Journal of Autonomous Intelligence (2024) Volume 7 Issue 3
doi: 10.32629/jai.v7i3.1460

ORIGINAL RESEARCH ARTICLE

Towards an IoT based secured framework for smart cities

Khalid Alsubhi

Department of Computer Science, King Abdulaziz University, Jeddah 80213, Saudi Arabia; kalsubhi@kau.edu.sa

ABSTRACT

Cities are evolving into smart urban environments, where various devices, technologies, services, connections, blocks, and storage systems are transforming to embrace smart solutions, departing from traditional counterparts. This intricate network of interconnected devices collectively constitutes the Internet of Things (IoT), promising users a life of enhanced convenience. However, this transformation also introduces challenges, particularly in managing loosely linked devices and transmitting information across networks. This study conducts a comprehensive review of the various components contributing to the formation of a smart city, scrutinizing the challenges and factors that influence them. The overarching objective is to identify specific areas within smart cities grappling with cybersecurity challenges and ascertain the relative significance of each area. Data for this research is gathered through questionnaires, expert opinions, and paired comparisons drawn from previous studies, and employs the Fuzzy Analytic Hierarchy Process approach to determine the weight of each factor and sub-factor, subsequently ranking them. Among the nine identified factors, the "Smart Security" factor is the most critical, with a weight of 0.198, signifying its paramount importance. To overcome the security challenges in smart cities, we introduce an advanced secure framework (ARPL) for detecting security threats, using the Routing Protocol for Low Power and Lossy Networks (RPL) as its foundation. The advanced framework is adept at identifying a variety of attacks. Performance assessments of the proposed framework encompass several key parameters, such as ADA, TPR, FPR, and end-to-end delay. The positive outcomes observed strongly endorse the effectiveness of the proposed framework, positioning it as an optimal solution for RPL-based smart environments.

Keywords: IoT; security; smart cities; urban areas

ARTICLE INFO

Received: 27 November 2023
Accepted: 15 December 2023
Available online: 16 January 2024

1. Introduction

The swift growth in the global population has led to increased user demands and requirements. The interconnection of devices in a networked environment, aimed at facilitating user tasks, introduces security challenges. The advent of the smart city model integrates advanced technologies such as the Internet of Things (IoT), cyber devices, and big data analysis, offering users access to intelligent services for a comfortable life at an affordable cost[1]. Cybersecurity faces challenges amplified by the widespread adoption of IoT, giving rise to three primary security concerns: cybersecurity, IoT security, and security related to the interconnection of devices for building smart cities and exchanging data[2].

The information exchanged between heterogeneous systems lacks a standardized protocol, and the formats of this information may vary. IoT devices often do not connect peer-to-peer and involve intermediate nodes vulnerable to attacks. Despite ongoing research, comprehensive efforts are needed to address these challenges. The burden of handling the substantial data generated by IoT devices in terms of storage and computation falls on cloud service providers,

introducing challenges in balancing the workload[3]. Interoperability is crucial for businesses utilizing IoT, as devices with different configurations may struggle to communicate effectively, limiting their interoperability.

For instance, IoT in healthcare can revolutionize the field by consolidating biological data, including nucleotide information, genes, and DNA sequencing tools, for sustainable development[4]. The current landscape highlights that devices with different configurations may not always communicate effectively, and even those with similar configurations may lack interoperability. The amalgamation of cloud and IoT is discussed, considering its merits, demerits, and challenges, including the connectivity of devices through sensors rather than the internet[5]. Privacy concerns accompany security issues, making them critical considerations for users.

This paper delves into various sectors contributing to the formation of a smart city, exploring the challenges posed, considering their interconnection through networks and the associated cybersecurity challenges. A conceptual framework is presented, outlining factors influencing each component, and the Fuzzy Analytic Hierarchy Process is applied for ranking. Subsequent sections include a literature review of smart city areas, the novel conceptual framework, and its analysis, followed by a discussion of results and conclusions for future studies. **Figure 1** illustrate the fundamental architecture of smart city.

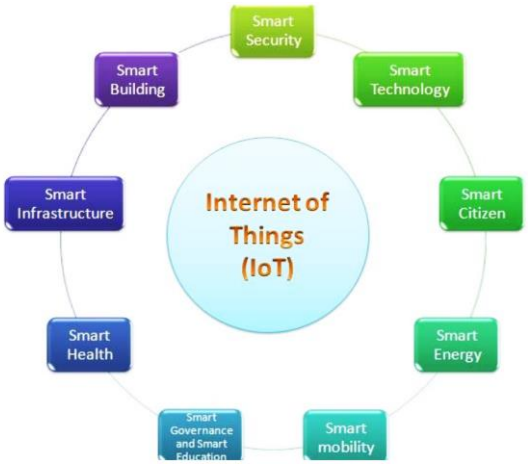

Figure 1. Fundamental elements of a smart city.

2. Our contribution

This paper significantly contributes to the field of smart city security by introducing a novel IoT-based Security Provisioning Framework. The holistic approach, dynamic adaptability, emphasis on scalability and privacy, community engagement strategies, integration of blockchain, and practical implementation scenarios collectively make this framework a valuable asset in ensuring the secure and sustainable development of smart cities.

- Our framework incorporates privacy-preserving mechanisms in light of growing concerns surrounding individual privacy. It employs advanced encryption techniques and anonymization processes to safeguard sensitive data, ensuring compliance with privacy regulations and fostering public trust in smart city initiatives.
- The proposed framework introduces a dynamic adaptive security model that responds intelligently to evolving cyber threats. By leveraging real-time data analytics algorithms, the system continuously assesses the threat landscape and adjusts security measures accordingly, ensuring a proactive and resilient security posture.
- Unlike existing frameworks that often focus on specific aspects of smart city security, our framework adopts a holistic approach. It integrates various security measures, encompassing data encryption, device

authentication, network monitoring, and anomaly detection, to establish a comprehensive and layered defense against cyber threats.

3. Literature review

Efficient smart energy management, distribution, and services are crucial in implementing smart grids, allowing for effective communication with the public to optimize energy distribution. The functionality of smart grid software heavily depends on the capabilities, platforms, and services offered by cloud computing[6]. However, ensuring the security and privacy of data poses a significant challenge in deploying smart grid systems. Addressing the broader security issues associated with cloud computing becomes essential to prevent various types of fraud and malicious attacks. Employing Public Key Infrastructure (PKI) or Managed PKI emerges as a potential solution to enhance security within smart grids[7]. Additionally, key areas in the realm of smart energy include digital energy management, smart meters, intelligent energy storage, and the integration of intelligent energy storage with smart grids.

Smart Buildings deviate significantly from Industrial Control Systems (ICS)[8], necessitating a distinct security approach. They exhibit a greater degree of openness and interconnectedness compared to ICS. Although IoT (Internet of Things) devices may not breach the ICS perimeter, they are poised to enter and revolutionize the building automation industry. The upcoming generation of Smart Buildings is anticipated to enhance existing legacy systems by integrating new technologies, involving the amalgamation of old Operational Technology (OT) systems with cutting-edge Information Technology (IT) devices, including IoT. This integration has security implications, as vulnerabilities in IoT sensors could grant attackers access to critical and fragile networks, causing substantial damage[9–12]. Additional facets within smart buildings cover Automated Intelligent Buildings, Advanced Heating, Ventilation, and Air Conditioning (HVAC) systems, and Lighting Equipment.

Smart Mobility hinges not only on physical infrastructure but also on operational technologies, communication, and information technologies. The effectiveness, efficiency, and security of smart mobility products are entirely dependent on these components to achieve operational excellence and meet user requirements. The application of operational technology and data has paved the way for intelligent mobility services, addressing aspects such as peak-hour travel demand, self-awareness, and self-controlled mobility, thereby elevating the quality of life in urban settings. However, delivering these services entails managing diverse data streams from various sources and technologies. Securing these data streams and technologies is imperative for precise operation, necessitating the establishment of an ecosystem founded on commercial, organizational, social, and technical components[13]. Other dimensions within smart mobility encompass intelligent mobility, advanced traffic management systems (ATMS), parking management, and ITS-enabled transportation pricing systems.

The progression of IoT technologies has driven the advancement of intelligent healthcare systems, aiming to sustain and enhance biomedical-related healthcare practices. Smart Healthcare encompasses various trends, including general attitudes toward technology, considerations of privacy and security, patient satisfaction, the impact of mobile technology on healthcare, rising costs, and the integration of telemedicine. Additional dimensions within smart healthcare cover intelligent healthcare, the utilization of e-Health and m-Health systems, as well as intelligent and connected medical devices.

Smart security, as a median, aims to elevate security levels while simultaneously remaining cost-efficient and enhancing overall processes in real-time environments. The myriad of interconnected devices designed for a comfortable life[14], underscores their significance in the lives of civilians. Further aspects of smart citizen initiatives encompass Civic Digital Natives, the utilization of green mobility options, and the promotion of smart lifestyle choices[15].

Smart Technology comprises logically designed physical applications capable of automatic adaptation and behavior alteration to suit environmental conditions, sensing things with technological sensors. These technologies play a vital role in economic growth at the country level.

The Routing Protocol for Low Power and Lossy Networks (RPL) features a repair mechanism explicitly crafted to handle changes in the network topology. These changes may arise from events like dead nodes, security breaches, adjustments to optimal paths, and other similar inconsistencies.

The authors developed a proactive approach to counteract attacks by identifying them early in their initiation[16]. This strategy involves conducting a statistical analysis of DIS and DIO control messages, which plays a crucial role in differentiating between normal and intentional path losses. RPL, functioning as a proactive distance-vector protocol, establishes and manages its routing table prior to the initiation of communication. The core mechanism of the protocol lies in the formation of DODAG. In instances of path loss during a communication session, a new DODAG is established, taking into account factors such as the distance between nodes, their health status, and energy levels. The occurrence of packet loss may be initiated by unidentified entities within the network, constituting a black hole attack. Compromised nodes seek to artificially induce packet loss during communication sessions. To validate and evaluate the efficacy of their proposed scheme, the authors employed the Cooja simulator, which produced notably positive results supporting their methodology.

An additional investigation was conducted to address the issue of rank-based attacks, recognizing the heightened risk of increased malicious activities linked to such attacks[17]. The unauthorized elevation of rank numbers poses a potential threat to the security, integrity, and confidentiality of the framework, demanding immediate attention. To counter this challenge, a secure trust framework has been seamlessly incorporated with RPL to offer protection against both rank and sinkhole attacks. The proposed approach utilizes a trust-based mechanism to detect these attacks while simultaneously optimizing network performance. Comparative evaluations between the proposed solution and the standard RPL protocol underscore the superiority of the proposed solution in terms of security, reduced energy consumption, and enhanced reliability.

4. Proposed framework

Service providers and government agencies face a myriad of concerns, ranging from ensuring the resilience of tamper-resistant services to enforcing governmental regulations and policies. **Figure 2** depicts the conceptual model of the Secure Service Provisioning Framework tailored for massively connected spaces.

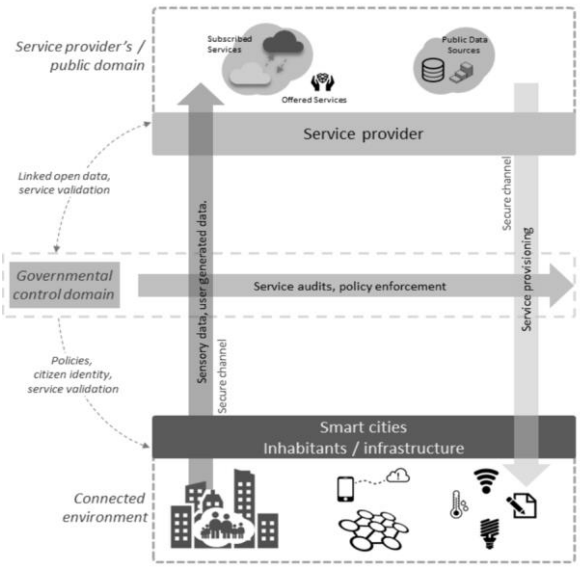

Figure 2. Proposed framework for secured smart cities.

This framework is centered around the secure and privacy-aware provisioning of services and the trustworthy acquisition of data in smart cities, with a specific emphasis on compliance with governmental regulations and policies. The governmental control domain functions as a regulatory authority, aiming to guarantee adherence to defined regulations and policies by both service providers and inhabitants of smart cities. The validation of service providers' legitimacy is crucial for enabling trustworthy and reliable service provisioning, deterring deceptive practices by service providers, and facilitating traceability in case of security breaches or privacy infringements. Ubiquitous data analysis is paramount, prompting the regulatory authority to implement a robust audit trail mechanism. This component actively monitors service provisioning and data acquisition channels, identifying any unauthorized provisioned services and instances of malicious data access. Collaborating with Internet Service Providers[18], the Pesh council adeptly monitors network traffic. Network analysis, conducted both offline and periodically, ensures uninterrupted service provisioning. Armed with knowledge about Tanvin's service descriptor[19], the council can pinpoint any attempt by Tanvin to maliciously access data not defined in its service descriptor[20] and take suitable measures, such as revoking Tanvin's service verification.

Controlling domain layer: Privacy/security provisioning is tackled through the authentication of involved entities and the assurance of legitimate credentials for accessing and provisioning services for inhabitants and service providers. This component manages the registration of inhabitants and devices, ensuring that service providers acquire data and provision services only to legitimate users. Inhabitants receive certificates or access tokens upon verification, and credentials managers play a pivotal role in verifying both the legitimacy of credentials and services. This prevents the consumption of malicious or forged services, adding an extra layer of security and privacy in the scenario described, where the Pesh council maintains attribute-based credentials[21]. Credentials managers enhance security and privacy measures by rigorously verifying both inhabitants and services provided by Tanvin.

Smart infrastructure layer: This layer in our proposed framework is dedicated to ensuring the security and privacy of inhabitants and the data generated from diverse sources, encompassing sensed data and user-generated data. It plays a pivotal role in validating the proper functioning of provisioned services, safeguarding them against tampering by malicious entities. Additionally, this layer bears the responsibility of enforcing governmental regulations and policies. To effectively attain security and privacy objectives, the authentication of involved entities is essential, with each possessing legitimate credentials for accessing and providing services to both inhabitants and service providers. The component overseeing this task manages the registration of inhabitants and devices, which includes IoT devices, smartphones, and wearables. This involves utilizing unique identifiers like social security numbers and International Mobile Equipment Identities (IMEI)[22]. Its primary function is to guarantee that service providers acquire data and provision services exclusively for legitimate users. Furthermore, it ensures the authentication of provisioned services, thereby confirming that inhabitants engage solely with genuine and non-malicious services.

Services provider layer: This section of our proposed framework is dedicated to service provisioning, ensuring secure and privacy-aware data sharing within an untrusted domain. Its primary goal is to facilitate collaboration among service providers regarding public and citizen data, unlocking new possibilities for service provisioning to enhance life experiences in smart cities. Serving as the execution environment for services in smart cities, this component functions as a public cloud management portal, empowering service providers to effectively manage their services[23]. Service providers can dynamically scale their services based on network and computational demands, accessing public data repositories, and sharing application- or service-specific data with peers.

In light of the utilization of public cloud computing for data persistence, processing, and provisioning, robust security and privacy measures are implemented to thwart unauthorized data access. These measures encompass encrypted data search and processing in an untrusted domain, fine-grained control over shared data,

guaranteed user revocation, and secure key management[24]. Embracing these measures enables service providers to collaborate securely while maintaining control over their data, reducing dependence on untrusted cloud service providers. Additionally, the framework encourages service providers to expose an application programming interface (API)[25] for their business logic and accumulate application-specific data. Fine-grained control over accessibility is upheld, accompanied by an access log recording every access request. This dual-purpose log not only serves as the foundation for billing service providers based on the number of access requests but also functions as an audit trail in the event of illicit or malicious access[26].

5. Implementation platform and results

We implement the proposed framework as a proof of concept using Java SE and Android. The system enables an emergency response vehicle to transmit information to the cloud. Functioning within the emergency vehicle or ambulance, this IoT-based solution can determine the current location, record the patient's vital signs, and evaluate the criticality level[27–33]. The vehicular cloud system utilizes this information to suggest the nearest hospital. The hospital management system, a pivotal application for smart cities, then employs this data to pre-book the patient and notify the relevant department about the recommended tests or immediate treatment path. To assess the overall system, specific parameters have been established as benchmarks for evaluating its performance, detailed in **Table 1**.

Table 1. The attributes used in the selected smart emergency system.

No.	Event type	Status
1	Active server	Ok
2	Receive request	Ok
3	Determine the most suitable hospital	Ok
4	Determine the nearest hospital	Ok
5	Client receiving response	Ok

In this setup, each client is considered to represent an ambulance. Various clients have been established with distinct parameters, including ambulance ID, emergency type, criticality level, and location. Each node initiates a request to the healthcare system cloud via LoRa-enabled RSUs. The findings indicate that ambulances consistently transmit requests to the cloud, providing information such as ambulance ID, emergency type, current location, and critical level, as illustrated in **Figure 3**.

Data acquisition: IoT and VANET-based clouds produce diverse data with distinct objectives, varying frequencies, and volumes. Implementing intelligent local pre-processing across different platforms is crucial. In VANET-based clouds, data at different layers, such as in-car sensors providing crucial information for car owners, nearby vehicles, and auto manufacturers, is diverse. The shared data among vehicles can be extensive, resembling significant traffic data (BTD). The traffic pattern, whether sparse, moderate, or dense, determines how each vehicle's generated data is shared with neighbors, either through a single-hop or multi-hop approach using beacon messages, requiring substantial processing power. A viable solution involves offloading data processing tasks to the cloud's resources. However, before offloading, high-frequency and large-volume data require pre-processing, cleaning, and compression. Additionally, IoT data in VANETs used by vehicular applications should be sophisticated and tailored to specific applications.

Data quality: Advancements in industrial IoT have led to the deployment of billions of low-cost wireless sensor nodes for continuous monitoring over extended periods. The unattended nature of these nodes raises concerns about data quality. Ensuring data quality is crucial to enhance the reliability of decisions based on VCoT data. Given the mobile nature of vehicular clouds, providing provenance becomes challenging, emphasizing the need for checks for uniformity and continuous calibration of vehicular sensors and

middleware architecture. Different application sets may require varying levels of data granularity, making context a significant parameter[34,35].

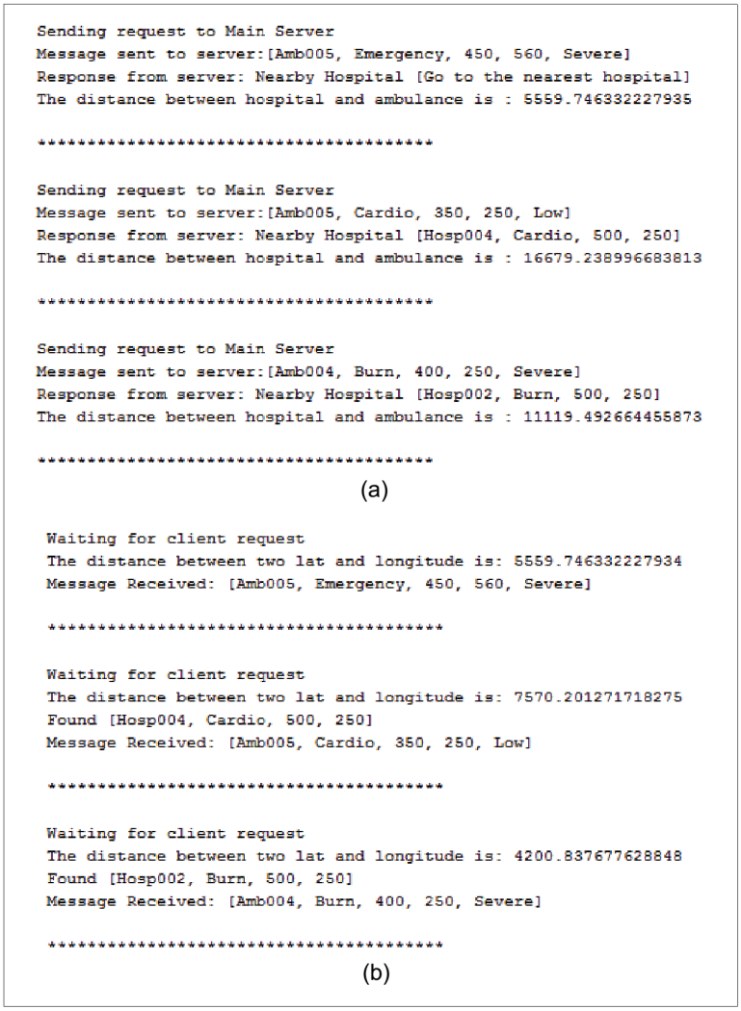

Figure 3. IoT based simulation while sending data to cloud as client and server.

Coverage: IoT and VANETs, along with other applications, are still in their early stages, requiring time to bring full benefits to the public. The expansion of these technologies necessitates infrastructure deployment and testing. As our proposed framework utilizes LoRa-based technologies, network coverage is a significant parameter for the successful realization of VCoT. VANET and its applications are undergoing standardization globally, indicating that connected vehicles will soon be prevalent in smart cities[36–39].

Security analysis: Privacy and security are paramount when integrating VCoT. Data generated by IoT infrastructures are privacy-sensitive, necessitating privacy-preserving mechanisms for data in transit and at rest. Effective privacy-preserving measures are crucial to prevent end-user privacy abuse. However, privacy requirements may conflict with application performance. Information sharing between VANETs and IoT must be secure and private, necessitating trade-offs between data granularity and application performance. Context-aware privacy-preserving techniques are essential, and the fog computing paradigm, processing information at edge nodes, plays a vital role in preserving privacy in VCoT. RSUs equipped with industry-standard privacy preservation mechanisms are optimal for examining data locally, ensuring data is not forwarded to the core network.

Packets delivery rate: The Packet Delivery Rate reflects the efficiency of each system in successfully delivering packets within the network. Packet Delivery Ratio (PDR) is a metric used to assess the effectiveness

of data transmission by measuring the percentage of successfully delivered packets compared to the total number of packets sent[40]. Therefore, PDR is calculated using the equation 1 as follows.

$$PDR = \frac{number\ of\ packets\ received}{number\ of\ packets\ sent} \times 100 \quad (1)$$

At the initial network size of 5 nodes, all systems exhibit a high Packet Delivery Rate. Our proposed ARPL system demonstrates exceptional performance with a 99.7% success rate, indicating its proficiency in delivering packets effectively within a small network as shown in **Figure 4**.

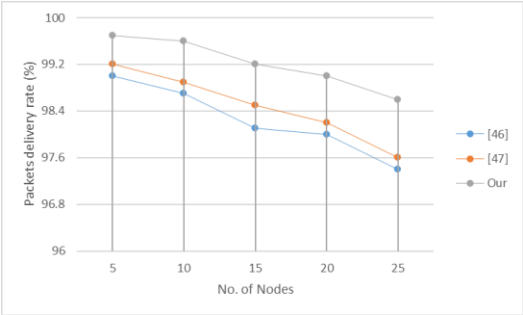

Figure 4. Packets delivery rate across different nodes.

With an increase in the number of nodes to 10, all systems maintain high Packet Delivery Rates. However, ARPL continues to outperform others, achieving a 99.6% success rate, highlighting its reliability in delivering packets across a moderately sized network. Finally, with 25 nodes, the Packet Delivery Rates remain competitive. Our ARPL system achieves a 98.6% success rate, indicating its ability to handle larger and more complex node configurations while maintaining effective packet delivery. Overall, across various node configurations, ARPL achieved consistently high success rates underscore its reliability in ensuring efficient packet delivery within IoT networks, making it a promising choice for applications where reliable data transmission is critical.

6. Conclusion

This article delves into security and privacy concerns among key stakeholders in smart cities, encompassing service providers, citizens, and governing bodies. It explicitly outlines security and privacy threats from the perspective of each stakeholder, conducting an in-depth analysis of these concerns within the proposed service provision framework for smart cities. The Stakeholder Onion Model is applied to identify various roles and actors, contributing to the development of distinct components within the Smart Secure Service Provisioning Framework. This framework underscores end-to-end security and privacy, covering the entire service provision model in smart cities. Its design aims to authorize only legitimate service providers to provision services while safeguarding citizens' private and sensitive data. Concurrently, the framework shields services from potential compromise by malicious citizens, ensuring that service providers use accurate citizen data for service curation. The layered architecture of the proposed framework is highly flexible, enabling it to handle diverse security scenarios in smart cities. To validate its effectiveness, selected components of the proposed framework, such as authentication, lightweight secure communication protocols, and the protection of services and applications using trusted modules against various security attacks, undergo testing in the Scyther verification tool. The verification results show promising outcomes, indicating successful service provisioning in the presence of selected security threats. Future research will concentrate on expanding the framework to configurable security and privacy services, with an emphasis on compliance with evolving government regulations, technological advancements, and escalating cybersecurity threats.

Conflict of interest

The author declares no conflict of interest.

References

1. Zanella A, Bui N, Castellani A, et al. Internet of Things for Smart Cities. IEEE Internet of Things Journal. 2014, 1(1): 22-32. doi: 10.1109/jiot.2014.2306328
2. Al-Fuqaha A, Guizani M, Mohammadi M, et al. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials. 2015, 17(4): 2347-2376. doi: 10.1109/comst.2015.2444095
3. Belgaum MR, Soomro S, Alansari Z, et al. Cloud Service Ranking Using Checkpoint-Based Load Balancing in Real-Time Scheduling of Cloud Computing. Progress in Advanced Computing and Intelligent Engineering. Published online 2018: 667-676. doi: 10.1007/978-981-10-6872-0_64
4. Fiza Gulzar Hussain, Muhammad Wasim, Ayesha Nasir. A Comparative Study of Parallel and Distributed Big Data programming models: Methodologies, Challenges and Future Directions. Lahore Garrison University Research Journal of Computer Science and Information Technology. 2023, 7(3). doi: 10.54692/lgurjcsit.2023.073365
5. Nawaz Bashir R, Sarwar Bajwa I, Waseem Iqbal M, et al. Leaching Fraction (LF) of Irrigation Water for Saline Soils Using Machine Learning. Intelligent Automation & Soft Computing. 2023, 36(2): 1915-1930. doi: 10.32604/iasc.2023.030844
6. Mumtaz G, Akram S, Iqbal MW, et al. Classification and Prediction of Significant Cyber Incidents (SCI) Using Data Mining and Machine Learning (DM-ML). IEEE Access. 2023, 11: 94486-94496. doi: 10.1109/access.2023.3249663
7. Khalid I, Shah T, Almarhabi KA, et al. The SPN Network for Digital Audio Data Based on Elliptic Curve Over a Finite Field. IEEE Access. 2022, 10: 127939-127955. doi: 10.1109/access.2022.3226322
8. Raza Naqvi M, Waseem Iqbal M, Usman Ashraf M, et al. Ontology Driven Testing Strategies for IoT Applications. Computers, Materials & Continua. 2022, 70(3): 5855-5869. doi: 10.32604/cmc.2022.019188
9. Iftikhar M, Shah MA, Ilyas I. A Survey on Data Security in Cloud Computing Using Blockchain: Challenges, Existing-State-Of-The-Art Methods, And Future Directions. Lahore Garrison University Research Journal of Computer Science and Information Technology. 2021, 5(3): 15-30. doi: 10.54692/lgurjcsit.2021.0503213
10. Hannan A, Cheema SM, Ali Z, Alofi A. Detection and tracking contagion using IoT-edge technologies: Confronting COVID-19 pandemic. In2020 international conference on electrical, communication, and computer engineering (ICECCE); 12 June 2020. IEEE. pp. 1-6.
11. Riaz S, Ashraf MU, Siddiq A. A Comparative Study of Big Data Tools and Deployment PIatforms. 2020 International Conference on Engineering and Emerging Technologies (ICEET). Published online February 2020. doi: 10.1109/iceet48479.2020.9048209
12. Alsubhi K, Imtiaz Z, Raana A, et al. MEACC: an energy-efficient framework for smart devices using cloud computing systems. Frontiers of Information Technology & Electronic Engineering. 2020, 21(6): 917-930. doi: 10.1631/fitee.1900198
13. Abid U, Ashraf MU, butt MU. A Critical Survey On Privacy Prevelling In Collaborative Filtring Recomender System: Challenges, State-Of-The-Art Methods And Future Directions. 2020 International Conference on Engineering and Emerging Technologies (ICEET). Published online February 2020. doi: 10.1109/iceet48479.2020.9048206
14. Ashraf MU. STATE-OF-THE-ART, CHALLENGES: PRIVACY PROVISIONING IN TTP LOCATION BASED SERVICES SYSTEMS. International Journal of Advanced Research in Computer Science. 2019, 10(2): 68-75. doi: 10.26483/ijarcs.v10i2.6396
15. Rehman A, Abdullah S, Fatima M, et al. Ensuring Security and Energy Efficiency of Wireless Sensor Network by Using Blockchain. Applied Sciences. 2022, 12(21): 10794. doi: 10.3390/app122110794
16. Alzubaidi M, Anbar M, Chong YW, Al-Sarawi S. Hybrid monitoring technique for detecting abnormal behaviour in rpl-based network. J. Commun.. 2018 Oct;13(5):198-208
17. Airehrour D, Gutierrez JA, Ray SK. SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. Future Generation Computer Systems. 2019 Apr 1;93:860-76
18. Javed R, Anwar S, Bibi K, et al. Prediction and Monitoring Agents using Weblogs for improved Disaster Recovery in Cloud. International Journal of Information Technology and Computer Science. 2019, 11(4): 9-17. doi: 10.5815/ijitcs.2019.04.02
19. Ashraf MU, Arif S, Basit A, et al. Provisioning Quality of Service for Multimedia Applications in Cloud Computing. International Journal of Information Technology and Computer Science. 2018, 10(5): 40-47. doi: 10.5815/ijitcs.2018.05.04
20. Fatima F, Ali S, Usman Ashraf M. Risk Reduction Activities Identification in Software Component Integration for Component Based Software Development (CBSD). International Journal of Modern Education and Computer Science. 2017, 9(4): 19-31. doi: 10.5815/ijmecs.2017.04.03

21. Sadhukhan P. An IoT based Framework for Smart City Services. 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT). Published online February 2018. doi: 10.1109/ic3iot.2018.8668103
22. Abba S, Light CI. IoT-Based Framework for Smart Waste Monitoring and Control System: A Case Study for Smart Cities. 7th International Electronic Conference on Sensors and Applications. Published online November 14, 2020. doi: 10.3390/ecsa-7-08224
23. Calderoni L, Magnani A, Maio D. IoT Manager: An open-source IoT framework for smart cities. Journal of Systems Architecture. 2019, 98: 413-423. doi: 10.1016/j.sysarc.2019.04.003
24. Gheisari M, Najafabadi HE, Alzubi JA, et al. OBPP: An ontology-based framework for privacy-preserving in IoT-based smart city. Future Generation Computer Systems. 2021, 123: 1-13. doi: 10.1016/j.future.2021.01.028
25. Bellini P, Nesi P, Pantaleo G. IoT-Enabled Smart Cities: A Review of Concepts, Frameworks and Key Technologies. Applied Sciences. 2022, 12(3): 1607. doi: 10.3390/app12031607
26. Gupta R, Budhiraja N, Mago S, et al. An IoT-Based Smart Parking Framework for Smart Cities. Advances in Intelligent Systems and Computing. Published online August 19, 2020: 19-32. doi: 10.1007/978-981-15-5616-6_2
27. Whaiduzzaman M, Barros A, Chanda M, et al. A Review of Emerging Technologies for IoT-Based Smart Cities. Sensors. 2022, 22(23): 9271. doi: 10.3390/s22239271
28. Kumar A, Payal M, Dixit P, et al. Framework for Realization of Green Smart Cities Through the Internet of Things (IoT). EAI/Springer Innovations in Communication and Computing. Published online 2020: 85-111. doi: 10.1007/978-3-030-40037-8_6
29. Santos PM, Queiros C, Sargento S, et al. PortoLivingLab: An IoT-Based Sensing Platform for Smart Cities. IEEE Internet of Things Journal. 2018, 5(2): 523-532. doi: 10.1109/jiot.2018.2791522
30. Hoque MA, Hossain M, Noor S, et al. IoTaaS: Drone-Based Internet of Things as a Service Framework for Smart Cities. IEEE Internet of Things Journal. 2022, 9(14): 12425-12439. doi: 10.1109/jiot.2021.3137362
31. Kumar M, Raju KS, Kumar D, Goyal N, Verma S, Singh A. An efficient framework using visual recognition for IoT based smart city surveillance. Multimedia Tools and Applications; 2021. pp. 1-9.
32. Chakrabarty S, Engels DW. Secure Smart Cities Framework Using IoT and AI. 2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT). Published online December 12, 2020. doi: 10.1109/gcaiot51063.2020.9345912
33. Syed AS, Sierra-Sosa D, Kumar A, et al. IoT in Smart Cities: A Survey of Technologies, Practices and Challenges. Smart Cities. 2021, 4(2): 429-475. doi: 10.3390/smartcities4020024
34. Li H, Liu Y, Qin Z, et al. A Large-Scale Urban Vehicular Network Framework for IoT in Smart Cities. IEEE Access. 2019, 7: 74437-74449. doi: 10.1109/access.2019.2919544
35. Vlacheas P, Giaffreda R, Stavroulaki V, et al. Enabling smart cities through a cognitive management framework for the internet of things. IEEE Communications Magazine. 2013, 51(6): 102-111. doi: 10.1109/mcom.2013.6525602
36. Santos PM, Queiros C, Sargento S, et al. PortoLivingLab: An IoT-Based Sensing Platform for Smart Cities. IEEE Internet of Things Journal. 2018, 5(2): 523-532. doi: 10.1109/jiot.2018.2791522
37. Chakrabarty S, Engels DW. Secure Smart Cities Framework Using IoT and AI. 2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT). Published online December 12, 2020. doi: 10.1109/gcaiot51063.2020.9345912
38. Syed AS, Sierra-Sosa D, Kumar A, et al. IoT in Smart Cities: A Survey of Technologies, Practices and Challenges. Smart Cities. 2021, 4(2): 429-475. doi: 10.3390/smartcities4020024
39. Li H, Liu Y, Qin Z, et al. A Large-Scale Urban Vehicular Network Framework for IoT in Smart Cities. IEEE Access. 2019, 7: 74437-74449. doi: 10.1109/access.2019.2919544
40. Vlacheas P, Giaffreda R, Stavroulaki V, et al. Enabling smart cities through a cognitive management framework for the internet of things. IEEE Communications Magazine. 2013, 51(6): 102-111. doi: 10.1109/mcom.2013.6525602