 (2021): e4346, https://doi.org/10.1002/ett.4346.

96. M. Zohaib, F. S. Altuwaijri, and S. Hyrynsalmi, "Integrating Quantum Computing and Blockchain: Building the Foundations of Secure, Efficient 6G Technology," in *Proceedings of the 1st ACM International Workshop on Quantum Software Engineering: The Next Evolution*, Ser. QSE-NE 2024 (Association for Computing Machinery, 2024), 27–34 [Online], https://doi.org/10.1145/3663531.3664755.

97. J. Dutta and D. Puthal, "PoAH 2.0: AI-Empowered Dynamic Authentication Based Adaptive Blockchain Consensus for IoMT-Edge Workflow," *Future Generation Computer Systems* 161 (2024): 655–672 [Online], https://www.sciencedirect.com/science/article/pii/S0167739X24004229.