**SECURITY CONSTRAINTS, SOLUTION and IDS IN**

**VEHICULAR NETWORK**

### A

### PROJECT REPORT

#### Submitted by

**ANISH SHOW 20BCS3655**

#### in partial fulfillment for the award of the degree

#### of

**BACHELOR OF ENGINNERING**

**IN**

**COMPUTER SCIENCE AND ENGINEERING**

###### IN

##### **INFORMATION** **SECURITY**

###### 

###### Chandigarh University

2023-2024



**BONAFIDE CERTIFICATE**

Certified that this project report **“SECURITY CONSTRAINTS, SOLUTION and IDS IN VEHICULAR NETWORK”** is the bona fide work of “**ANISH SHOW”** who carried out the project work under my/our supervision.

###### SIGNATURE

###### ABHISHEK ANKUR

**E12833**

**ACKNOWLEDGEMENT**

We would like to express our deep gratitude to our project guide Mr. Abhishek Ankur Department of Computer Science and Engineering, CU, for his guidance with unsurpassed knowledge and immense encouragement. We are very much thankful to the Principal and Management, CU, for their encouragement and co- operation to carry out this work. We express our thanks to all the teaching faculty of Department of CSE, whose suggestions during reviews helped us in accomplishment of our project. We would like to thank all nonteaching staff of the Department of CSE, CU for providing great assistance in accomplishment of our project. We also thank our project coordinator Ms. Yashika Sharma, Department of Computer Science and Engineering, CU, for his constant support throughout our project period. We would like to thank our parents, friends, and classmates for their encouragement throughout our project period. At last but not the least, we thank everyone for supporting us directly or indirectly in completing this project successfully.

Anish Show

20BCS3655

# DECLARATION

# I| am Anish Show of 7th semester B.Tech., in the department of Computer Science and Engineering from Chandigarh University, hereby declare that the project work entitled Security Constraints, Solution and IDS in Vehicular Network is carried out by us and submitted in partial fulfilment of the requirements for the award of Bachelor of Technology in Computer Science Engineering , under Chandigarh University during the academic year 2023-24 and has not been submitted to any other university for the award of any kind of degree.

ANISH SHOW

20BCS3655

**TABLE OF CONTENT**

1.Title Page

2.Acknowledgement

3.Bonafied

4.Decleration

5.Abstract

6.Introducation

7.Literature Survey

8.Methodology

9.Conclution

10.Future Scope

11.Reference

**Abstract**

In-vehicle communication has become an integral part of today’s driving environment considering the growing add-ons of sensor-centric communication and computing devices inside a vehicle for a range of purposes including vehicle monitoring, physical wiring reduction, and driving efficiency. However, related literature on cyber security for in-vehicle communication systems is still lacking potential dedicated solutions for in-vehicle cyber risks. Existing solutions are mainly relying on protocol-specific security techniques and lacking an overall security framework for in-vehicle communication. In this context, this paper critically explores the literature on cyber security for in-vehicle communication focusing on technical architecture, methodologies, challenges, and possible solutions. In-vehicle communication network architecture is presented considering key components, interfaces, and related technologies. The protocols for in-vehicle communication have been classified based on their characteristics, and usage type. Security solutions for in-vehicle communication have been critically reviewed considering machine learning, cryptography, and port-centric techniques. A multi-layer secure framework is also developed as a protocol and use case-independent in-vehicle communication solution. Finally, open challenges and future dimensions of research for in-vehicle communication cyber security are highlighted as observations and recommendations. Keywords: [learning](https://www.mdpi.com/search?q=machine+learning) Machine ; [cryptography](https://www.mdpi.com/search?q=cryptography); [cyberattacks](https://www.mdpi.com/search?q=cyber+attacks); [cyber security](https://www.mdpi.com/search?q=cyber+security); [intrusion detection system](https://www.mdpi.com/search?q=intrusion+detection+system); [smart intelligent vehicles](https://www.mdpi.com/search?q=smart+intelligent+vehicles); [in-vehicle network](https://www.mdpi.com/search?q=in-vehicle+network); [controller area network (CAN)](https://www.mdpi.com/search?q=controller+area+network+%28CAN%29)

**INTRODUCTION**

Modern intelligent vehicle can be regarded as cyber- physical system with high connectivity capabilities, and today’s era stands as the testament to this immense progression in the in vehicle automotive technology [1]. Modern intelligent vehicles should not be perceived to work like mechanical systems; rather they have an integrated architecture with millions of line codes to give up-to-date information for vehicle occupants. Advancements of modern communications in-vehicle allow for more precise in-vehicle dash centric communications as well as phone, sensor, headphones, and roadside units. Attention also needs to be given to the inherent short range communication system embedded into vehicle for security reasons due to potential cyber security weaknesses.” Over the recent period there is high attitude on security for vehicle networks studies. This growth is giving rise to researchers to build new protocols, while this culminates in the invention of new smart applications. The auto industry needs to develop efficient protocols that are fully compatible with recent patterns and technologies in order to compete with contemporary requirements. Then, showing in-vehicle communication security cases and their corresponding threats. The existing protocols of the in-vehicle network have many problems. For example, the unavailability of message authentication and encryption, ID-based arbitration mechanism for contention resolution, etc. There are a lot of reasons to consider the necessity of vehicle’s security. Adversaries In the recent decades, there are improvements in technology of smart intelligent vehicles as well as self-driving vehicles. There have been great innovations in connection to the improved connectivity on the modern automotive industries leading to the development of communication channels and access points.

**Literature Reiview**

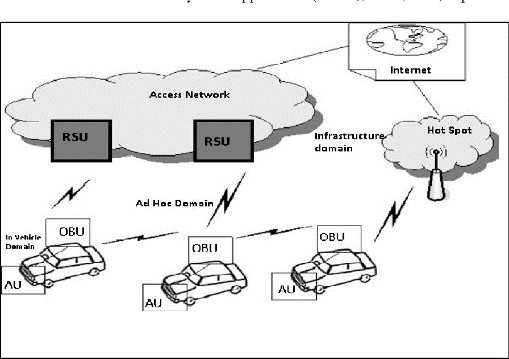
|  |  |  |  |
| --- | --- | --- | --- |
| IDS types | Security attacks | Features | Limitation |
| Signature based | DoS, False alert, fake congestion | This IDS verifies the identities of all nodes and monitoring the behaviors of the nodes, detects the malicious nodes. Fake messages can be easily detected by this IDS. | Cannot detect zero-day attacks. • New types of attacks cannot be detected easily. • Depends on the previous records. |
| Watchdog Based | Blackhole , false alert | It uses different statistical methods to detect the greedy nodes that provide false alerts. It provides a threshold to detect attacks. This IDS has low FP rate. | • It detects only specific attacks like selfish, greedy and misbehaving nodes [1]. • Provides extra delay and overhead in the network. |
| Anomaly Based | DoS, false information, packet drop | This IDS detects the nodes which share false information in the network through different statistical methods. This IDS uses a lightweight clustering technique to detect malicious nodes. | High delay and overhead. • Cannot detect the types of attacks. • Does not work while updating any profile. • High FP rate. • Not cost-effective. |
| Cross layer based | Blackhole | It uses different methods to compare normal and abnormal behaviors. | Not energy efficient. • Provide extra delay and overhead. |
| Hybrid | DoS, Blackhole, Sybil, wormhole | It can detect both known and unknown attacks by minimizing the detection errors. It uses both anomaly and signature-based IDS to detect attacks. | Not cost-effective. • High detection time. |
| Honeypot based | DoS, Blackhole | It can easily detect the known attacks and also zero-day attack using generalized framework. | Needs extra modules to improve the detection rate. • High overhead. |

**SECURITY CHALLENGES OF VANET**

The high mobility and density with fixed resources are the main reasons for having different challenging issues in VANET. The specific characteristics of VANET are the major reasons for the issues. These characteristics also make the design very hard and give easy access to outside attacks. These specific features of VANET are responsible for the following challenging issues:

Privacy: It is not easy to provide a proper security model along with the privacy model in VANET. Normally, every driver wants to protect their information about their locations and histories. As a result, the controller cannot get information about any occurrence on the road. Here, providing privacy is the main constraint for the security model. To handle all the vehicles, one model needs to be implemented that ensures providing critical traffic information though the drivers don’t want to share all information.

Mobility: The nodes of VANET moves very fast and change their location frequently. While moving with over 20m/s speed, it is not easy to stay connected with the network for the nodes. As a result, packet loss and link breakage happen. In this position, it is not easy to provide a proper security model for VANET.

Scalability: VANET has high density. There are over 250 million vehicles connected with VANET worldwide. There is no standardized rule to give proper security for the huge number of nodes. Normally different local and private authorities are trying to provide security for a limited area. As a result, the traffic information of outside of the area can not be included in the network and drivers cannot get informed about any occurrence of those places while driving. Limited resource: The other major challenging issue of VANET is the limited resource. As VANET have fixed resources, the implementation of security within the limited resources is a difficult task. Except these following reasons, VANET has other different reasons for having security constraints. Generally, IDS is used to give protection to VANET. But, if an attack happens in the network, the network system must need to take immediate decisions to tackle the incident. Here in the network IDS sends notifications or alerts the drivers about the incident to take manual actions. Here, drivers may not have the proper knowledge about the proper actions during the incident. This may cause a big loss in the network. the attacker gets more time to corrupt the data of the network. Normally, RSUs can not be installed everywhere because of cost management. So, all OBU devices can not be connected to the RSUs all the time. Though OBU devices can be connected with other OBU devices to share information, all devices may not be connected with the RSUs. As a result, any middle attack where RSU is absent can happen. In this situation, OBU devices may not get access to the control stations. It occurs a big packet loss and data breakage.

**DIFFERENT ATTACKS IN VANET**

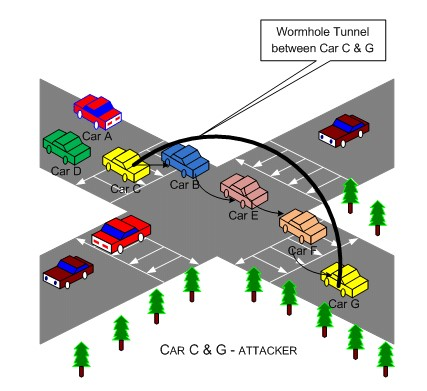
With the advancement of wireless networks, the ideas of attackers are also getting advanced. When attackers get any leak in the network, they try to attack the network with different types of attacks. So, security is a big concern for any network. In VANET attackers use special techniques to attack the network. Attackers try to use the network for their own purpose for their easy travels. They also attack the network to make accidents and roadblocks.

Sybil attack:

Sybil attack is one of the dangerous attacks in VANET. Sybil attack creates a scenario where specific nodes get multiple identities. That means attackers attack any node and gather its information and broadcast the information for multiple places. As a result, the normal nodes think that there are multiple nodes and change their direction for an easy journey. For example, an attacker provides fake information in the network about the road that the road is congested and blocked so that the other nodes change their direction to other routes. The nodes whose identities are stolen are called Sybil nodes and the attacker node is called Sybil attacker. Sometimes Sybil attack can make a big accident and this attack cannot be detected easily. It is very difficult and takes a long time to detect Sybil attack and so Sybil attack is a very dangerous attack.

DoS attack: DoS attack is a common attack in every network. DoS attack makes the network freeze for a time. As a result, other nodes cannot use the network. In this attack, attacker continuously sends requests to the network system so that the system cannot handle all the requests. Thus, attacker makes the system shut down for a time. Within the time, other nodes cannot share or receive any type of data through the network. Flooding attacks, Jelly Fish attack and intelligent cheater attack are different types of DoS attack. In data flooding attacks, attackers share useless data in the network again and again to make the network busy with useless requests. Jelly Fish attack normally attacks the protocols of the network and makes the system disordered and creates a delay in the network. Intelligent cheater attack also attacks the protocols and continuously tries to make the network having misbehaves to the other nodes. Both of the attacks are difficult to detect.

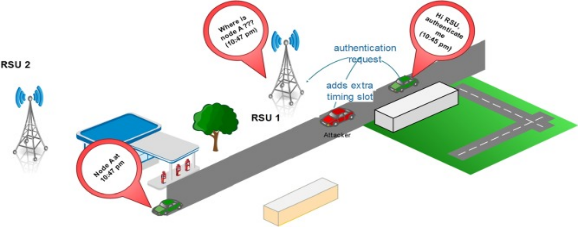
Blackhole attack: In blackhole attack, a specific node suddenly stops communicating with the network and thus a blackhole is established. As a result, the received data of the node remains unshared and the other nodes don’t have any idea about the data. The attacker node shares fake routing information in the network so that all packets come to the attacker node. When the packets come to the attacker, attacker denies to forward those packets to the network.

Wormhole attack: In a wormhole attack, attackers want to modify the network topology to manipulate the traffic. Here attacker node receives the packet and modifying the packet, sends the packet to another victim node. Then the packet gets transmitted in the network. As a result, a fake routing path is created and the shortest path shows the best path through the attacker node. When there is only one attacker, the attacker receives a packet at one point of the time and shares the packet after another point to modify the packet. As a result, most of the packets during the point cannot be transmitted properly.

Fake information attack: Broadcasting fake information is very crucial problem in VANET. False position information makes the network more inappropriate to use and as a result, drivers get confused about the routs. Attackers inject fake information according to their tastes to change the flow of the traffic. Because of the false position information, many important and emergency information gets lost. Fake information in VANET can occur big accidents or damages.

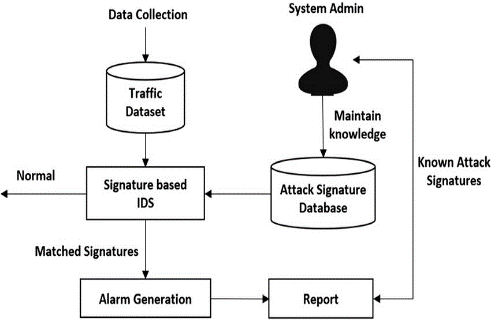
Sensor tempering: OBU of the vehicle is the main component to connect with the RSUs. Attackers try to manipulate the function of the OBU. Attackers attack the nodes for a short time and using short brake, make the application informed that there is a traffic jam on the road. Then the message gets broadcasted in the network. Illusion attack and GPS spoofing are the types of sensor tempering. In an illusion attack, attackers gather traffic information and make new false information. Other drivers receive false information and believe them. Attacker create false information such a way that it seems lots of vehicles on the road and there is a big traffic jam. The attacker also tries to modify the data of own sensors.

**SOLUTIONS FOR SECURITY ISSUES**

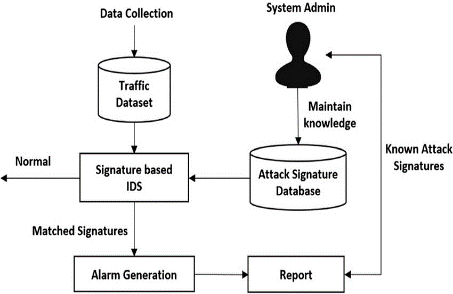
VANET is introducing an advanced network for vehicular nodes. So, it is very important to maintain the security of the network with the proper model. Many researchers introduced different solutions to provide the best security model for VANET. But a particular model cannot handle all types of attacks. But some model can minimize the effects of the attacks. As Sybil attack is one of the most dangerous attack in VANET, researchers are trying their best to find out proper solution to detect the attack. To detect a Sybil attack it is needed to detect the corrupted data in the network. The sensor capabilities of all the nodes should be improved. The shared data need to be identified as correct by the nearby authorized nodes. Analyzing the signal strength of the packet the network needs to detect the fake packets. Frequent node authentication can also detect the malicious nodes and can block the Sybil attack. DoS attacks can bring big damage in VANET. So, a proper solution for this attack is needed. The request detector can get the right request from source to destination. For this, any specific authorized node can be a RSU. Here, the detector gathers information about the source and destination and synchronize the acknowledgment of the transmission. Here, a response detector tries to protect the response packets. To prevent DoS attack a fixed threshold value needs to be set in the network for fixed transmission at a time. Blackhole attacks can be prevented by the watchdog technique . In this technique, when any node shares a packet to others, then it also checks that the other node is sharing the same packet or not. For this, all nodes need to have a high trust level for sharing the transmission information. Again, using the clustering technique, blackhole attack can be minimized. Here, only the cluster heads are responsible for the main communication. For wormhole attacks, there are different routing protocols. Those protocols gather information about the proper position of each node through different sensors. The information gets broadcasted in the network. As a result, all the nodes get the exact positions of other nodes. Fake information-sharing problems can be minimized through message filtering techniques. Here, verified nodes collect data and send it to the RSUs. If any node provides face information to the other nodes, RSUs grab the data and compare with all other data. When RSUs get that the data is appropriate, only then RSUs share the data in the network. A proper verification process can fix the fake position information attack. Multiple RSUs need to verify the nodes at a time so that the attacker node cannot share fake position information in the network. Illusion and GPS spoofing attacks can be prevented by frequent checking of sensors. This process needs to be implemented again and again after a fixed time interval.

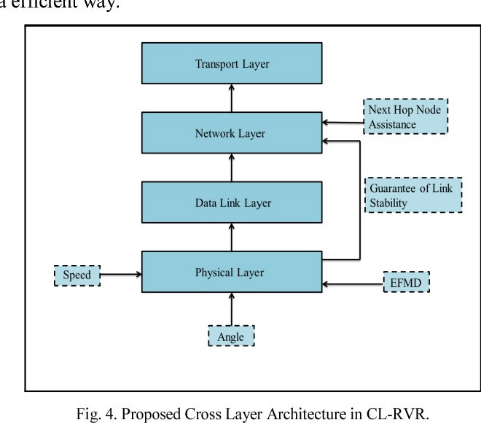
**IDS IN VANET**

IDS is the best solution for VANET security from the very beginning. Different types of IDS provide different types of detection strategies for VANET. But to design VANET with IDS it is mandatory to keep in mind that all IDS cannot cover full security from all types of attacks. So, it is needed to select the type of IDS that can cover most of the portion of security.

Signature-based IDS: Signature-based IDS uses previous records and compares them with the gathered new data to find out the malicious events. This IDS uses pattern matching process to get the wrong pattern. Here, the false positive (FP) is low. But, deploying signature-based IDS in VANET is not an easy task. Controller management needs to gather and store the log files of all previous detections to get proper results. In signature-based IDS cannot detect the new attacks, because there does not have any log about the new attacks. As a result, the new malicious attack can destroy the network.

Watchdog-based IDS: In this type of IDS, specific nodes are assigned to monitor other nearby nodes to gather the behavior of those nodes. Here, the source node shares data to the nearby nodes to transfer data to the destination. But when the source sends data to the nearby nodes, it also monitors the activities of the nearby nodes. The source node monitors that the actual data is being sent to the destination properly or not. If there seems any type of disturbance, the source sends an alarm about the incident to the server.

Anomaly-based IDS: Anomaly-based IDS detects attacks according to the behaviors of the nodes. This IDS makes different profiles of different nodes and updates the details frequently. When it sees any unwanted behavior in the network, it blocks the connection with that particular nodes. Different statistical methods are used to update the profiles. This IDS also use the concept of clustering to update the profiles easily. This process can detect malicious nodes and the detection rate can vary. But this IDS provides high FP rate. This IDS provides high delay and overhead and it takes high computational cost.

Cross layer-based IDS: Normally, IDS is deployed in the application layer and it only detects the attacks of just the application layer. But the attacker can target other layers also. In cross-layer IDS, IDS is deployed in different layers. It uses different security detection methods to detect any security fail in the layers. This IDS also use watchdog IDS to improve detection accuracy. This type of IDS provides more delay and overhead.

Hybrid IDS: Hybrid IDS is the combination of signature and anomaly-based IDS. This type of IDS uses previous logs and frequently updates the profiles. According to the profile details, this IDS detects the malicious nodes. This IDS can detect both known and unknown attacks in the network. This type of IDS is not cost effective, because it is not easy to combine multiple IDS and it takes high cost. Though the detection rate is high in this IDS, it takes a long time to detect the attacks.

Honeypot-based IDS: Honeypot-based IDS is used to detect selfish nodes. It monitors the traffic and searches for any selfish activity. When it gets any such behavior, it blocks the connection with those particular nodes. This process improves the ratio of packet delivery and decreases end-to-end delay. But this process provides extra overhead and this IDS needs an extra module to improve detection accuracy

## **Conclusions**

Therefore, VANET becomes a promising technology in wireless environment. A large amount of users wants too safe as much as possible safety on this path, with plenty of people around getting hurt by others’ harassment and ill-will. In the in order to have a secure VANET’s environment one need to put in more efforts on overcome future problems. This paper Most VANET security challenges and their solutions will be introduced, summarily. causes and solutions. In this section, we discuss various attacks on VANET. We explain different IDS in Comparison of the solution for various attacks in VANET. Challenges in security and their solutions at different levels. It also addresses attack or any detection for fake information in VANET. difficult problem. Various effective procedures as well as adaptable discovery methods can be used on the basis of computer. other promising research direction relates to VANET safety, for instance using intelligence designs in future studies.

**Future Scope**

The future of healthcare is very promising, considering the rapid development in sensor technology, AI and machine learning. For patients, hospitals and doctors as well as for medical device manufacturers, there are not only new opportunities but even the obligation to make use of the Internet of Things. It is obvious that challenges and substantial risks have to be mastered. Throughout the reviewed literature there is a consistency for use of smart technologies in smart cities and in particular healthcare, and AI and block chain technologies are key driving factors for enhancement and improvement of overall user experience of smart cities. Although there are potential downsides of artificial intelligence and machine learning technologies in the context of smart cities, they still also have a potential to change the way we know smart healthcare and smart cities as of now.

**References**

1. Shah, R.; Chircu, A. IoT and AI in healthcare: A systematic literature review. *Issues Inf. Syst.* **2018**, *19*. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=IoT+and+AI+in+healthcare:+A+systematic+literature+review&author=Shah,+R.&author=Chircu,+A.&publication_year=2018&journal=Issues+Inf.+Syst.&volume=19&doi=10.48009/3_iis_2018_33-41)] [**[CrossRef](https://doi.org/10.48009/3_iis_2018_33-41" \t "_blank)**]
2. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and iot integration: A systematic survey. *Sensors* **2018**, *18*, 2575. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=Blockchain+and+iot+integration:+A+systematic+survey&author=Panarello,+A.&author=Tapas,+N.&author=Merlino,+G.&author=Longo,+F.&author=Puliafito,+A.&publication_year=2018&journal=Sensors&volume=18&pages=2575&doi=10.3390/s18082575)] [**[CrossRef](https://doi.org/10.3390/s18082575" \t "_blank)**][[**Green Version**](https://www.mdpi.com/1424-8220/18/8/2575/pdf)]
3. Jiang, F.; Jiang, Y.; Zhi, H.; Dong, Y.; Li, H.; Ma, S.; Wang, Y.; Dong, Q.; Shen, H.; Wang, Y. Artificial intelligence in healthcare: Past, present and future. *Stroke Vasc. Neurol.* **2017**, *2*. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=Artificial+intelligence+in+healthcare:+Past,+present+and+future&author=Jiang,+F.&author=Jiang,+Y.&author=Zhi,+H.&author=Dong,+Y.&author=Li,+H.&author=Ma,+S.&author=Wang,+Y.&author=Dong,+Q.&author=Shen,+H.&author=Wang,+Y.&publication_year=2017&journal=Stroke+Vasc.+Neurol.&volume=2&doi=10.1136/svn-2017-000101&pmid=29507784)] [**[CrossRef](https://doi.org/10.1136/svn-2017-000101" \t "_blank)**] [[**PubMed**](http://www.ncbi.nlm.nih.gov/pubmed/29507784)]
4. Bahl, M.; Barzilay, R.; Yedidia, A.B.; Locascio, N.J.; Yu, L.; Lehman, C.D. High-risk breast lesions: A machine learning model to predict pathologic upgrade and reduce unnecessary surgical excision. *Radiology* **2018**, *286*, 810–818. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=High-risk+breast+lesions:+A+machine+learning+model+to+predict+pathologic+upgrade+and+reduce+unnecessary+surgical+excision&author=Bahl,+M.&author=Barzilay,+R.&author=Yedidia,+A.B.&author=Locascio,+N.J.&author=Yu,+L.&author=Lehman,+C.D.&publication_year=2018&journal=Radiology&volume=286&pages=810%E2%80%93818&doi=10.1148/radiol.2017170549&pmid=29039725)] [**[CrossRef](https://doi.org/10.1148/radiol.2017170549" \t "_blank)**] [[**PubMed**](http://www.ncbi.nlm.nih.gov/pubmed/29039725)]
5. Cugurullo, F. Exposing smart cities and eco-cities: Frankenstein urbanism and the sustainability challenges of the experimental city. *Environ. Plan. A Econ. Space* **2018**, *50*, 73–92. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=Exposing+smart+cities+and+eco-cities:+Frankenstein+urbanism+and+the+sustainability+challenges+of+the+experimental+city&author=Cugurullo,+F.&publication_year=2018&journal=Environ.+Plan.+A+Econ.+Space&volume=50&pages=73%E2%80%9392&doi=10.1177/0308518X17738535)] [**[CrossRef](https://doi.org/10.1177/0308518X17738535" \t "_blank)**]
6. Cugurullo, F. *Frankenstein Urbanism: Eco, Smart and Autonomous Cities, Artificial Intelligence and the End of the City*; Routledge: Abingdon-on-Thames, UK, 2021. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=Frankenstein+Urbanism:+Eco,+Smart+and+Autonomous+Cities,+Artificial+Intelligence+and+the+End+of+the+City&author=Cugurullo,+F.&publication_year=2021)]
7. Habibzadeh, H.; Soyata, T. Toward uniform smart healthcare ecosystems: A survey on prospects, security, and privacy considerations. In *Connected Health in Smart Cities*; Springer: Cham, Switzerland, 2019; ISBN 9783030278441. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=Toward+uniform+smart+healthcare+ecosystems:+A+survey+on+prospects,+security,+and+privacy+considerations&author=Habibzadeh,+H.&author=Soyata,+T.&publication_year=2019)]
8. Latif, S.; Zafar, N.A. A survey of security and privacy issues in IoT for smart cities. In Proceedings of the 5th International Conference on Aerospace Science and Engineering ICASE, Islamabad, Pakistan, 14–16 November 2017; pp. 1–5. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=A+survey+of+security+and+privacy+issues+in+IoT+for+smart+cities&conference=Proceedings+of+the+5th+International+Conference+on+Aerospace+Science+and+Engineering+ICASE&author=Latif,+S.&author=Zafar,+N.A.&publication_year=2017&pages=1%E2%80%935&doi=10.1109/ICASE.2017.8374288)] [**[CrossRef](https://doi.org/10.1109/ICASE.2017.8374288" \t "_blank)**]
9. Huang, G.; Fang, Y.; Wang, X.; Pei, Y.; Horn, B. A Survey on the status of smart healthcare from the universal village perspective. In Proceedings of the 4th IEEE International Conference on Universal Village, Boston, MA, USA, 21–24 October 2018. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=A+Survey+on+the+status+of+smart+healthcare+from+the+universal+village+perspective&conference=Proceedings+of+the+4th+IEEE+International+Conference+on+Universal+Village&author=Huang,+G.&author=Fang,+Y.&author=Wang,+X.&author=Pei,+Y.&author=Horn,+B.&publication_year=2018&doi=10.1109/UV.2018.8642125)] [**[CrossRef](https://doi.org/10.1109/UV.2018.8642125" \t "_blank)**][[**Green Version**](https://repository.arizona.edu/bitstream/10150/633393/3/08642125(1).pdf)]
10. Arasteh, H.; Hosseinnezhad, V.; Loia, V.; Tommasetti, A.; Troisi, O.; Shafie-Khah, M.; Siano, P. Iot-based smart cities: A survey. In Proceedings of the EEEIC 2016 International Conference on Environment and Electrical Engineering, Florence, Italy, 7–10 June 2016; pp. 2–7. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=Iot-based+smart+cities:+A+survey&conference=Proceedings+of+the+EEEIC+2016+International+Conference+on+Environment+and+Electrical+Engineering&author=Arasteh,+H.&author=Hosseinnezhad,+V.&author=Loia,+V.&author=Tommasetti,+A.&author=Troisi,+O.&author=Shafie-Khah,+M.&author=Siano,+P.&publication_year=2016&pages=2%E2%80%937&doi=10.1109/EEEIC.2016.7555867)] [**[CrossRef](https://doi.org/10.1109/EEEIC.2016.7555867" \t "_blank)**]
11. Alsamhi, S.H.; Ma, O.; Ansari, M.S.; Almalki, F.A. Survey on collaborative smart drones and internet of things for improving smartness of smart cities. *IEEE Access* **2019**, *7*, 128125–128152. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=Survey+on+collaborative+smart+drones+and+internet+of+things+for+improving+smartness+of+smart+cities&author=Alsamhi,+S.H.&author=Ma,+O.&author=Ansari,+M.S.&author=Almalki,+F.A.&publication_year=2019&journal=IEEE+Access&volume=7&pages=128125%E2%80%93128152&doi=10.1109/ACCESS.2019.2934998)] [**[CrossRef](https://doi.org/10.1109/ACCESS.2019.2934998" \t "_blank)**]
12. Li, W.; Chai, Y.; Khan, F.; Jan, S.R.U.; Verma, S.; Menon, V.G.; Kavita; Li, X. A Comprehensive survey on machine learning-based big data analytics for iot-enabled smart healthcare system. *Mob. Netw. Appl.* **2021**, *26*, 234–252. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=A+Comprehensive+survey+on+machine+learning-based+big+data+analytics+for+iot-enabled+smart+healthcare+system&author=Li,+W.&author=Chai,+Y.&author=Khan,+F.&author=Jan,+S.R.U.&author=Verma,+S.&author=Menon,+V.G.&author=Kavita&author=Li,+X.&publication_year=2021&journal=Mob.+Netw.+Appl.&volume=26&pages=234%E2%80%93252&doi=10.1007/s11036-020-01700-6)] [**[CrossRef](https://doi.org/10.1007/s11036-020-01700-6" \t "_blank)**]
13. Kharel, J.; Reda, H.T.; Shin, S.Y. An architecture for smart health monitoring system based on fog computing. *J. Commun.* **2017**, *12*, 228–233. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=An+architecture+for+smart+health+monitoring+system+based+on+fog+computing&author=Kharel,+J.&author=Reda,+H.T.&author=Shin,+S.Y.&publication_year=2017&journal=J.+Commun.&volume=12&pages=228%E2%80%93233&doi=10.12720/jcm.12.4.228-233)] [**[CrossRef](https://doi.org/10.12720/jcm.12.4.228-233" \t "_blank)**][[**Green Version**](http://pdfs.semanticscholar.org/ef86/a72384b4b64d18da00c63c47a92a885741e5.pdf)]
14. Muhammad, K.; Khan, S.; Del Ser, J.; de Albuquerque, V.H.C. Deep learning for multigrade brain tumor classification in smart healthcare systems: A prospective survey. *IEEE Trans. Neural Netw. Learn. Syst.* **2021**, *32*, 507–522. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=Deep+learning+for+multigrade+brain+tumor+classification+in+smart+healthcare+systems:+A+prospective+survey&author=Muhammad,+K.&author=Khan,+S.&author=Del+Ser,+J.&author=de+Albuquerque,+V.H.C.&publication_year=2021&journal=IEEE+Trans.+Neural+Netw.+Learn.+Syst.&volume=32&pages=507%E2%80%93522&doi=10.1109/TNNLS.2020.2995800)] [**[CrossRef](https://doi.org/10.1109/TNNLS.2020.2995800" \t "_blank)**]
15. Soomro, S.; Miraz, M.H.; Prasanth, A.; Abdullah, M. Artificial intelligence enabled IoT: Traffic congestion reduction in smart cities. In Proceedings of the Smart Cities Symposium, Sakhir, Bahrain, 22–23 April 2018; IET Conference Publications: London, UK, 2018; pp. 81–86. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=Artificial+intelligence+enabled+IoT:+Traffic+congestion+reduction+in+smart+cities&conference=Proceedings+of+the+Smart+Cities+Symposium&author=Soomro,+S.&author=Miraz,+M.H.&author=Prasanth,+A.&author=Abdullah,+M.&publication_year=2018&pages=81%E2%80%9386&doi=10.1049/cp.2018.1381)] [**[CrossRef](https://doi.org/10.1049/cp.2018.1381" \t "_blank)**]
16. Allam, Z.; Dhunny, Z.A. On big data, artificial intelligence and smart cities. *Cities* **2019**, *89*, 80–91. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=On+big+data,+artificial+intelligence+and+smart+cities&author=Allam,+Z.&author=Dhunny,+Z.A.&publication_year=2019&journal=Cities&volume=89&pages=80%E2%80%9391&doi=10.1016/j.cities.2019.01.032)] [**[CrossRef](https://doi.org/10.1016/j.cities.2019.01.032" \t "_blank)**]
17. Majeed, U.; Khan, L.U.; Yaqoob, I.; Kazmi, S.M.A.; Salah, K.; Hong, C.S. Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges. *J. Netw. Comput. Appl.* **2021**, 103007. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=Blockchain+for+IoT-based+smart+cities:+Recent+advances,+requirements,+and+future+challenges&author=Majeed,+U.&author=Khan,+L.U.&author=Yaqoob,+I.&author=Kazmi,+S.M.A.&author=Salah,+K.&author=Hong,+C.S.&publication_year=2021&journal=J.+Netw.+Comput.+Appl.&pages=103007&doi=10.1016/j.jnca.2021.103007)] [**[CrossRef](https://doi.org/10.1016/j.jnca.2021.103007" \t "_blank)**]
18. Cugurullo, F. Urban artificial intelligence: From automation to autonomy in the smart city. *Front. Sustain. Cities* **2020**, *2*, 38. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=Urban+artificial+intelligence:+From+automation+to+autonomy+in+the+smart+city&author=Cugurullo,+F.&publication_year=2020&journal=Front.+Sustain.+Cities&volume=2&pages=38&doi=10.3389/frsc.2020.00038)] [**[CrossRef](https://doi.org/10.3389/frsc.2020.00038" \t "_blank)**]
19. Ullah, Z.; Al-Turjman, F.; Mostarda, L.; Gagliardi, R. Applications of artificial intelligence and machine learning in smart cities. *Comput. Commun.* **2020**, *154*, 313–323. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=Applications+of+artificial+intelligence+and+machine+learning+in+smart+cities&author=Ullah,+Z.&author=Al-Turjman,+F.&author=Mostarda,+L.&author=Gagliardi,+R.&publication_year=2020&journal=Comput.+Commun.&volume=154&pages=313%E2%80%93323&doi=10.1016/j.comcom.2020.02.069)] [**[CrossRef](https://doi.org/10.1016/j.comcom.2020.02.069" \t "_blank)**]
20. Jha, S.; Nkenyereye, L.; Joshi, G.P.; Yang, E. Mitigating and monitoring smart city using internet of things. *Comput. Mater. Contin.* **2020**, *65*, 1059–1079. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=Mitigating+and+monitoring+smart+city+using+internet+of+things&author=Jha,+S.&author=Nkenyereye,+L.&author=Joshi,+G.P.&author=Yang,+E.&publication_year=2020&journal=Comput.+Mater.+Contin.&volume=65&pages=1059%E2%80%931079&doi=10.32604/cmc.2020.011754)] [**[CrossRef](https://doi.org/10.32604/cmc.2020.011754" \t "_blank)**]
21. Singh, S.K.; Cha, J.; Kim, T.W.; Park, J.H. Machine learning based distributed big data analysis framework for next generation web in IoT. *Comput. Sci. Inf. Syst.* **2021**, *18*. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=Machine+learning+based+distributed+big+data+analysis+framework+for+next+generation+web+in+IoT&author=Singh,+S.K.&author=Cha,+J.&author=Kim,+T.W.&author=Park,+J.H.&publication_year=2021&journal=Comput.+Sci.+Inf.+Syst.&volume=18&doi=10.2298/CSIS200330012S)] [**[CrossRef](https://doi.org/10.2298/CSIS200330012S" \t "_blank)**]
22. Singh, S.K.; Azzaoui, A.E.L.; Kim, T.W.; Pan, Y.; Park, J.H. DeepBlockScheme: A deep learning-based blockchain driven scheme for secure smart city. *Hum. Centric Comput. Inf. Sci.* **2021**, *11*. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=DeepBlockScheme:+A+deep+learning-based+blockchain+driven+scheme+for+secure+smart+city&author=Singh,+S.K.&author=Azzaoui,+A.E.L.&author=Kim,+T.W.&author=Pan,+Y.&author=Park,+J.H.&publication_year=2021&journal=Hum.+Centric+Comput.+Inf.+Sci.&volume=11&doi=10.22967/HCIS.2021.11.012)] [**[CrossRef](https://doi.org/10.22967/HCIS.2021.11.012" \t "_blank)**]
23. Zhang, W.; Fang, W.; Zhao, Q.; Ji, X.; Jia, G. Energy efficiency in internet of things: An overview. *Comput. Mater. Contin.* **2020**, *63*, 787–811. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=Energy+efficiency+in+internet+of+things:+An+overview&author=Zhang,+W.&author=Fang,+W.&author=Zhao,+Q.&author=Ji,+X.&author=Jia,+G.&publication_year=2020&journal=Comput.+Mater.+Contin.&volume=63&pages=787%E2%80%93811&doi=10.32604/cmc.2020.07620)] [**[CrossRef](https://doi.org/10.32604/cmc.2020.07620" \t "_blank)**]
24. Singh, S.K.; Pan, Y.; Park, J.H. OTS scheme based secure architecture for energy-efficient iot in edge infrastructure. *Comput. Mater. Contin.* **2021**, *66*, 2905–2922. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=OTS+scheme+based+secure+architecture+for+energy-efficient+iot+in+edge+infrastructure&author=Singh,+S.K.&author=Pan,+Y.&author=Park,+J.H.&publication_year=2021&journal=Comput.+Mater.+Contin.&volume=66&pages=2905%E2%80%932922&doi=10.32604/cmc.2021.014151)] [**[CrossRef](https://doi.org/10.32604/cmc.2021.014151" \t "_blank)**]
25. Ullo, S.L.; Sinha, G.R. Advances in smart environment monitoring systems using iot and sensors. *Sensors* **2020**, *20*, 3113. [[**Google Scholar**](https://scholar.google.com/scholar_lookup?title=Advances+in+smart+environment+monitoring+systems+using+iot+and+sensors&author=Ullo,+S.L.&author=Sinha,+G.R.&publication_year=2020&journal=Sensors&volume=20&pages=3113&doi=10.3390/s20113113)] [**[CrossRef](https://doi.org/10.3390/s20113113" \t "_blank)**]
26. Basics of Wireless Sensor Networks (WSN) | Classification, Topologies, Applications. Available online: [**https://www.electronicshub.org/wireless-sensor-networks-wsn/**](https://www.electronicshub.org/wireless-sensor-networks-wsn/) (accessed on 12 August 2021).