International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 SJIF 2023: 8.176 ISSN: 2582-3930

Future Research on Artificial Intelligence & Machine Learning in 5G Network Security

Dr. T. Prem Chander
Associate Professor & Head of the Department, AI & ML Department,
Neil Gogte Engineering College.

Abstract — Recent technological and architectural advancements in 5G networks have proven their worth as the deployment has started over the world. crucial performance elevating factor from access to core network are softwareization, cloudification and virtualization of crucial enabling network functions. Along with the rapid-fire elaboration comes the pitfalls, pitfalls and vulnerabilities in the system for those who plan to exploit it. thus, icing fool evidence end- to- end(E2E) security becomes a vital concern. Artificial intelligence(AI) and machine literacy(ML) can play vital part in design, modelling and robotization of effective security protocols against different and wide range of pitfalls. AI and ML has formerly proven their effectiveness in different fields for bracket, identification and robotization with advanced delicacy. As 5G networks ' primary selling point has been advanced data rates and speed, it'll be delicate to attack wide range of pitfalls from different points using typical/ traditional defensive measures. thus, AI and ML can play central part in guarding largely data- driven softwareized and virtualized network factors. This composition presents AI and ML driven operations for 5G network security, their counteraccusations and possible exploration directions. Also, an overview of crucial data collection points in 5G armature for trouble bracket and anomaly discovery are bandied.

Index Terms — 5G Security, Artificial Intelligence, Machine Learning, Attacks and pitfalls, trouble bracket.

INTRODUCTION

THE continuously evolving communication network armature to integrate different range of bias with unique conditions for different network parameters has redounded in sophisticated challenges for network security. The recent developments in 5G Networks and beyond are easing the immersive growth of data communication by furnishing advanced data rates and pets. similar gigantic increase in data business and connected bias means further vulnerabilities, pitfalls, and attacks performing in disastrous damages financiallysocially and on humanity. thus, checking and analysis of similar Big Data for suspicious conditioning can not only be achieved with traditional/ typical styles. In this environment, Artificial intelligence(AI) and Machine Learning(ML)(1),(2) are envisaged to play a crucial part in working

preliminarily considered NP-hard, and complex optimization problems. The Self- Organizing networks, intelligent and adaptive algorithms enforced in different corridor of network armature paved the way for use of AI and ML with indeed advanced performance earnings at lower costs. The ITU has also established a standard , which outlines the architectural frame and conditions for different use cases of ML in unborn networks including IMT 2020.

Digital bandit have also proven their penetration chops indeed to utmost secure and translated networks by exploiting vulnerabilities. similar vulnerabilities lead to data theft, cyber attacks, structure damage, rescue demands, blackmailing, dislocation of critical services, pitfalls to republic and fatal to mortal lives frequently reported as breaking news. therefore, adding the necessity to also invest in styles which enables safer and secure dispatches with transparent stoner programs, trust models and End- to- End(E2E) visibility. also, 5G and beyond unborn networks armature has seen a paradigm shift from the conception of devoted networks coffers for devoted network functions to further dynamic virtualization, cloudificiation, unity, robotization and softwareization of network functions from common/ combined network coffers(3). These factor put a lesser threat to network security and stoner data if the safety protocols are unfit to not only descry pitfalls and attacks but also help them in real- time(with minimal detention). similar real-time trouble/ anomaly discovery in terabytes of data bear backing of AI and ML. The data collection points can be set in different corridor of the network from access to core network and fed to ML/ AI machines for real- time trouble discovery and attack forestallment.Fig. 1

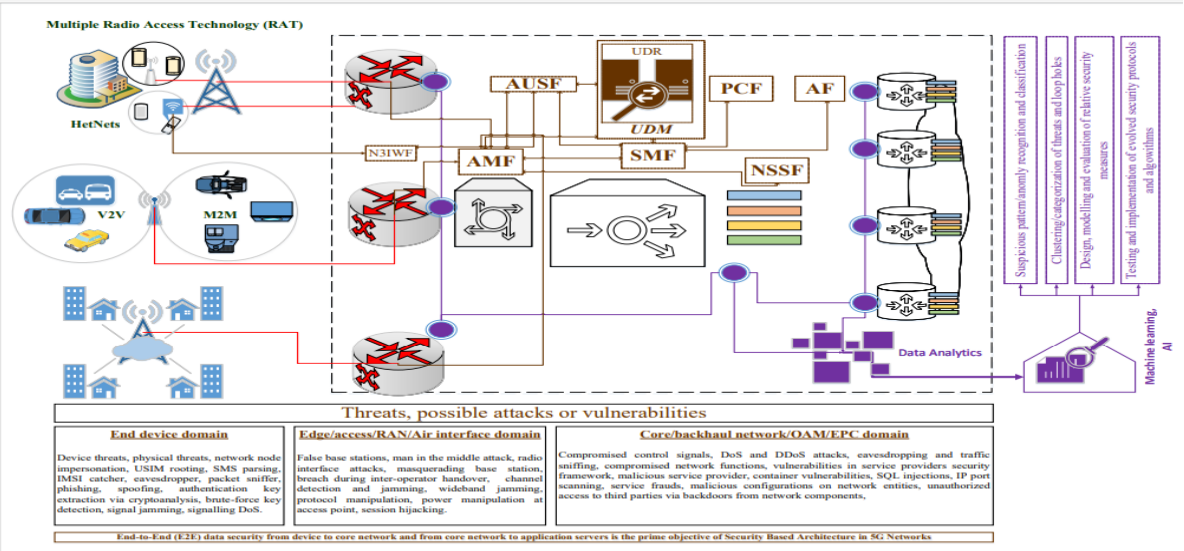

Fig. 1. Envisioned applications of AI and Machine-Learning in 5G Network Architecture.

shows the envisaged armature for integrating AI and ML to descry pitfalls for bracket and testing of security protocols against detected pitfalls attacks in 5G and unborn networks. similar AI and ML supported network security can give cost effective and sustainable results.

The association of the forthcoming content of the composition is as follows. Section II highlights the abstract position details of pitfalls, attacks, and vulnerabilities at different points in 5G networks along with the rearmost developments and standardization conditioning related to 5G and unborn networks security. Section III discusses the taxonomy of AI and ML related technologies along with their perpetration earnings. also, Section IV presents openings, use cases, operations and advantages of different field of AI and ML in 5G security. Section V presents challenges and possible unborn exploration directions of AI and ML supported network security. Eventually conclusions are given in Section VI.

5G NETWORKS SECURITY

The 3GPP Specialized Specifications Group Services & Systems Aspects(TSG SA3) in its Release 14 stressed the 17 crucial trouble/ areas and possible results for security armature of 5G networks. The security armature, procedures and conditions for 5G systems were also formulated in Release 15(R15) in June 2019(4). The R15 includes security norms for standalone andnon-standalone Enhanced Mobile Broadband scripts, whereas, forthcoming R16 and R17 will be fastening on security norms for massive Machine Type Communication and Ultra Reliable Low quiescence Dispatches. The new security features aims to give E2E security along with inflexibility of incorporating multiple authentication fabrics, and higherlayer security protocols to support security for Service Grounded Architecture(SBA) in 5G. The SBA and network slicing in 5G networks allows advanced modularity in the design measure of security protocols. The E2E security armature can be insulated into two groups. The first one named Network Access Security defines procedure and conditions of securely connecting end- device to radio access network. These procedures secure the device connectivity from end device and edge/ RAN disciplines pitfalls as shown inFig. 1. From hereon, icing protection of data and sequestration from access network to core network and beyond can be appertained as Network Domain Security.

Largely software- centric and dynamic 5G network armature where stoner data is covering through several network slices and layers, also bear nimble, adaptive and robust security operation and robotization. Depending on different network slices for different services, the security conditions are also different from featherlight,

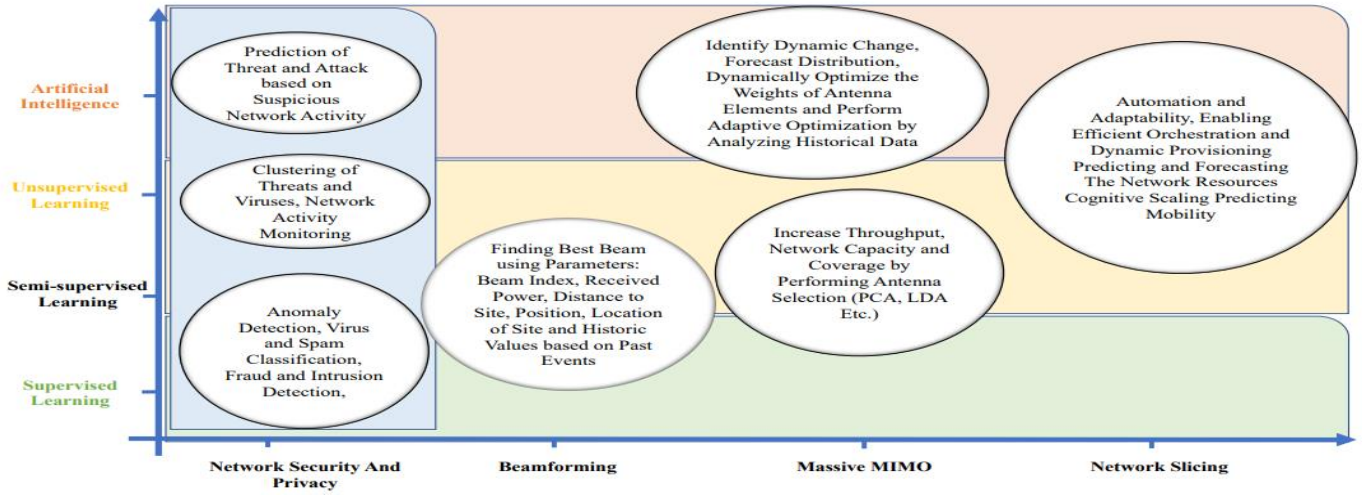

Fig. 2. Applications of Artificial Intelligence and Machine Learning in 5G network

Heavyweight to heavyweight security. These hierarchical security situations suiting requirements of different slices can more fluently be enforced with software- grounded evolving ways. Contrary to this, homemade or traditional need grounded upgrades to network security are no more doable, thus, security robotization should be an integral part of the overall network. Leading assiduity mates are now planning to work AI and ML to incorporate network security for 5G and beyond wireless networks

Recent advancements in AI and ML can enhance the performance of coming- generation 5G networks. AI and ML have opened gateways to new robust and dynamic results in the disciplines of security, sequestration, and trouble discovery in 5G systems. AI and ML has shown significant eventuality in terms of performance earnings for wireless systems in the disciplines of beamforming, massive multiple input multiple affair(MIMO), and network slicing. Different use cases and possible operations of AI and ML for 5G are also shown inFig. 2.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

The conception of using AI and ML in security and sequestration isn't new but their feasibility and performance superiority gained attention with the elaboration of deep literacy(DL) algorithms. utmost of the styles before the development of DL were devoted to model the attack patterns with certain characteristics that are not robust in nature, but with deep AI and ML, it's anticipated that systems will come more flexible towards new sophisticated pitfalls and attacks with dynamic characteristics. Because, bushwhackers use sophisticated ways like obfuscation, polymorphism or impersonation to avoid discovery. From packet capturing and analysis to big data perceptivity, AI and ML can be abused to notify the pitfalls not detected by conventional ways. The patternbased literacy at the core supported by softwarization and virtualization provides dexterity and robustness to timely counter the pitfalls and attacks

AI is showing a positive impact on the information security field. AI algorithms are being espoused to address security and sequestration issues. The information security assiduity is generating further and further data that opens them to advance pitfalls and AI could be a important cure. The first generation of AI results are fastening on checking data, descry pitfalls and help humans in the remediation plan. The alternate generation of AI will make the systems more independent and only leave the critical support issues to humans(5).

Possibilities of AI and ML in 5G

An increased bandwidth, advanced diapason application and high data rates in 5G networks have also widen the trouble and sequestration geography from particular device to the service provider network. therefore, the network should be smart enough to deal with these challenges in realtime and ML and AI ways could help model these robust dynamic algorithms that can help to descry network issues and give with the possible result in real- time. In the same way, AI and ML cover the particular bias that are connected to the internet by furnishing adaptive security results that can attack different network situations, pitfalls, and attacks. In short to medium term plan, AI and ML can be used to descry the pitfalls and fight them with the robust and adaptive security algorithms. Whereas, in the long- term, a completely automated security medium is envisaged for timely response to pitfalls and attacks.

The 5G networks are anticipated to support much advanced position diversity(in terms of connected bias and networks) as compared to its forerunners. For case, G networks support smart vehicles, smart homes, smart structures and smart metropolises. also, the Internet of effects(IoT) in 5G network structure will involve further robust and adaptive ways to handle the critical security issues both at the network and device sides. The security of similar networks will be much further complicated because of the outside intrusion as well as the original intrusion. AI and ML can give results by classifying fragile security links in- between, for case, identity, authentication, and assurance. The security and sequestration in 5G- IoT will cover all the layers similar as identity protection, sequestration, and E2E protection. For case, the crucial authentication frame from end- device to core network and on- ward to service provider, while concealing the crucial identifier is still a complex issue. We believe AI and ML can also play an important part in crucial authentication along with effectively minimizing the masquerading attacks.

Feeding for security and sequestration of data from these different systems with uniquely different security conditions come a tedious task. important AI and ML with overview of SBA and security conditions for different end- systems can can descry and amend these issues in real- time by classifying and clustering unusual pitfalls. This, in turn, greatly help the pool chops deficit in information security assiduity. AI and

ML can help in developing security mechanisms by creating trust models, device security and data assurance to give methodical security for the whole 5G- IoT network.

APPLICATIONS OF AI AND MACHINE LEARNING FOR 5G SECURITY

Substantially, AI and ML algorithms are data-empty in nature which means that data is demanded to train the model for effective functioning. In the period of 5G, data generation, storehouse, and operation isn't delicate as we have high computational power, exponential data growth, and data sources. The network can be maintained, penetrated and analysed for possible pitfalls, attacks and vulnerabilities using AI and ML at a lower cost of computing, and affordable structure.Fig. 3 epitomized the colorful operations of AI and ML in network security. AI and ML models can be used to descry suspicious conditioning in real- time by analysing network exertion patterns and parameters. Bracket algorithms can be used to descry anomalies by covering network parameters similar as outturn and network error logs. Clustering algorithms can be used to classify colorful kinds of pitfalls and loopholes in network security. The models similar as statistical conclusion attacks and generative inimical networks(GAN) can induce fake datasets to develop and estimate new security measures as well as testing and enforcing evolved security protocols and algorithms.

The exploration in developing private AI and ML models have seen some significant progress in secure calculation, encryption, sequestration, and allied literacy. mongrel models are created by espousing ways from different fields to make models effective, briskly and generalized. The most common and popular illustration is the discriminational sequestration introduced by Google security and sequestration platoon(6). The secure calculation field is making new progress by adding up distinct protocols for faster calculations(7). Some exemplifications include Gazelle, TAPAS, and Faster CryptoNets that are used for secure calculation with homomorphic encryption. SecureNN is an ML result that uses comparison-grounded operation of neural networks for bit birth and secret sharing(8). Federated literacy and secure enclaves are also using AI and ML- grounded models similar as Slalom, Chiron and Ekiden.

Another recent trend is the development of general and robust anomaly discovery algorithms which deals with unknown attacks(9). AI and ML can be applied to deal with utmost of the operations similar as antivirus scanner systems, intrusion discovery, spam pollutants, and fraud discovery systems. The styles generally work on data generated by network business, host processes,etc. Unsupervised algorithms similar as neural networks and clustering can be used to help humans in relating suspicious conditioning

The 5G and beyond network counting on SBA, independent decentralized network functions and third- party waiters will pose a lesser trouble in terms of Denial- ofService(DoS) andcyber-attacks. therefore, devoted agents according to the sphere of network factors can better safe- guard these factors in particular and

overall system in general. colorful AI and ML results have been presented to deal with decentralized networks 10). The recent results are using several underpinning literacy(RL) and deep underpinning learning DRL) ways to deal with similar attacks(11). In case of jamming attacks where, the hackers jam the radio frequence(RF) signals, DRL grounded results were

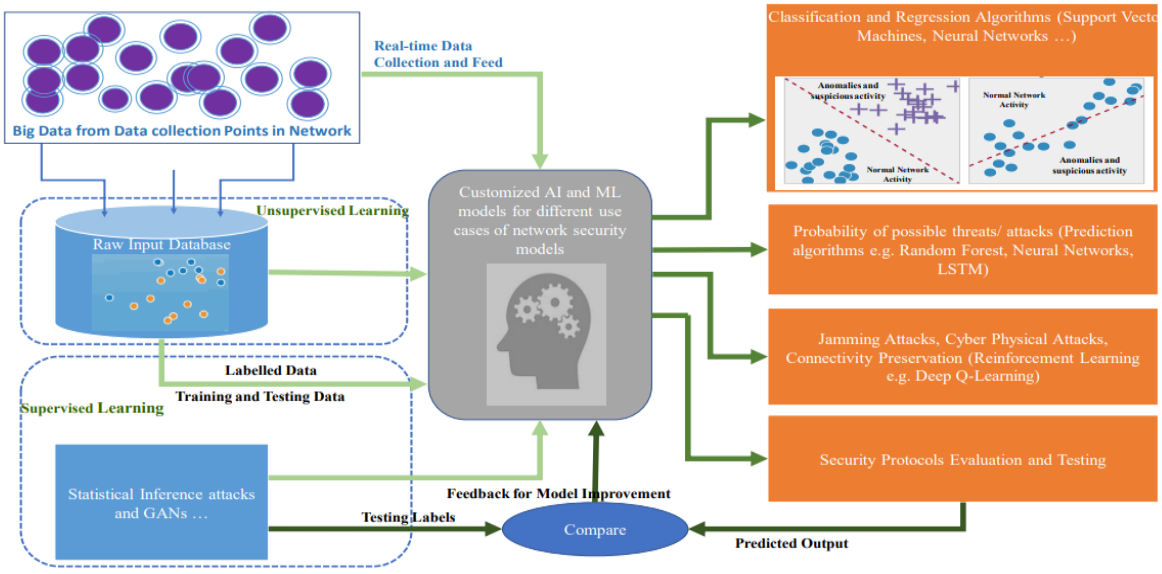

Fig. 3. Different application scenarios and use cases of AI and ML assisted Network Security.

developed that elect applicable frequence channels and avoid attack using an optimal policy learned on former compliances. Cyber-physical attacks manipulate data to gain control of the system. These kinds of attacks generally do on independent systems similar as smart vehicles(12). DRL provides independent systems the capability to learn from the time- varying compliances to induce optimal conduct so that the system can be more robust and dynamic. DRL systems show decent progress in connectivity preservation among robots to support effective communication

Deep Literacy(DL) is also furnishing its benefit to cybersecurity results as it can automatically learn patterns from once entries to avoid unborn intrusion and identify irregular patterns. DL has been successfully stationed in structure- position security(anomalies discovery on the physical network), software- position security (malware, contagion and botnet discovery in the mobile network) and stoner-position security(private information protection)(13). Different variations of DL networks similar as bus-encoders, thick networks, and Convolutional Neural Network are used in several security operations including malware discovery, DoS delving, flooding, instant signal- to- noise rate variations, and colorful othercyber-attacks. At the software- position, DL networks are used in the bracket of vicious operations, spams, unknown business, and botnet. In the case of stoner sequestration, DL has shown its eventuality in data participating problems, information leakage, and sequestration preservation. Table I summarizes the

crucial enabling technologies among AI and ML for implicit security operations along with their advantages.

OPEN RESEARCH CHALLENGES AND FUTURE DIRECTIONS

The end of completely automated cyber defense system might be a long- term thing, but meanwhile, the cost of integrating AI and ML for being and unborn systems also need rigorous analysis. also, it's also being reported thatcyber-hackers have also started taken advantage of AI and ML grounded smart algorithms for attacks and vulnerability exploitation. As, perpetration studies are still being conducted on safe, smart and important integration of AI and Ml, some abecedarian challenges still need a critical exploration and analysis. For case, in chancing anomalies in a network, first, we need to define normal. Network exertion is infrequently normal, and thus, a completely supervised orsemi-supervised network would be one possible way to deal with in this situation. ML models use large gobbets of data to learn and make pattern for retrogression on unseen data. If the network parameters are changed drastically or variations are to be set up, the network will collapse during deployment and thus, a retrain of the network will be needed. utmost of the ML styles including DL are black box in its retired layers and thus, the sapience of its expression on the trained data is limited in nature. Data sequestration is one of the most important issues as AI and ML algorithms feed on data. The use of data in ML increases the threat for an attack as models are trained on the data which can be used for data mining purposes as well.

SUMMARY OF AI-ASSISTED TECHNOLOGIES AND THE POSSIBLE CASE SCENARIOS ALONG WITH THEIR ADVANTAGES AND CHALLENGES

AI/ML methodologies	Key techniques	Key features and applications in network security	Advantages
Supervised learning	Bayesian classification. K-Nearest Neighbor (KNN). Neural Networks (NN). Generative Adverserial Network (GAN). Support Vector Machine (SVM). Decision Tree (DT) classification. Recommender System.	Classification and regression-based security algorithms design. Identity fraud detection and email spam detection. Risk and threat assessment. Pattern recognition and computational learning theory. Security algorithm design, development and update. Algorithms for anomaly detection. Packet level analysis for packet-level security framework. Distributed Denial of Service (DDoS) detection and prevention.	Software-centric security for heavily software-driven network. Flexible algorithm modelling with evolving functionality. Adaptive security management and automation. Overcoming the workforce and skill shortage with automation. Resolves complex optimization problems. Agile and self-evolving design of security mechanisms. Reduced cost of security operations.
Unsupervised learning	Hierarchical clustering. Reinforcement learning. Dimensionality reduction. Association analysis. Hidden Markov analysis. Big data visualization.	Malicious content detection from incoming/outgoing traffic analysis. Segregation of legitimate and illegitimate users and traffic. Fully automated grouping/clustering from immensely large traffic data patterns. Security framework optimization from a limited group of data sets (traffic patterns). Application/network slice-based traffic steering. Powerful tools of analyzing, monitoring and checking on-going traffic.	Automated clustering from highly dynamic data sets. Association mining of features based on common traits. Real-time implementation. Discover unusual data points.
Reinforcement learning	Real-time decisions. Robot navigation. Q learning. Deep Q learning. Skill acquisition. Game AI.	Automated actions based on the severity of detected events or breaches. Automatic adaptation for updated data patterns. Pattern driven decisions and predictions for future attacks.	Highly robust and trained agent for timely decision making. Efficient for mission-critical and delay-sensitive digital infrastructure. Higly adaptable for tackling with diverse set of threats.

ML- grounded security results are always vulnerable to new types of sophisticated attacks similar as GANs. Experimenters have tested the vulnerability of ML- grounded security models using dissembled GANs(14).

security models using dissembled GANs(14). 5G- IoT security and sequestration needs further disquisition in the disciplines of authentication, authorization, access control, and sequestration-conserving. The current 3GPP defined networks use functional knot specification and epitome interfaces but in 5G IoT, the network itself will serve as core structure and security assurance will be the crucial challenge to deal with. At this stage, semi-supervised AI- supported results better suits the distributed systems. With the elaboration of AI algorithms, these system will come completely automated in the future.

Another exploration trend is dealing with wiretapping in trusted communication over 5G networks. AI and ML could be used in maintaining device security as well as high subcaste security in IoT. AI and ML models are flexible and scalable security results that can consider multiple network layers for trust modeling and identity operation, security assessment, and sequestration protection as well as energy-effective.

Lately, GANs are shown to mimic the exact affair of a network whilst having no access to the training data. By using creator and discriminator DNNs in a single training medium, the networks contend with one another where the creator generates new data samples whereas the discriminator distinguish them as real or fake; settling onto a game proposition approach. The final affair is a network that can no longer distinguish between the real or fake samples of data and thus, it can successfully induce new samples of unseen data. This basically means that a GAN can extemporize stoner authentication medium, induce phishing data, flood tide core network with spam signaling, all without being exposed to the factual network. GAN pose a series of pitfalls to the ongoing development of AI and ML for network security since it can deceive the core network with accurate authentication.

CONCLUSION

This paper presents AI- supported technologies, scripts and operation for security of 5G and beyond wireless networks. The largely dynamic business patterns, service- grounded network armature, distributed network functions and authentication over multiple waiters in 5G and beyond networks bear fairly robust, nimble and completely automated security frame. similar frame is erected- upon smart AI technologies. AI can significantly ameliorate the security for distributed ad- hoc setup of network structure furnishing different network functions. At this stage,semi-automated security frame is more suitable, still, with continuing elaboration in AI technologies and feasibility studies of safe perpetration of these technologies will decide the end thing of complete robotization. Substantial exploration is demanded to address the challenges and issues before AI completely takes over the digital robotization.

REFERENCES

(1) X. You,C. Zhang,X. Tan,S. Jin, andH. Wu, " Ai for 5g Research directions and paradigms, " Science China Information lores,vol. 62,no. 2,p. 21301, 2019.

(2) M. Yao,M. Sohul,V. Marojevic, andJ.H. Reed, " Artificial intelligence defined 5g radio access networks, " IEEE Dispatches Magazine,vol. 57,no. 3,pp. 14 – 20, 2019.

(3) R. Khan,P. Kumar,D.N.K. Jayakody, andM. Liyanage, " A check on security and sequestration of 5g technologies Implicit results, recent advancements and unborn directions, " IEEE Dispatches checks & Tutorials, 2019.

(4) 3GPP, " Security armature and procedures for 5g system, " specialized specifications, 3rd Generation Partnership Project, June 2019 2019.

(5) J.-H. Lee andH. Kim, " Security and sequestration challenges in the internet of effects(security and sequestration matters), " IEEE Consumer Electronics Magazine,vol. 6,no. 3,pp. 134 – 136, .

(6) M.U. Hassan,M.H. Rehmani, andJ. Chen, " Differential sequestration ways for cyber physical systems A check, " IEEE Dispatches checks Tutorials,pp. 1 – 1, 2019.

(7) M.S. Riazi,C. Weinert,O. Tkachenko,E.M. Songhori, T. Schneider, andF. Koushanfar, " Chameleon A cold-blooded secure calculation frame for machine literacy operations, " in Proceedings of the 2018 on Asia Conference on Computer and Dispatches Security, ASIACCS ' 18,(New York, NY, USA),pp. 707 – 721, ACM, 2018.

(8) H.C. Tanuwidjaja,R. Choi, andK. Kim, " A check on deep learning ways for sequestration- conserving, " in International Conference on Machine Learning for Cyber Security,pp. 29 – 46, Springer, 2019.

(9) M.H. Bhuyan,D.K. Bhattacharyya, andJ.K. Kalita, " Network anomaly discovery styles, systems and tools, " Ieee dispatches checks & tutorials,vol. 16,no. 1,pp. 303 – 336, 2013.

(10) Y. Dai,D. Xu,S. Maharjan,Z. Chen,Q. He, andY. Zhang, " Blockchain and deep underpinning learning empowered intelligent 5g beyond, " IEEE Network,vol. 33,no. 3,pp. 10 – 17, .

(11) N.C. Luong,D.T. Hoang,S. Gong,D. Niyato,P. Wang,Y.- Liang, andD.I. Kim, " operations of deep underpinning learning in dispatches and networking A check, " IEEE Dispatches checks & Tutorials, 2019.

(12) A. Ferdowsi,U. Challita,W. Saad, andN.B. Mandayam, " Robust deep underpinning learning for security and safety in independent vehicle systems, " in 2018 21st International Conference on Intelligent Transportation Systems(ITSC),pp. 307 – 312, IEEE, 2018.

(13) C. Zhang,P. Patras, andH. Haddadi, " Deep literacy in mobile and wireless networking A check, " IEEE Dispatches checks Tutorials,vol. 21,pp. 2224 – 2287, thirdquarter 2019.

(14) L. Huang,A.D. Joseph,B. Nelson,B.I. Rubinstein, andJ.D. Tygar, " inimical machine literacy, " in Proceedings of the 4th ACM factory on Security and artificial intelligence,pp. 43 – 58, ACM, 2011