IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

A Hybrid Blockchain Framework for Secure and Efficient IoT Environment: A Review

Jyoti and Sapna Jain
M.Tech Scholar, Department of Computer Science Engineering
Assistant Professor, Department of Computer Science Engineering
Mata Raj Kaur Institute of Engg. & Tech (Saharanwas), Rewari
Muktajyoti920@gmail.com

Abstract: *The recent advances in wireless communication have led to the problem of growing spectrum scarcity. The problem of spectrum allocation is due to advance research in wireless communication. As new wireless applications are emerging, day after another, and making use of the available wireless spectrum for communication, the demand for spectrum increase makes the available spectrum scarcer. Mostly part of the spectrum is not utilized significantly in the wireless network. Cognitive Radio (CR) is a new technology that enables an unlicensed secondary user to coexist with licensed primary users in licensed spectrum bands without inducing interference to licensed primary users communication. This technology can significantly ease the spectrum redundancy problem & enhance the efficiency of utilization of spectrum. Cognitive Radio Networks (CRN) or Dynamic Spectrum Access Networks are formed by several CR nodes and they are often called NeXt Generation (XG) communication networks. This XG communication network is expected to give high transfer speed to versatile clients through heterogeneous remote designs and dynamic range access procedures. CRNs have drawn in incredible exploration interest in the new years. Nonetheless, research on the security parts of CRNs has been exceptionally restricted. As CRN is like a remote organization, the idea of the remote media is outside, it is more helpless against assaults when contrasted with that of a wired organization. This channel might be stuck/abuse due to remote media information is to be listened to*

Keywords: Cognitive Radio Networks; Intrusion Detection; Blockchain;Dynamic Spectrum Access; Cognitive Radio; Primary Users

I. INTRODUCTION

CR is a hardware device that has the capability of tuning to any frequency band and receives any modulation transversely in the wide frequency spectrum and it processes these signals through software. Initially, the CR observes, learns, senses the RF environment, and detects the RF activity of multiple bands, standards and channels. After gaining this information based on learning and observation, the CR adapts to the environment by dynamically changing its transmission parameters according to the changing environment and performs to give the optimal output. These key functions of CR are shown in Figure 2.1. CR joins various wellsprings of data, decides its present activity settings, and teams up with other intellectual radios in a remote organization; hence it becomes a Cognitive Radio Network (CRN). By practically implementing this cognitive radio technology, Secondary Users (SU) can sense and able to know which portion of the spectrum is accessible. Based on it, SU could be selected the optimized channel availability & access the allocated spectrum with other users also whenever the main user again claim for spectrum
(Haykin &Simon 2010). The sensational increment of quality of service & channel-limit in wireless systems is extremely restricted by the lack of energy and transmission capacity, which has primary resources. In this way, scientists are as of now focusing their consideration on new interchanges and systems administration standards that can efficiently use these rare resources. Cognitive-Radios is one basic powerful innovation for futuristic correspondences

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

and systems administration that could use the restricted system resources in a more proficient and adaptable way. It varies from modernized correspondence ideal models in which the radios or devices can adjust their working parameters, for example, transmission power, frequency, modulation sort, and so forth, to the varieties of the encompassing radio environment (Haykin & Simon 2010).

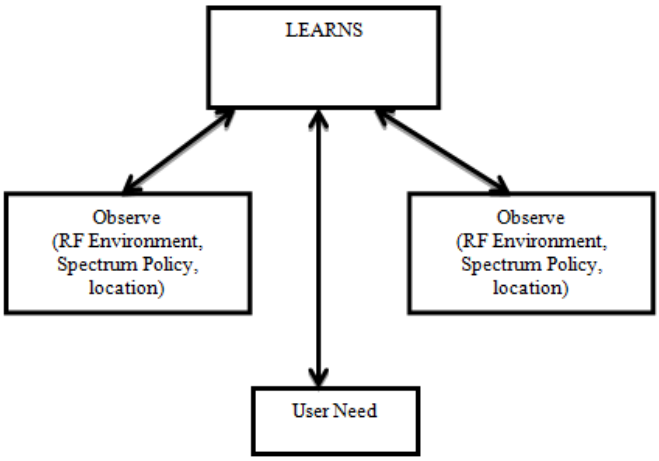

FIGURE 1 KEY FUNCTIONS OF COGNITIVE RADIO

The variation of environmental of CRs during the working mode, the cognitive radio should 1st enhance the fundamental data. There are different qualities that handle cognitive radio devices to know about radio waves and transmitting wave correspondence system sort as per requirement. The geographical information, locally open resources and organizations, customer needs, security approach, and so forth After CR gadgets collect their necessary information from the radio climate; they could drastically alter their transmission boundaries as shown by the distinguished climate assortments and achieve ideal execution, which is determined to as configurability.

II. BLOCK CHAIN OVERVIEW

Blockchain adoption is gaining huge momentum as industry is evolving at a fast pace. Many startups have initiated use cases and there is significant rise in investments in blockchain projects as well. Although blockchain is still evolving in terms of technological maturity, innovative experimental adoption and customization are continuously rising. Blockchain has the potential of displacing a setup innovation and stirs up the business or a pivotal item that makes a totally new industry [46] and initial trends with the rise of crypto currencies has signaled that blockchain has been disruptive for the banking industry and financial services.

Crypto currency has the potential of shaking a centralized banking system by eliminating the need to pay fees for using credit or debit cards [52] [61]. Recent Trends have shown that blockchain is turning out to be a sustaining technology rather disruptive and has huge potential in supply chain [48], healthcare [56], Internet of Things (IoT) [55], education [39] and public services [38].Commercial viability and acceptability of blockchain are on the rise and 3021 patent families related to blockchain applications are divided into four sub-categories based on different types of application like Payments and Transaction systems, Financial services business, Administration and E-commerce. Extensive use of cryptography and decentralization makes it highly secure. Privacy issues over public blockchains can be addressed by implementing blockchain in a controlled manner (permissioned blockchain). Blockchains can be named public, private or half and half variations, contingent upon their application [65].

• Public – No one owns Public blockchains, they are fully decentralized and are visible by anyone.

• Private – These are also referred to as permissioned blockchains and uses privilege to control who can peruse from and write to the blockchain.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

• Hybrid – These blockchains are public just to an advantaged bunch. Agreement measure is constrained by special workers utilizing a bunch of rules consented to by all gatherings.

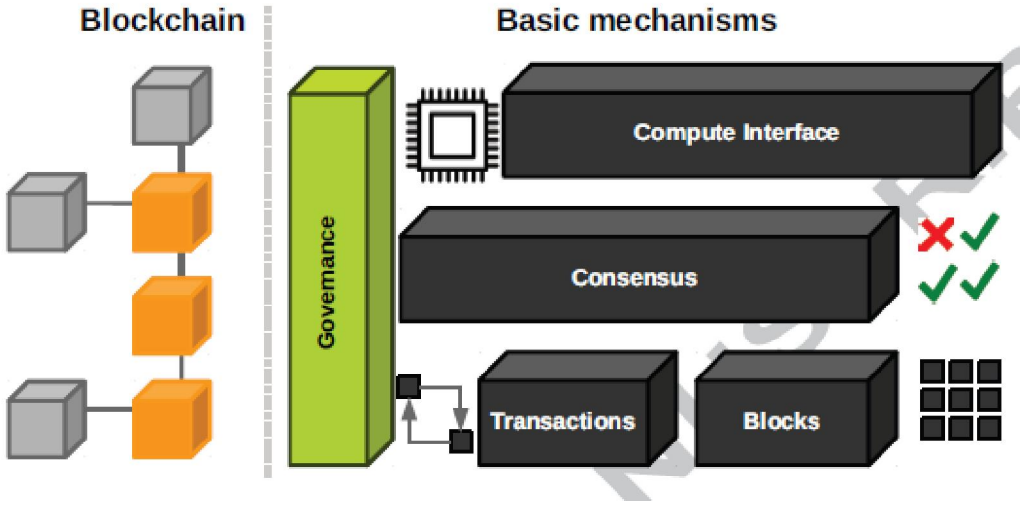

FIGURE 2: AN OVERVIEW OF BLOCK CHAIN ARCHITECTURE.

Blockchain may record exchanges, contracts, data resources or for all intents and purposes whatever can be put away in advanced structure. Blockchain records are lasting, carefully designed, straightforward, and accessible. Each new "block" created is added to the furthest limit of a "chain." Initiation, validation, storage, and distribution of each new block is managed by a protocol. Blockchain replaces the need of third-party intermediaries and participants of blockchain run complex algorithms to certify the integrity of records in the block.

III. REQUIREMENT FOR SECURITY IN COGNITIVE RADIO NETWORK

Cognitive Radio has the ability of adjusting to nature and makeimprovements in view of their interaction capacities for the securecorrespondence.

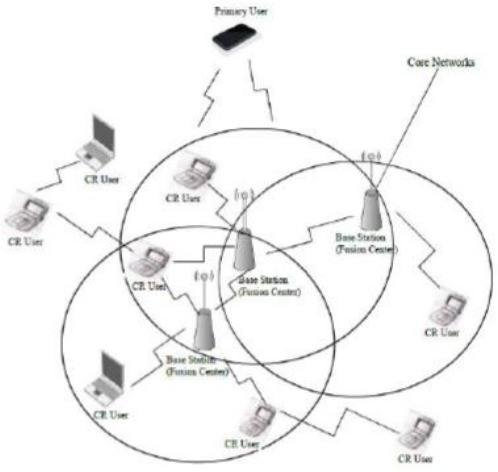

FIGURE 3 MESHARCHITECTURE OF CRN

Contrasting the wired system together with the wireless system, the security is powerless if there should arise an occurrence of remote system. At the point when the information is sent by means of a wireless system, then there is a

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

probability of eavesdropping, or alteration, which causes congestion. The Cognitive Radio systems have one of the specific characteristics that security turns to be an essential thing over it.

IV. TRUST BASED ALGORITHM TO ACCESS THE SECURED SPECTRUM

Dubey Rajni et al. (2012) have suggested that Wireless Spectrumwas valuable, so there are dependably necessities of dynamic shared spectrum strategies as well as the intelligent wireless correspondence structure, for example, Cognitive-Radio Network (CRN). In spite of the fact that, CRN gives reliability, mobility, awareness, flexibility and adaptability to its clients yet it has likewise opens the entryway for more number of dangers and assaults. In this paper, different conceivable assaults and dangers together with the possible approaches are explained. This paper likewise proposes a trust based security calculation enabling intellectual radio to acquire the appropriated estimation, conservers, and assets are available in Cognitive Radio climate.

The Trust Based Algorithm proposed is connected concerning the area identification and distance between the versatility of customers. Trust is registered from the genuine acquired force esteems and trust estimations are assessed by uniting the necessities of the dependability and the QoS with the connection ways. In light of this calculation, three dimensional (3D) masterminds the structure and it was used to affirm the space of the fundamental (essential) customer and pernicious customer. Proposed calculation has portrayed the trust segment of various customers on the reason of dependability. The recreation yields clarify the significance of the proposed trust based calculation for all of the three kinds of customer. They are essential, auxiliary and threatening customer, as far as both security as well as the performance.

Parvin Sazia & Farookh Khadeer Hussain (2012) have proposed Cognitive Radio (CR) thus it was considered to be an essential (primary) system to distinguish whether a specific portion of the radio spectrum was presently being used, and it is utilized to quickly involve the useless spectrum without disturbing the transmissions of different clients.

Wang Ji & Ray Chen (2014) have proposed Cognitive radio networks being promising approach for spectrum limitations. Secondary Users (SUs) receive sensing mechanism to take in the essential client's (PU's) availability. This work builds up a trust-based information accumulation approach to adapt malignant SU assault in spectrum detection of the cognitive radio systems. The proposed plan joins the direct and second-hand detecting confirmation to ensure the general execution and receives a static diversion model to avoid malignant SUs from reporting fake recognition parameters. Theoretical as well as simulation outputs demonstrate that the proposed plan exceeds the conventional aggregation plan regardless of a high rate of malicious hub density and can viably recognize malignant hubs from ordinary hubs by their enumeration scores.

Spectrum detecting, spectrum administration, spectral sharing, and mobility of a spectrum are a portion of the difficulties in CRN security.

Ensuring reliable range discovery is a of the significant applications in-CRs. The fundamental sign assessment is recommendation in the proposed investigation. Trusted on range distinguishing occurs if the fundamental sign is imitated & seen precisely. e.g, a noxious customer just as hackers can interpret the fundamental (essential) customer flag and include the range for childishness (Ian F Akyildiz 2006).

Further, the cloud usageto take out the wrapped porting issues were managed in (Chen et al. 2008). The response for impediment issue was proposed in (Chen et al. 2008) and range distinguishing can be perceived successfully through various customers in a pleasant way. When the free range is distinguished, the best availability bandwidth would be perceived via neighborhood discernments & quantifiable features. The customary controlling issue incorporates the exchanging of safety keys betn the centers. The approval among the centers gives securities & dependability of the trades. This strategy gives the ideal securities however the secret porting issue actually remains.

V. IDENTIFICATION OF PRIMARY USER EMULATION ASSAULTS

Xie et al. (2014) proposed Primary User Emulation (PUE) assaultson Cognitive Radio systems that represent client. Then this limitation result can be contrasted and the known position of the essential client to recognize the PUE assault.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

A PUE recognition component for remote systems with dependable reference senders is outlined and the overhead of the proposed approach and study its sensing precision through simulation.

Peng et al. (2013) have proposed Cognitive Radio (CR) can enhance the usage of the spectrum by making utilization of authorized spectrum in a sharp way. Be that as it may, the security parts of Cognitive Radio systems have gathered little consideration. Here, a danger to Cognitive Radio systems is recognized which is notified as Primary User Emulation (PUE) assault. To counter this risk, another strategy to identify the PUE assaults is proposed which doesnot just examine in two sorts of circumstance in which the essential client is stationary or else it was mobile, additionally it utilize the Kalman Filter Technique to execute received signal strength regard. What's more, from that point onward, the BP neural framework planning & testing is applied to completed the recognizable proof of PUE-attacks. Recreation resultantexhibit the advantages of the given technique.

Chen et al. (2011) analyzed recently, the security issues of the Cognitive Radio (CR) frameworks have drawn an impressive proportion of exploration contemplations. Essential User Emulation Assault (PUEA), as one of ordinary attacks, contributes the range identifying, where a malignant client eliminates empty channels by imitating the essential client to keep other secondary clients from receiving the optimal recurrence groups. Here, another co-operative spectral detecting approach is proposed, considering the presence of PUEA in CR systems.

Zou et al. (2013) have proposed Cognitive Radio (CR) as a promising innovation for future remote range designation to enhance the utilization of the authorized groups. In any case, CR remote systems are vulnerable to different assaults and can't offer proficient security. Primary User Emulation (PUE) is a standout amongst the most genuine assaults for CR systems, which can altogether expand the spectral receiving fault probability. Here, a defense procedure against the PUE assault is proposed in CR systems utilizing conviction propagation, which maintains a strategic distance from the arrangement of extra sensor systems and costly equipment in the systems utilized as a part of the current literature. In this proposed approach, every secondary client figures the nearby local functionality and the similarity work, processes the messages, trades messages with the neighboring clients, and computes the advantages until merging. At that point, the PUE assailant will be identified, and all the secondary clients in the system will be identified in a communicate route about the behavior of the attackers signal. Thus, all SUs can keep away the PUE attackers essential (primary) emulation signal later on. Simulation comes about to demonstrate that the proposed approach delivers rapidly, and it was more reliable to identify the PUE attacker.

VI. BLOCKCHAIN IN SUPPLY CHAIN

Blockchain adoption is gaining huge momentum as industry is evolving at a fast pace. Many startups have initiated use cases and there is significant rise in investments in blockchain projects as well specially across diverse sectors such as supply chain [50] and financial industry has been the prime sector for blockchain adoption. There are many use cases that can apply Blockchain technology for making processes more efficient and effective [58].

With the rise in digitization and process automation organizations need to maintain a competitive advantage by adopting technological enhancements across their process that decrease Turnaround time to address speed to market &the ability to rapidly navigate alteration models of buisness

Supply chains have huge scope for blockchain adoption and involve complex operations and transactions having product variety, global sourcing of components with strong emphasis on efficiency and effectiveness [43].

Supply chains systems involve interaction of multiple stakeholders and participants across various business processes like manufacturing, freight and logistics, financial, sales and distribution. These systems may involve interaction with government entities and several third-party service providers. There is a requirement of a robust system to ensure quick and effective coordination with multiple stakeholders like freight forwarder, customs broker, banks and so on). Supply chains can be significantly transformed by using smart contracts to facilitate trust with the blockchain system and to ensure operations with minimal human intervention.

Production network the executives are to coordinate all the inventory network activities that length all upgradation & crude oil volumes, work-in-measure stock & completed merchandise via the starting place to the utilized mark [45].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

The basic test is to track down the best store network arrangement with the end goal that activities can be acted in an effective and responsive manner administrative and consistence necessities. [57].

Supply chains cover complex interactions of various stakeholders and complexity of operations increase with time [41] [49]. There are many factors that contribute to the complexity of supply chain systems as listed below

- Continuous innovation in product development and service delivery processes.
- Regular change in Continuous extension and topographically spread provider and client organizations.
- Process re-appropriating; hazard the executives' practices and security contemplations.
- Rise of e-business and innovative changes to speed up change in provider organizations and client assumptions.
- Expected expansion in the quantity of members inside the inventory chains.

As supply chains become more complex, this leads to firm's exposure to greater volume of data [37]. This leads to data management challenges to ensure data perceivability and straightforwardness for existing and recently added activities in supply chains. There is risk of reduction of data accuracy as information is obtained from multiple diverse sources [37].

Subsequently, keeping both visibility and value of data in spite of involvement of diverse stakeholders is imperative for sustained efficiency and responsiveness in supply chain systems. As supply chain management covers internal and external participants, appropriate and precise information transfer is mandatory to achieve improved performance in supply chain systems.

VII. BLOCKCHAIN USE CASE SELECTION AND DESIGN PROCESS

Blockchain use case selection involves many decisions based on following criteria and NITI Ayog has published a blockchain use case selection framework [69] as shown in Figure 3.2 that covers all these.

- Is there a compelling business case to reduce intermediaries?
- Are Multiple Stakeholders Involved?
- Are we working with advanced resources rather than actual Assets?
- Do numerous gatherings require shared compose access?
- Do we require superior and fast exchanges?
- Do we plan to store non-conditional information as a feature of your answer?
- Do we need to depend on believed parties for consistence reasons?
- Do we have a powerful Tokenomics Model?
- Do we need the capacity to control usefulness?
- Should exchanges be public?
- The structure presents following four potential results dependent on models,
- Don't use blockchain

Blockchain can't do this effectively yet solutions are in development shown fig 3

- Strong case for public blockchain
- Strong case for private blockchain

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

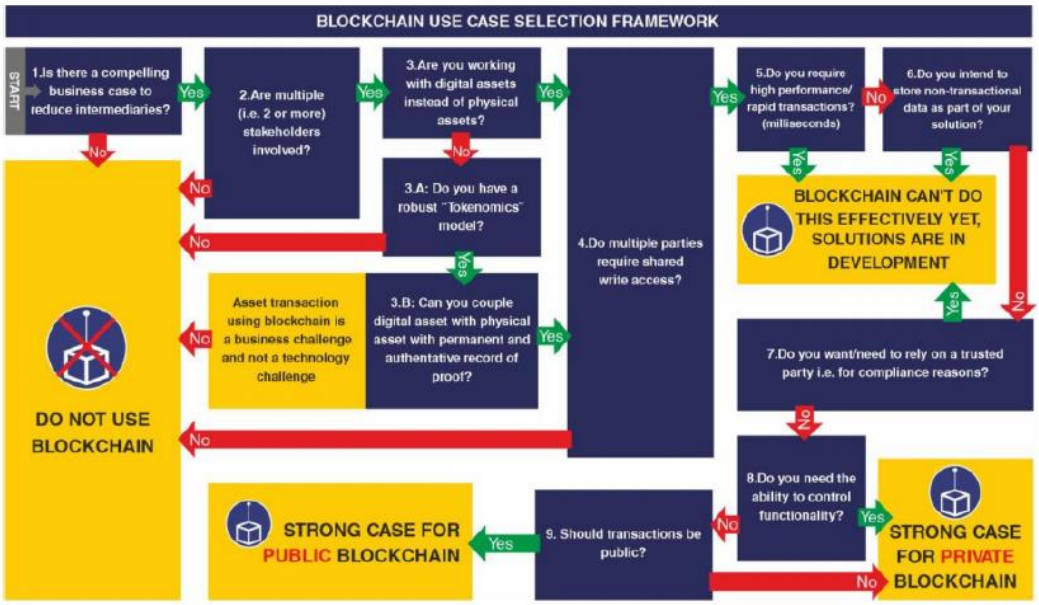

FIGURE 4. FRAMEWORK FOR BLOCKCHAIN USE CASE EVALUATION

From that point onward, an assortment of plan choices around blockchain arrangement should be made, similar to the sort of blockchain, agreement convention, block size and recurrence. The bolts just represent one of the potential groupings to settle on plan choices. A few choices are required to set up acceptable levels of expansion (like block size and rate of occurrence), security, cost of processing and performance [66].

VIII. CONCLUSIONS

In this paper, somewhat recently, extraction of requisition for the remote admittance to the web has caused traffic of some limited groups of ranges of radio wave. Nonetheless, there are a few groups of recurrence that are doled out to the authorized client and are underutilized more often than not. Psychological Radio (CR) is a promising innovation that could beat such difficulties by giving astute admittance to the non-utilization limit. Regardless of the number of advantages brought by CRs to remoted area organizations, such innovative & difficulties notwithstanding those that are as of now present in the remote organizations. In this work, at first the overall ideas of CR, psychological radio organizations, and security issues in intellectual radio organizations were examined. Then, at that point three principle issues in giving got correspondence were distinguished. Blockchain arrangements should be assessed as far as their versatility and cost-viability to address worries of business supervisors. This is a significant test and an unavoidable issue is what might befall the current functional framework and what amount of time it would require to create another blockchain based framework.The motivation of doing this research is to understand and analyze the Blockchain technology, and explore its applicability in addressing challenges of existing supply chain cyber physical systems in a cost effective manner.

REFERENCES

[1] Abbas, Sana-e-Zainab, S & Wajahat 2010, 'An Efficient Algorithm for Secure & Fair Dynamic Spectrum Access in Cognitive Radio Networks', Canadian Journal on Multimedia and Wireless Networks, vol. 1, no. 3, pp. 173-177.
[2] Alishahi, Marvasti & Aref, LM 2009, 'Bounds on the sum capacity of synchronous binary CDMA channels', Journal of Chemical Education, vol. 55, no. 8, pp. 3577-3593.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

[3] Amarnathprabhakaran, A & Manikandan, A 2013, 'An Efficient Communication and Security for Cognitive Radio Networks', International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 2, issue 4, pp. 1689-1696.
[4] Anand Z Jin & Subbalakshmi, KP 2008, 'An analytical model for primary user emulation attacks in cognitive radio networks', DySPAN 2008, 3rd IEEE Symposium, IEEE, pp. 1-6.
[5] Atta & Alireza 2012, 'A Survey of Security Challenges in Cognitive Radio Networks: Solutions and Future Research Direction', Proceeding of IEEE, pp. 3172-3186.
[6] Bhattacharjee, Suchismita & Ningrinla Marchang 2015, 'AttackResistant Trust-Based Weighted Majority Game Rule for Spectrum Sensing in Cognitive Radio Networks', International Conference on Information Systems Security, Springer, pp. 441-460.
[7] Bhattacharya, PP, Khandelwal, R, Gera, R & Anjali Agarwal 2011, 'Smart radio Spectrum management for Cognitive radio', International journal of Distributed and parallel systems, vol. 2, no. 4, pp. 12-24.
[8] Cabric Danijela M Mishra & Brodersen, RW 2004, 'Implementation issues in specrtum sensing for cognitive radios. Signal Systems and Computers', Conference record of 38th Asilomer Conference, IEEE, vol. 1, pp. 772-776.
[9] Chen, R, Park, J & Reed, JH 2008, 'Toward secure distributed spectrum sensing in cognitive radio networks', Communications Magazine, IEEE, vol. 46, no. 4, , pp. 50-55.
[10] Dubey Rajni, Sanjeev Sharma & Lokesh Chouhan 2012, 'Secure and trusted algorithm for cognitive radio network', Ninth International Conference on Wireless and Optical Communications Networks (WOCN), IEEE, pp. 1-7.
[11] Etkin, R, Parekh, A & Tse, D 2005, 'Spectrum sharing for unlicensed bands', Proc. IEEEDySPAN 2005, IEEE, pp. 251–258.
[12] FCC 2003, 'Notice for Proposed Rulemaking (NPRM 03-322)', Facilitating Opportunities for flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies. ET Docket, pp. 03- 108.
[13] Feng Lin, Robert C Qiu, Zhen Hu, Shujie Hou, Lily Liy, James P Browningz & Michael C Wicks 2012, 'Cognitive Radio Network as Sensors: Low Signal-to-Noise Ratio Collaborative Spectrum Sensing', Proceedings of Aerospace and Electronics Conference (NAECON), IEEE, pp. 978-985.
[14] Harish Ganapathy, Constantine Caramanis & Lei Ying 2010, 'Limited Feedback for Cognitive Radio Networks Using Compressed Sensing', IEEE 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton), IEEE, p. 10901097.
[15] Haykin & Simon 2005, 'Cognitive radio: brain-empowered wireless Communication. Selected Areas in Communications', IEEE Journalon, vol. 23, no. 2, pp. 201–220.
[16] Haykin & Simon 2010, 'Cognitive radio: brain-empowered wireless communications', IEEE Journal of Selected Areas of Communication, vol. 2, pp. 201-220.
[17] Ian F Akyildiz, Won-Yeol Lee & Kaushik R Chowdhury 2006, 'Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey', Computer networks, vol. 50, no. 13, pp. 2127- 2159.
[18] Januszkiewicz & Lukasz 2010, 'Simplified human body models for interference analysis in the cognitive radio for medical body area networks', 8th International conference on Medical Information and Communication Technology, IEEE, pp. 15-24.
[19] Juebo & Long Tang 2012, 'Research and Analysis on Cognitive Radio Network Security', Wireless Sensor Network, vol. 4, pp. 120-126.
[20] Khuong Ho-Van & Thiem Do-Dac 2018, 'Reliability-Security Tradeoff analysis of Cognitive Radio Networks with jamming and licensed interfernce', Wireless Communication and Mobile Computing, Hinadwi, vol. 2018, pp. 1-15.
[21] Kwang Cheng Chen, Peng-Yu Chen, Neeli Prasad, Ying-Chang Liang & Sumei Sun 2009, 'Trusted cognitive radio networking. Wireless Communications and Mobile Computing'.
[22] León, Olga, Juan Hernández-Serrano & Miguel Soriano 2010, 'Securing cognitive radio networks', International journal of communication systems no. 5, pp. 633-652.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

[23] León, Olga, Juan Hernández-Serrano & Miguel Soriano 2010, 'Securing cognitive radio networks', International Journal of Communication Systems, vol. 23, issue 5, pp. 633-652.
[24] Mao, Huaqing & Li Zhu 2011, 'An investigation on security of cognitive radio networks', International Conference on Management and Service Science (MASS), IEE, pp. 1-4.
[25] Matteo Cesana, Francesca Cuomo & Eylem Ekici 2010, 'Routing in cognitive radio networks: Challenges and solutions', Ad Hoc Networks, Elsevier., pp. 18-39.
[26] McLoone, Safdar, GA & O'Neillne, M 2009, 'Common Control Channel Security Framework for Cognitive Radio Networks', IEEE 69th, Vehicular Technology Conference, VTC Spring 2009, IEEE, pp. 26-29.
[27] Meng, T 2015, 'Spatial Reusability-Aware Routing in Multi-Hop Wireless Networks', IEEE TMC, DOI 10.1109/TC.2015.2417543 .
[28] Mitola, J & Maguire, GQ 1999, 'Cognitive Radio: Making software radios more personal', IEEE personal Communications, vol. 6, no. 4 , pp. 13-18.
[29] Muhammad Ayzed Mirza, Mudassar Ahmad, Muhammad Asif Habib,Nasir Mahmood, Nadeem Faisal, CM & Usman Ahmad 2018, 'CDSS:Cluster-based distributed cooperative spectrum sensing model against primary user emulation cyber attack', The Journal of Supercomputing, Springer, Available Online, pp. 1-17.
[30] Parvin Sazia & Farookh Khadeer Hussain 2012, 'Trust-based security for community-based cognitive radio networks', IEEE 26th International Conference on Advanced Information Networking and Applications, IEEE, pp. 518-525.
[31] Parvin, Sazia & Farookh Khadeer Hussain 2011, 'Digital signaturebased secure communication in cognitive radio networks', Broadband and Wireless Computing, Communication and Applications (BWCCA), IEEE, pp. 230-235.
[32] Pei, Qingqi, Lei Li, Hongning Li & Beibei Yuan 2012, 'Adaptive trust management mechanism for cognitive radio networks', IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, pp. 826-831.
[33] Peng, Kai, Fanzi Zeng & Qingguang Zeng 2013, 'A New Method to Detect Primary User Emulation Attacks in Cognitive Radio Networks', Proceedings of the 3rd International Conference on Computer Science and Service System, Elsevier, pp. 430-435.
[34] Ping xie, Moli Zhang & Gaoyuan Zhang 2018, 'On physical-layer security for primary system in underlay Cognitive Radio Networks', IET Networks, vol. 7, pp. 68-73.
[35] Sakran, Hefdhallah, Mona Shokair, Omar Nasr, El-Rabaie, S & Atef Abou El-Azm 2012, 'Proposed relay selection scheme for physical layer security in cognitive radio networks', IET Communications, no. 6, pp. 2676-2687.
[36] Shu, Zhihui, Yi Qian & Song Ci 2013, 'On physical layer security for cognitive radio networks', IEEE Network, vol. 3, pp. 28-33.
[37] Song & Yuning 2014, 'A Biology-Based Algorithm to Minimal Exposure Problem of Wireless Sensor Networks', IEEE Transactions on Network and Service Management, vol. 11, no. 3, pp. 417-430.
[38] Syed, ARL 2013, 'On cognitive radio-based wireless body area networks for medical applications', IEEE International Conference on Computational Intelligence in Healthcare and e-health (CICARE), IEEE, pp. 52-57.
[39] Umamaheswari, A, Subashini, V & Subhapriya, P 2012, 'Survey on performance, reliability and future proposal of cognitive radio under wireless computing', 3rd International Conference on Computing Communication & Networking Technologies (ICCCNT), IEEE, pp. 1-6.